# WILEY HANDBOOK OF SCIENCE AND TECHNOLOGY for HOMELAND SECURITY

EDITED BY

JOHN G. VOELLER

WILEY

# WILEY HANDBOOK OF SCIENCE AND TECHNOLOGY FOR HOMELAND SECURITY

# WILEY HANDBOOK OF SCIENCE AND TECHNOLOGY FOR HOMELAND SECURITY

Edited by

**JOHN G. VOELLER**
Black & Veatch

The Wiley Handbook of Science and Technology for Homeland Security is available online at:
http://mrw.interscience.wiley.com/emrw/9780470087923/home/

WILEY

**A JOHN WILEY & SONS, INC., PUBLICATION**

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada



***Library of Congress Cataloging-in-Publication Data:***

Wiley handbook of science and technology for homeland security / edited by John G. Voeller, Black & Veatch.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-471-76130-3 (cloth : set) – ISBN 978-0-470-13846-5 (cloth : v. 1) – ISBN 978-0-470-13848-9 (cloth : v. 2) – ISBN 978-0-470-13849-6 (cloth : v. 3) – ISBN 978-0-470-13851-9 (cloth : v. 4)
1. Civil defense–Handbooks, manuals, etc. 2. Security systems–Handbooks, manuals, etc. 3. Terrorism–Prevention–Handbooks, manuals, etc. I. Voeller, John G.
UA926.W485 2010
363.34–dc22
2009041798

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

# CONTENTS

# PREFACE

The topic of homeland security did not begin with the World Trade Center or the Irish Republican Army (IRA) or the dissidents of past empires, but began when the concept of a nation versus a tribe or kingdom took root and allegiance to people was a choice, not a mandate. The concept of terrorism is part of homeland security but not all of it, as there are other risks to homeland security that come from Mother Nature or our own lack of action, like infrastructure renewal, that have much higher probabilities of creating substantial damage and loss of life than any group of terrorists could ever conceive. Hence, the focus of this Handbook focuses more on the insecurities that can disrupt or damage a nation, its people and economy, and the science and technology (S&T) ideas and tools that can assist in detecting, preventing, mitigating, recovering, and repairing the effects of such insecurities.

The number of S&T topics that are involved in the physical, cyber, and social areas of homeland security include thousands of specialties in hundreds of disciplines, and no single collection could hope to cover even a majority of these. The Handbook was designed to discuss those areas that form a foundation of knowledge and awareness that readers can use to base their understanding on and move to higher levels of sophistication and sensitivity as needed. For example, the many different areas of detection of chemical substances alone could take around 100 volumes to cover, but there is a subset of this knowledge that brings the reader a solid base on which to build a more advanced knowledge view, if desired. Such subsets in each major topic area were the targets of the Handbook.

The Handbook is organized in sections with each addressing a major topic from cyber security to food safety. The articles within each section are designed to range from instructions about fundamentals to some of the latest material that can be shared. Over time, we will add new sections and articles within each to make the Handbook a living entity. John Wiley & Sons has done many such large collections, some being truly massive, and has developed support systems to address such a challenge.

Several key goals were paramount in the creation of this Handbook. First was to gather true experts from all sources to talk about S&T for homeland security, homeland defense, and counterterrorism with very limited control over what was presented. Some of what is done in this vast S&T space has to be classified so as to not "communicate our punches" to our adversaries, which is especially true in a military setting. However, homeland security is largely domestic, and solutions must be available for sale, operation, and maintenance in public infrastructure and networks. Having experts speak in an open channel in the Handbook is important to inform the public, officials, law enforcement, researchers, academics and students so that they can work together and increase our collective national knowledge.

A second goal was to take a portion of the thousands of possible sources of knowledge about the hundreds of S&T topics that are part of homeland security and put them in one location. Moreover, this Handbook increases the opportunity for an expert in one topic to easily find connected, adjacent or codependant topics that would have normally required other searches, references and licenses to access. Homeland security involves so much of cross-discipline action and interdependency examination that this goal was considered especially important.

A third goal was to create a venue where knowledge of different theories, approaches, solutions, and implications could be compared. There are many ways to address homeland security concerns and needs in different disciplines and specialties that nothing less than a multivolume, multiyear project looking for hundreds of authors out of thousands of candidates was required. The Handbook addressed this by the services of some of the best in the world in each major topic area acting as Section Editors. These top experts knew whom to invite, whom could contribute, and most important how much of the overall knowledge in their specialty could be conveyed without drifting into sensitive areas. The Handbook would have been impossible to produce without their incredible efforts in selecting, reviewing, and overseeing their section content.

A fourth goal was to provide a place where even experts in one facet of homeland security could learn about other facets with confidence that the quality of the information would meet their standards. From exceptional discussions about how the European Union views cyber security differently from the United States to massive work on all the different food-safety-detection equipment available, the focus of all contributors was journal quality, peer-reviewed knowledge, with references and links to additional knowledge to allow the reader to go deeper.

A fifth goal was the creation of a substantial enough body of knowledge about the many different facets of homeland security so that policy and decision-makers could get a picture of how much has been done and how much needs to be done to create robust solutions in all the needed areas. Even in places that have dealt with terrorism for over a century, the world still does not have strong, cost-effective solutions to some of the most fundamental problems. For example, we have very limited to no ability to spot a bomb in a car moving toward a building at a sufficient distance to know whether to destroy or divert it before it can damage the target. Even simpler, the ability to spot a personnel-borne improvised explosive device (IED) in a crowd coming into a Las Vegas casino is still beyond our collective capability. The bounding of what we know and don't know that can be applied in a domestic setting needed to be documented at least in part for dozens of major areas in homeland security.

A sixth goal that was not part of the pages of the Handbook was to create a visibility of expertise among all the contributors and reviewers to help them connect with others and

enable collaboration. Only a large collection of this type creates such a vast opportunity in known areas of S&T for shared learning and new relationships.

A seventh goal was to present the S&T of homeland security in a way that would allow one of the most important aspects of the economics involved to be considered. This is not the economics of creating or acquiring one solution but rather finding more than one use for a given solution. An inescapable issue in many areas of homeland security S&T is that a fully successful solution applied to only one small market will likely fail because there is insufficient revenue and market to sustain the provider. Building a few hundred detectors for specific pathogens is likely to fail because of lack of volume or will perhaps never see funding as this becomes evident in the original business plan. The solution to this issue is finding multiple uses for each device. For example, a chemical detector looking for contraband or dangerous materials a few days a year may provide continuous service in looking for specific air pollutants related to allergy mitigation in a building. The Handbook provides exposure to the reader in capabilities built for homeland security that might bring benefit in other more frequently needed areas thereby making both applications more viable.

The Handbook authors were asked to contribute material that was instructional or that discussed a specific threat and solution or provided a case study on different ways a problem could be addressed and what was found to be effective. We wanted new material where possible, but given the nature of a handbook we wanted to also bring great work that might already be published in places not easily encountered and with proper permission could be repurposed into the Handbook for broader visibility.

One of the conditions set by the Senior Editor before taking on the project was that the Handbook needed to be published both in print and on the Web. The dynamic online collection will not only allow new articles and topics to be added but also updated when threats, solutions, or methods change. The Senior Editor greatly appreciates John Wiley & Sons for accepting this challenge.

The Section Editors of the Handbook have done a superb job of assembling their authors and topics and ensuring a good balance of foundations and details in their articles. The authors in the Handbook have produced valuable content and worked hard with the Wiley editing staff to enhance quality and clarity. And finally, the Wiley staff has taken on the management of hundreds of contributors with patience and energy beyond measure.

This Handbook was conceived as a living document designed to mutate and grow as the topics presented changed or the capabilities of S&T advanced to meet existing and new threats. We hope readers will consider how they might be able to contribute to the Handbook body of knowledge and consider writing about their special expertise for submission sometime in the future.

*Editor-in Chief*
John G. Voeller

# INTRODUCTION AND OVERVIEW

# POLICY DEVELOPMENT FOR HOMELAND SECURITY

JEFFREY HUNKER
*Carnegie Mellon University, Pittsburgh, Pennsylvania*

## 1 INTRODUCTION

In science and technology, five factors make effective and consistent Policy Development for Homeland Security difficult [1].

- The definition and goals of Homeland Security continue to evolve.
- Multiple decision makers and high levels of organizational complexity diffuse decision-making authority and responsibility and make policy prioritization difficult.
- Policy prioritization is further challenged because of the breadth and ambiguity of Homeland Security threats. This, together with highly differentiated interests and levels of support for different projects from the research community challenge policy makers ability to distinguish and invest in the important, not just the interesting.
- Metrics for judging project contribution frequently are difficult to create.
- Distinct roles for key Homeland Security functions—intelligence, prevention, response and reconstruction, and "defend and respond"—overlap with and can be difficult to distinguish from the Nation's overall National Security agenda.

For the practicing policy maker, these characteristics—shifting goals, complex and competing interests, and difficulty in measuring results—are not uncommon. It is the mark of good policy development to overcome these challenges and to produce results that benefit the nation.

## 2 OVERVIEW OF POLICY DEVELOPMENT

Policy development, in any field, is an art, not a science.

## 2.1 Defining Policy; Defining Homeland Security

A *policy* is an attempt to define and structure a rational basis for action or inaction [2]. Policy is a long-term commitment; tactics are short-term actions. Tactics and implementation are overlapping concepts in the execution of policy.

Policy also needs to be distinguished from (but overlaps with) *administration* and *politics*. "Administration" is the "management of any office, employment, or organization direction" [3]. Administration is decision making in bounded rationality—making decisions that are not derived from an examination of all the alternatives [2, p. 278]. *Politics*, from the Greek for citizen, is about "exercising or seeking power in governmental or public affairs" [3]. Policy, at least ideally, takes into consideration all alternatives, distinguishing it from administration. A focus, or lack thereof, on power distinguishes policy from politics.

However, policy development is critically constrained by both administration and politics. Political feasibility requires elected officials (or their proxies) to support the policy. Organizational feasibility requires the requisite organizations to support the policy and implement it in a way that makes its success possible [4] (President Kennedy is noted for saying "I like the idea, but I'm not certain that the Government will".).

*Homeland Security*, the object of policy development for this article, has a shifting definition. *The National Strategy for Homeland Security* (2002) defines it as "a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur" [5]. In practice, however, homeland security now includes protection against and response to natural or accidental manmade disasters, such as hurricanes and toxic spills.

Reflecting this reality, this article principally will address policy development related to terrorism, but will also refer to issues in the prevention and response to natural and accidental disasters.

Homeland Security is thought of in multiple ways even within the narrower confines of protection against terrorism. For example, in protecting key economic and national security assets such as the electric grid, our telecommunication network, and basic utilities, different constituencies will refer to agendas in "critical infrastructure protection (CIP)", "critical information infrastructure protection", or "protection of physical assets". These agendas overlap, but each has its own scientific and political constituency.

The shifting definition of "Homeland Security" as a policy goal prompts three observations. First, prevention and response to natural and accidental disasters is a relatively mature policy agenda in comparison to the terrorism agenda (though provision of insurance for hurricane disasters and perspectives on climate change challenge policy makers and politicians alike). Had not the Federal Emergency Management Agency (FEMA) and the Coast Guard—two principal Federal agencies with responsibilities for natural and accidental disasters—been included in the Department of Homeland Security, it may indeed have been the case that the "mission creep" apparent in the definition of Homeland Security would not have taken place.

However, whether or not natural and accidental disasters are "Homeland Security" issues, policy makers at Department of Homeland Security (DHS) must address these agendas. Their challenge is to integrate and seek synergies in pursuing disparate policy goals. The search for synergies is an important, but oftentimes overlooked, element in policy development. Finally, FEMA's performance, in particular, in responding to Hurricane Katrina highlights the gulf between policy and implementation that policy makers ignore at their peril. The author has reviewed the policies regarding hurricane

response in the Gulf of Mexico; on paper they appear more than adequate. Implementation was the problem.

## 2.2 The Policy Development Process

A common characterization of policy development, useful but inaccurate, lists a series of steps [2, p. 77]:

- *Defining the problem.* What is the context for a policy?
- *Defining the solution.* Who specifies it, the and why?
  - Identifying alternative responses/solutions
  - Evaluating options
  - Selecting the policy option
- *Implementation.* Who implements it, and why? Who follows it, and why?
- *Evaluation.* How is conformity with a policy tracked and evaluated?

This taxonomy is useful in that it describes the steps that any emergent policy follows. However, this taxonomy ignores the real world of policy making, involving interacting cycles of multiple constituencies within government (at many different levels) and outside of government [2, p. 80].

An example of Homeland Security policy development helps to illustrate this observation: In 1999, during the preparation of the first National Plan for Information Systems Protection (the National Plan) [5, 6] a series of informal discussions between two White House offices (the National Security Council and the Office of Science and Technology Policy) and other Executive Branch agencies (the National Science Foundation (NSF) and the Critical Infrastructure Assurance Office (CIAO)) led to the insight that most federally funded cyber security R&D was directed toward mission-specific goals of the funding agencies (e.g. the Defense Advanced Research Projects Agency (DARPA) and the National Security Agency (NSA). Consequently, there were serious gaps in addressing research questions that, although important, did not garner a specific agency constituency. Following several workshops with outside researchers and prolonged internal discussions, a proposal was developed to create a "virtual National Laboratory"—a consortium of US-based research institutions—charged with identifying and addressing the gaps in the Nation's cyber research agenda. This work led to the inclusion in the National Plan of the goal to "establish a new public–private mechanism to coordinate Federal R&D in information systems security with private sector needs and efforts" [6, p. xxi].

Discussions with Congressional members and staff during 1999 evinced considerable interest, but no positive results. Meanwhile, a number of research institutions began vigorously to express interest both to Congress and the Executive Branch in becoming the host institution. That year, Congressional action, independent of Administration's thinking as to possible host institutions, created the Institute for Security Technology Studies (ISTS) at Dartmouth College. With the creation of the DHS, funding and oversight of the ISTS was located in the Science and Technology Directorate. Oversight of ISTS initiatives always has been vigorous, but no quantifiable metrics for performance exist.

There are several lessons from this example. In developing the policy options, there was never a formal development and ranking of alternatives. Consultation with constituencies within and outside the Federal government (Congress, Federal agencies

funding cyber R&D, first responders, and outside research institutions) was continuous throughout the policy development process. Events (such as the placement at Dartmouth) were not necessarily planned by the policy makers (though not unwelcome). Quantifiable metrics were never developed; in particular there was never any consideration of cost/benefit analysis.

A final point—of all of the stages of policy development, policy evaluation is perhaps the most difficult. Practicing policy makers often describe policies as "*effective*" or "*ineffective*", yet the policy literature speaks most often of "*efficiency*". A particular allocation of resources is *efficient* if and only if there is no better allocation of those same resources [4, p. 32]. A policy is *effective* if it is adequate to accomplish a purpose, producing the intended or expected result [3]. From a practitioner's perspective, measures of allocative efficiency are rarely meaningful—effectiveness is the most commonly employed heuristic.

To summarize, policy development does not translate easily into the abstract. The context for a policy, who specifies it, who implements it, who follows it, and how conformity of policy is tracked and evaluated, are situation specific. Some generalizations are possible, but not many.

## 3 CASE EXAMPLES OF POLICY DEVELOPMENT

Three short case examples illustrate the range of issues in developing Homeland Security policy.

### 3.1 Cyber Security: A Challenge of Defining the Threat and Establishing Incentives

"Cyber Security" means security of our electronic information and communication systems—notably the Internet but also proprietary computer networks (whether used by business or government) including wireless networks [7].

The focus here is on intentional attacks, and mostly on attacks that could affect the "critical functions" that keep a society running well—in commerce, government, and national security/homeland defense.

Following Presidential Decision Directive 63 in May 1998 (CIP) the protection of cyber and information systems against attack has been a national priority. The Department of Defense (DOD), with a focus on protecting its own extensive systems, and DHS, in the Information Analysis and Infrastructure Protection Directorate, have primary Federal responsibility. National Plans and associated Research and Development plans coordinate Federal policy. Private sector participation is key to the policy's effectiveness. In particular, sector specific organizations (e.g. for banking and financial institutions) have been created to both promote private sector cyber security and, very importantly, share information within themselves and with the Federal government about cyber threats and attacks [8].

Our understanding of threats, however, is limited. Proactive anticipation of new threats is difficult because the complexity of software makes *a priori* identification of security vulnerabilities difficult and because new forms of attack (e.g. spear phishing, or distributed denial of service attacks) continually evolve. Publicly available statistics on cyber security are poor. Surveys and compilations of cyber attacks and violations

rely on voluntary reporting, and interviews with Chief Information Officers and other officials responsible for security indicate a widespread reluctance to report most intrusions, including even attempted intrusions [9]. With this caveat, the following are examples.

- More than 2,000,000 personal computers are infected and attackers store and serve pornography from them, attack other computers or send out spam using them, or install spy ware to obtain credit card numbers and other personal information.
- Large numbers of sensitive government and contractor computers have been infected with hidden software that records everything done on those computers, and reports back to those that installed that software [8].

General types of threats may include:

- *Cyber-crime* (phishing, extortion, fraud, etc.). This crime is already rampant and is growing in scale and sophistication.
- *Cyber-terror* (attacking a crucial website or a computer-controlled infrastructure (e.g. the electric power grid) or, for example, attacking New York Stock Exchange (NYSE) systems). Many "mischief" attacks of this kind have already been tried and succeeded. They too could easily grow in scale and sophistication—with the potential for use by terrorists.
- *Cyber-warfare* (cyber-terror or cyber-espionage used by one state against another). It appears that this has already been tried at least twice, in the Chinese attempts at reprisals against United States government information networks after the May 1999 accidental bombing of the Chinese embassy in Belgrade, and again by Russian distributed denial of service attacks against Estonian computer networks in May 2007 (both countries deny any involvement).

But key unanswered questions persist. What are the chances that a skilled group of cyber-criminals might hire themselves out as mercenaries for cyber-terror or cyber-warfare? What might they be most likely to attack, and how? Our ability to answer these questions is limited, yet an understanding of where and how threats might materialize is central to building effective policies for protection and response.

Consequently, our security responses, though often quite sophisticated, tend to be piecemeal, ad hoc, and not infrequently focused on the short term.

The possible consequences are not well characterized either. These may include:

- immediate damage or disruption ("planes fall out of the sky", the power grid goes down);
- loss of confidence (e.g. no confidence in NYSE systems, so people begin to take their securities listings and their trading somewhere else);
- general deterioration of an industry or an activity due to constant low-level incidents.

A second major cyber security policy challenge is to create incentives for action. Software developers, for example, are largely immune from tort liability actions challenging the security and reliability of their products. Several states have codified this exemption. The "tragedy of the commons" is also at work in networked systems. The software that

acts as "traffic cop" for the Internet—the Border Gateway Protocol (BGP)—is sensitive to accidental (or deliberate) misconfigurations. A decade ago an accidental BGP misconfiguration redirected the entire Internet to a single site in Florida. Although technical solutions to make a repeat of this incident less likely exist, in essence, no single Internet routing point has an incentive to install these solutions. Hence, a decade later, the network still relies upon the good faith and good programming skills of an increasingly large (and increasingly global) community of service providers.

Cyber security presents an example of how although national focus has led to an extensive and detailed policy framework, it has failed to address key foundations. Scientific and understanding the extent and nature of cyber threats, and in technical work in technology solutions (e.g. encryption, firewalls, and intrusion detection) abounds; however, progress in creating risk management systems, and managerial/network imperatives for action are far less advanced.

### 3.2 Fire: Consistent and Effective Public–Private Partnership

Fire has long been recognized as a serious danger to urban society, commerce, and natural systems. There have been myriad individual homes and businesses destroyed by fire, and occasional large-scale catastrophes—the great London and Tokyo fires of the 17th century, the Chicago fire, and major forest fires such as in Yellowstone Park a decade ago. Though yet to occur, major urban conflagrations, from nuclear or other causes, remain a real, though distant, threat.

Four major outcomes have emerged from our concern with fire.

- Governments, private businesses, and citizens have long worked to *understand* how fires start and spread, how they can be contained and extinguished, and how they can be prevented. Continuous and sustained research has successively addressed new issues, as, for example, when new materials enter into building construction or furnishings, or when new sources of combustion, such as electrical wiring, are introduced. Research takes place at the Federal (e.g. National Institute of Standards and Technology), state, and private sector levels.
- In parallel, common pools of risk knowledge have been created, updated, and perhaps most importantly, widely shared among insurers, risk managers, and researchers. This statistical data provides the necessary foundation for managing the risk of fire.
- The result is a well-developed system in which we have fire codes, fire insurance, agreed-upon standards for products and for fire protection systems, and well-defined procedures and resources in place for calling firefighting companies to the scene of a fire—all backed up by a good knowledge of what the losses could be, in terms of both dollars and human life, and therefore a good way of assessing risk, justifying costs, and compensating for damage.
- For the (fortunately) special case of major conflagrations (forest fires, major urban conflagrations) a well-exercised system of coordinated Federal resources (Department of the Interior, Department of Agriculture, Defense Department (National Guard), DHS (FEMA), and state and local assets) is in place.

The policy response to fire exemplifies an almost three century-long process integrating widespread recognition of the threat together with private and public investments in

understanding the threat, working to reduce it, creating systems to respond to fires (large and small) when they occur, and developing sophisticated regulatory and risk management mechanisms to reduce and spread risk. What is most notable is that this policy structure was not created "top–down", but developed from enlightened self-interest and the recognition of a Federal role in two dimensions—research and emergency response and reconstitution. The policy structure is not perfect; for example a comprehensive national fire code has yet to be adopted in place of a myriad of local codes. Nonetheless, it stands as a model of successful policy development.

### 3.3 Y2K: Top–Down Policy Response to a Specific Threat

From the preparation and execution of Y2K some key lessons can be drawn.

- A clear decision for action was made by the White House, with clear goals and timelines.
- A strong leader, with close ties to the President, and extensive business and government credibility, was chosen.
- Education—of the business community and government agencies—was a major and long term focus.
- Incentives, but not regulation, were used to enhance both action and cooperation among the private sector. For example, the Securities and Exchange Commission (SEC) did not require filing organizations to take action, merely to report publicly in their filings what if any action an organization was taking. National legislation, to promote information sharing and reduce liability for Y2K related actions, was enacted.
- Public–private partnership was emphasized.
- A sophisticated operations' center, coordinating business and government resources and information, was built (the Information Coordination Center); strong leadership (a retired Marine Corps General) led the effort.
- Constant and effective communications kept the press and public informed.
- Extensive and effective outreach to key non-US constituencies, including the UN, helped to ensure that preparation for the Y2K event was, if not global, certainly not exclusively a US priority.
- The core operational team managing the issue was a tight, small, high quality team based at the White House.

The response to the "Y2K bug" illustrates an effective policy development and implementation process. Clear goals (motivated by a pressing threat, though skeptics abounded), strong leadership, effective implementation driven by a subtle combination of "carrot-and-stick", and measurable outcomes (things either worked, or they did not) characterize this initiative.

Some key observations emerge from these case examples. Policies, however detailed, that fail to address fundamental issues reduce their likelihood of being effective (this is sometimes referred to as the "elephant in the drawing room" syndrome—there's an elephant, but no one acknowledges its presence). Policy can be emergent, constructing itself through the uncoordinated actions of various constituencies. Clear goals, strong leadership, and measurable outcomes are critical to successful policy.

## 4 SELECT RESEARCH AGENDAS AND IMPLICATIONS FOR POLICY DEVELOPMENT

A representative but certainly not exhaustive list of major Homeland Security research topics illuminates some key drivers for policy development.

One taxonomy [10] for research divides scientific challenges into those which have been around for a while and those which have emerged more recently, either in response to new policy concerns (e.g. terrorism, global climate change, and so on) or evolutions in the technology frontier (e.g. greater computational and networking capabilities).

The former includes:

- identification and treatment of known pathogens;
- better technologies for emergency responders;
- blast-resistant and fire-resistant structures;
- air filtering against known pathogens and chemicals;
- decontamination techniques; and
- technologies to enhance security against cyber attacks.

Areas that have emerged more recently include the following.

- creating an intelligent, adaptive electric power grid;
- revising land use and disaster preparedness/response policies in the face of global climate change;
- capturing, analyzing, and assessing useful information for emergency officials and responders with new sensor and surveillance technologies;
- creating a common risk model that allows comparison between and across infrastructures;
- developing methodologies to accurately identify and predict both actors perpetrating and motivations for cyber attacks;
- identifying and predicting paths and methods of currently undetectable food and water alteration;
- developing networks—both physical (e.g. transportation) and electronic (e.g. the Internet) in which security is being imposed as a basic design consideration, not as an add on;
- designing self diagnosing and self repairing systems and facilities; and
- providing a common Homeland Security operating picture available to all decision makers at all levels.

Many other agendas exist. For example the *Draft National Plan for Research and Development in Support of Critical Infrastructure Protection* [11] identifies nine key themes.

- detection and sensor systems;
- protection and prevention;
- entry and access portals;
- insider threats;

- analysis and decision support systems;
- response, recovery, and reconstitution;
- new and emerging threats and vulnerabilities;
- advanced infrastructure architectures and system design;
- human and social issues.

With a mission of "filling gaps" in the Homeland Security R&D agenda, the Institute for Information Infrastructure Protection has identified potentially key R&D grand challenges [12]:

- secure digital healthcare infrastructure;
- value-added infrastructure protection;
- cost-effective CIP through Information Infrastructure Resilience;
- trusted realms;
- national critical infrastructure web for disaster and attack management, analysis, and recovery;
- spatial clustering of information infrastructure—a basis for vulnerability assessment;
- beyond the domain name system (DNS); and
- establishing a national identity.

*Implications for Policy Development:* These lists of noteworthy projects challenge policy development for Homeland Security in at least four ways.

- There exist numerous and highly differentiated scientific and technical agendas. New challenges with long-standing infrastructures—such as port security—or new issues—like the identification of potentially explosive liquid combinations—continue to emerge. For policy makers, no clear, widely accepted methodology to prioritize initiatives across domains exists.
- Input metrics (e.g. dollars spent) for each initiative are easy to develop; meaningful output metrics (e.g. how much safer are coastal communities from the threat of catastrophic hurricanes, how much safer are US citizens from terrorist threats) largely do not exist.
- The scientific and technical communities demonstrate widely different levels of interest and effort in engaging these topics. For example, of 80 key researchers in Homeland Security at a 2005 conference [13], less than 6 were focused on human and social issues such as insider threats. Detection and sensor systems were the focus of the bulk of the work.
- Some issues of perhaps paramount importance barely appear in the research portfolio. There appears to be a systematic underinvestment in key areas like human social interactions. Interoperability between networked systems was the subject of a recent special session of the IEEE, and is, arguably, a critical element in any system of effective Homeland Security, yet little basic work appears to be taking place [14].

Thus, opportunities in scientific and technical research and deployment for Homeland Security are numerous and varied; this abundance challenges policy makers in establishing clear goals and monitoring and assessing their impact.

## 5 ORGANIZATIONAL COORDINATION FOR POLICY

The multiplicity of research agendas as well as organizations with a stake in research and development make vital a strong and dynamic integrative framework for communication and cooperation across domains and constituencies, both for policy makers and researchers. Some agendas address issues of immediate concern and impact, while others focus on expanding the frontiers of knowledge. Shortly we will consider in detail an example of such an effective integrative framework, but first we will outline some overall challenge to policy coordination.

### 5.1 Complexity of the System

Homeland Security should not be thought of as the DHS, but as a system that incorporates a breadth of constituencies—Federal agencies, states and localities, private organizations, individual citizens, and other countries and international organizations.

At least 22 disparate organizations make up the DHS [1, pp. 59–60], [15]. In addition, the FBI, DOD, and the intelligence community are parts of this system. Policy development for science and R&D in this complex system faces several tensions:

- identifying and establishing policies for R&D requirements;
- matching these with the threats;
- resolving organizational conflicts over resources and priorities; and
- measuring progress and success.

Complexity can be viewed on at least two planes. Within the Federal government most agencies have at least some part of the Homeland Security agenda. As an example, the *National Strategy to Secure Cyberspace* engages at least 15 major Federal departments and agencies apart from DHS. Each element brings to bear differing perspectives (law enforcement, National R&D capabilities, new technology policies, and responsibility for economic sectors or citizen concerns) [15, pp. 348–350, 416–419]. Within this framework, the ultimate level of coordinating authority matters. While in the Clinton Administration coordination ultimately rested with a National Coordinator of White House rank, coordination for cyber security policy now resides at a lesser level within DHS.

A more complete, and hence complex, picture of the same agenda (again, only a small part of the Homeland Security agenda) shows how many agents at the first level, firms and their individual actors, at the second, a panoply of legal instruments and national plans (including but not only those of the US), and finally a larger and emerging multinational agenda play a role, each with its own area of focus.

A short (and partial) listing of the published policy plans gives a rough idea of the variety of Homeland Security policies.

- DHS, *Interim National Infrastructure Protection Plan* (2005).
- DHS, *National Response Plan* (2004).
- National Research Council, *Making the Nation Safer: The Role of Science and for Countering Terrorism* (2002).
- Office of Management and Budget (OMB), *2003 Report to Congress on Combating Terrorism* (2003).

- RAND National Defense Research Institute, *The Physical Protection Planning Process*, Proceedings of workshops (2002) sponsored by OSD.
- White House, Homeland Security Presidential Directive 7 *(HSPD-7): Critical Infrastructure Identification, Prioritization, and Protection*, 2003.
- White House, *National Strategy for Homeland Security* (2002).
- White House, *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (2003).
- White House, *National Strategy to Secure Cyberspace* (2003).
- White House, NSC-63; *Critical Infrastructure Protection* (1998).

### 5.2 Coordination of Policy

Overall coordination of these policies takes place in three levels [15].

At its highest level, a Homeland Security Coordination Council, modeled in part on the National Security Council (Cabinet level attendance) provides integration.

For the plethora of plans, several key instruments are used.

- *National Response Plan (NRP)*: The purpose of the NRP is to establish the single comprehensive approach required to enhance US ability to respond to domestic incidents. It provides a framework of incident management protocols to address these threats. Established on the basis of HSPD-5—Management of Domestic Incidents (2003)—the NRP applies to high impact events requiring a coordinated and, as appropriate, combined response. As a Response Plan, it does not directly establish science policy, though as a policy document it has a major impact [16].
- An integral component of the NRP is the National Incident Management System. Its purpose is to provide a consistent nationwide approach to prepare for, respond to, and recover from domestic incidents of consequence.
- HSPD-7 assigns responsibility to Sector Specific Agencies' (SSAs) designated for protection activities in specific areas—for example the Department of Energy is responsible for protection of energy assets, including the production, refining, storage, and distribution of oil, gas, and electric power. SSAs report to the DHS on these actions.

As the examples of Y2K and fire protection policy illustrate, numerous and engaged constituencies need not be a barrier to effective policy. However, the evolving definition of what comprises Homeland Security, the long histories of many of the organizations involved, and the sometimes inchoate understanding of what the goals of Homeland Security policy are certainly challenge effective policy making.

## 6 FEDERAL CYBER SECURITY R&D POLICY: AN EXAMPLE OF EFFECTIVE POLICY DEVELOPMENT

Since 1998, the framework for cyber security R&D has evolved, and now shows great promise of providing an effective framework for decision making. It serves as a good example both of how structures for policy coordination and development evolve over

time, and also of how coordination can be achieved by the thoughtful use of metrics and the acquisition of supporting data.

Three themes stand out in this evolution

- focusing the policy making process to incorporate needed cross-cutting and integrative perspectives;
- developing and institutionalizing detailed knowledge of both the "baseline" of R&D projects, and current and projected resource allocations for these projects; and
- Continuous progress to seamlessly integrate cyber security R&D into the CIP agenda, and the even broader homeland security agenda, while also tackling difficult challenges such as technology transfer of R&D results.

As such, federal cyber security R&D policy is a good example for readers of this article.

It is worth noting that federal cyber security programs are relatively small, both in terms of the number of people involved and the dollar amounts. Total federal support for cyber security R&D is of the order of $500 mm, with much of it within the DOD. The number of policy makers engaged is also small. Cyber security R&D is a complex topic, however, and requires a probably unprecedented understanding of and cooperation with the private sector in order to be effective.

### 6.1 Focusing the Policy Making Process

After PDD 63, the Critical Infrastructure Protection R&D Interagency Working Group (CIP R&D IWG) was formed to coordinate federal R&D policy. The IWG included the principal agencies that performed cyber security R&D work (Defense, National Science Foundation, National Institute of Standards and Technology, and Energy) as well as representatives from agencies charged with working with specific private sectors (energy, information and communications, banking and finance, transportation, vital services, and international). The IWG had a complex reporting structure—a theme that runs through the entire evolution of the policy making process here—and reported to three groups: (1) the Committee on National Security, part of the National Science and Technology Council (NSTC)that in turn was chaired by the White House Office of Science and Technology Policy (OSTP); (2) the Committee on Technology (also a NSTC committee); and (3) the Critical Infrastructure Coordination Group, responsible for coordination all CIP policy, which was chaired by the National Security Council.

The CIP R&D IWG organized its work by sector, and, while important work was done, the sector focuses inadequately addressed at least five challenges [10, p. 4]:

- many different sectors contain infrastructure that is vulnerable to exactly the same threats;
- the majority of the sector specific policies did not address the inherent and broadly applicable interdependencies between infrastructure sectors;
- physical threats and solutions were considered separately from cyber threats and solutions;

- the process was challenged to address simultaneously two different paths toward improved security—special efforts to reduce vulnerabilities and improvements coming from the normal efforts to design new infrastructures for higher performance and quality of service;
- The process was also challenged in evaluating new threats and opportunities coming from new technological advances that might not be readily incorporated into the normal design process.

Along with these challenges, starting in 2002 a number of other changes in the overall policy environment led to a restructuring of the organization and focus of federal cyber security R&D policy. The *Cyber Security Research and Development Act* (Nov 2002) gave responsibility for coordinating cyber security R&D to OSTP, with special charges to NSF and NIST to perform research. The *National Strategy to Secure Cyberspace* was issued in February 2003. The report recommended that OSTP coordinates development of an annual federal cyber security research agenda. Homeland Security Presidential Directive 7 (December 2003) required an annual CIP R&D plan to be developed by OSTP and DHS. A series of outside reports on cyber security R&D—from the National Science Foundation (2002), RAND (2002), the President's Information Technology Advisory Committee (February 2005), and the interagency InfoSec Research Council Hard Problem List (November 2005)—all provided perspective on research priorities, or appropriate strategies, for federal cyber security research.

Following one intermediate reorganization of the policy making process, in mid 2005 the Cyber Security and Information Assurance Working Group (CSIA) was formed to shape federal cyber security R&D policy, reporting to both the NSTC Subcommittee on Networking and Information Technology R&D (NITRD) and the Subcommittee on Infrastructure. Reflecting the continuing theme of complex reporting relationships, these subcommittees in turn report variously to the NSTC Committees on Technology and Homeland and National Security.

Three important and positive changes resulted from this evolution.

- NITRD jointly overseeing CSIA made explicit the recognition that cyber security has a broad impact on the nation's interests beyond just CIP.
- In place of sector-specific policies, initiatives are organized around integrative themes addressing both physical and cyber threats and solutions. In the April 2006 cyber security R&D plan [17] there are eight initiatives:
  - functional cyber security and information assurance;
  - securing the infrastructure;
  - domain-specific security;
  - cyber security and information assurance characterization and assessment;
  - foundations for cyber security and information assurance;
  - enabling technologies for cyber security/information assurance R&D
  - advanced and next-generation systems and architecture;
  - social dimensions of cyber security/information assurance.

- Policy themes and projects are compared and correlated with outside perspectives, starting with the NSF and RAND reports, and also the R&D chapters of the "sector specific" plans developed for the National Infrastructure Protection Plan, and international perspectives from the EU and elsewhere. There is also continued consultation with academia, government labs, and industry. There is a strong match between the themes and projects prioritized by all groups, and recent consultations have surfaced only a few projects that were not already in the plans [18].

### 6.2 Transparency into the Granularity of Projects and Budgets

A second very important evolution in cyber security R&D policy development has been to create the administrative systems so that decision makers can look at the universe of individual R&D projects and the resources applied to each project.

Previously, there was no comprehensive database of cyber security R&D projects across relevant Federal agencies. A major step forward over the past two years has been to create a very specific database by project—a "program" level perspective is too coarse to provide the needed insight into various efforts—cross-referenced by threat, by sector, by technology, by stage of the project (e.g. basic research), and by agency.

Together with this baseline of projects is a breakout of budget support for cyber security research, starting with the President's FY07 budget submission. Previously, budget amounts for cyber security research were difficult to identify because they were often grouped with noncyber security research in other program areas. While some agencies did not participate in the FY07 NITRD budget breakout for cyber security R&D in the FY07 budget supplement (notably DHS and some elements of the Department of Energy), the Office of Management and Budget's annual budget guidance now requires agencies to submit separate budget amounts for cyber security R&D as part of their annual budget submissions.

These reforms provide two important benefits.

- Decision makers are now able to map R&D priorities against the set of specific projects and their funding, and identify gaps in the national agenda;
- Individual agencies can now identify areas where their individual interests and projects complement or duplicate work going on elsewhere in the Federal government.

### 6.3 Integrating Cyber Security R&D into Broader Agendas

There is a complex and not universally agreed-upon overlap and integration between the concepts of "cyber security", "CIP", and "homeland security", and this article is, simply put, not the place for an adequate discussion of these issues. Suffice to say that there is a multiplicity of plans addressing some of these different perspectives, as well as a widespread feeling that ultimately cyber security R&D policy needs to be integrated into a comprehensive homeland security R&D policy that also includes consideration and linkages to issues like weapons of mass destruction, and other threats to homeland security. There is also a need to adopt a national perspective—not just a government perspective—that incorporates private sector initiatives and priorities.

Both of these thrust for broader integration are underway. Work is currently being done to integrate cyber and weapons of mass destruction R&D policy, with an explicit

goal, as one policy maker said, of "erasing some of these plans" [18]. With "sector coordinating councils" that serve as the forum for dialog between government and the private sector, there is also a forum that appears to be reasonably effective in talking with industry. Hence, the current policy framework shows great promise of being able to not only provide an integrated platform for making effective choices about cyber security R&D policy, but also a way of integrating cyber security with other facets of the broad homeland security R&D agenda across both the government and private sector.

### 6.4 Challenges

The progress made in creating a framework for effective cyber security R&D policy is by no means complete. One major challenge, for example, is to improve technology transfer from federally funded R&D projects into the hands of users. This is a long-standing challenge, and agencies have adopted various strategies and programs to address it. NSF, for example, largely relies on the project specific researchers to disseminate the results of their work, while the service laboratories in the defense department have technology transfer offices charged with that mission. What is important to note is that this issue is very much a focus of attention by policy makers in OSTP and elsewhere charged with cyber security R&D, and that, while the challenge of tech transfer may never be "solved", considerable improvement can, and most likely will, be made.

To summarize, there is value in looking at instances in which policy system has evolved to provide an ongoing and sustaining framework for better decision making. The evolving structure for Federal cyber security R&D policy provides one such example.

## 7 LESSONS FOR BETTER POLICY DEVELOPMENT

With a broad set of science and technology research initiatives, the role of Homeland Security policy is to drive, in the national interest, to match policy needs with opportunities. Some key themes for improving policy development for Homeland Security include the following:

### 7.1 Threats Should Prioritize Policy

Effective Homeland Security policy development is challenged by our incomplete articulation of what we are preparing either to defend against or respond to. The inability to clearly identify threats has at least three significant consequences.

- *Blurring the distinction between policy and tactics.* Policy defines the (longer term) investment interests, tactics relate to more immediate actions, and without a lack of clarity in threats, policy and tactical responses are blurred, and implementation suffers.
- *Impeding organizational coordination.* With multiple and indiscriminate threats, different organizations will focus, without clear metrics, on their perceptions, not on the national needs.
- *Impeding the prioritization of policy goals.* Above all, the lack of a clear structure linking threats to goals tries our ability to prioritize resources to goals of greatest importance.

### 7.2 Tension, Managed Properly, Makes Good Policy

As an element of good policy development, a tension needs to be managed—but not avoided—between duplication of initiatives on one hand, and on the other hand ensuring a portfolio of projects, perhaps in some cases competitive, but integrated into an operable policy framework.

### 7.3 Better Metrics Are Needed

Sometimes metrics need not measure direct impacts, but can be proxies for outputs that are inherently difficult to capture. A non-Homeland Security example: ALCOA embarked on a corporate wide and intensive program to improve its safety performance. The genius of this high priority initiative was that a focus on safety was in fact a proxy for a wide range of process improvements within the company and its network of suppliers and customers. A safer workplace was not only a laudable goal in itself, it drove major productivity improvements.

### 7.4 Implementation Matters

Although policy defines and structures a basis for action, the impact of policy ultimately depends on the actions taken by the plethora of actors—Federal, state, and local agencies; the private sector; and individuals—who are, figuratively or literally, "on the ground". Creating the incentives and structures for assessing effort and impact remains perhaps the single greatest weakness in policy development and implementation—and also the greatest opportunity for improvement.

### 7.5 Clarifying the Line Between National Security and Homeland Security

Among the major challenges are the existing distinctions between Homeland Security and "National Defense" generally. DOD policies and willingness to engage in homeland defense continue to evolve; a clear set of policies here are needed [1, pp. 213–230]. Secondly, the integration of federal programs and investments with state and local capabilities (both as first responders and as an integral part of ensuring defensive and protective capabilities) is an area for improvement. While integrated communications capabilities, for example, are important, a stronger integration into R&D is needed.

However, an expansion of a single integrative organization—an original conceptualization of DHS—would address this second concern, but does not appear to have much promise given current political realities.

### 7.6 Leveraging Lessons from the Private Sector

The use of market mechanisms may provide novel insight for more effective policy development, particularly in science and research. Managing key financial and operational risks is central to any organization (e.g. even the United States Government has "Continuity of Government" requirements). Greater use of market mechanisms may prove an important part of better linking policy goals with effective implementation.

### 7.7 Delegating Responsibility and Dividing the Labor: Who Deals With What?

Ultimately, one who studies Homeland Security policy development is faced with a troubling observation: it remains unclear as to who knows what to do, who manages or drives the policy agenda, and who is in charge of implementation. Ultimately, who terminates projects, and nurtures others? Who reviews the portfolios of investments? Who are the "they" who really will make the decisions?

## 8 CONCLUSION

As this article indicates, policy development for homeland defense not only supports a vigorous science and technology portfolio but also has room for improvement. Both from a science and technology perspective and as an operational set of activities, significant reforms need to be made. Lessons from our existing post 9/11 experience, from other successful (and less successful) federal agencies, and from non-federal sources can all provide useful insights.

In conclusion, four observations were made

- Policy development for homeland security is highly complex for reasons both of substance and organization.
- Policy making and implementation is fundamentally challenged by the need for effective communication and cooperation—with appropriate metrics to support these policies.
- R&D policy faces a tension between duplication and managing portfolios of competitive initiatives integrated through an operable policy framework;
- Competing interests in conjunction with great organizational and topical complexity can mask or provoke a gap in leadership. Who actually is in charge—both with "big" decisions and smaller projects?

## REFERENCES

1. Ranum, M. J. (2004). *The Myth of Homeland Security*, Wiley Publishing Company, Indianapolis, Indiana, pp. 1–50 for a good overview (total pages 1–230).
2. Parsons, W. (1995). *Public Policy: An Introduction to the Theory and Practice of Policy Analysis*, Edward Elgar, Brookfield, Vermont, p. 14 (total pages i–xviii, 1–675).
3. Stein, J. (1966). *The Random House Dictionary of the English Language; The Unabridged Edition*, Random House, New York.
4. Munger, M. C. (2000). *Analyzing Policy: Choices, Conflicts, and Practices*, WW Norton and Co., New York, pp. 14–15 (total pages I–xvii, 1–430).
5. The White House. Office of Homeland Security (2002). *National Strategy for Homeland Security*, The White House, Washington, D.C., July 2002, p. 2. (total pages 1–71).
6. The White House (1999). *Defending America's Cyberspace: National Plan for Information Systems Protection (draft)*, The White House, Washington, D.C., May 1999 (total pages i–xxvi,1–128).

7. Fischer, Eric A. (2005). Creating a National Framework for Cyber Security: An Analysis of Issues and Options. CRS RL 32777, Congressional Research Service, The Library of Congress, February 22, 2005. p. 6, 1–56.
8. *The White House, The National Strategy to Secure Cyberspace.* Washington, DC: The White House, February 2003.
9. Paller, A. (2006). *Research Director, The SANS Institute, Bethesda, Maryland*. Presentation at Carnegie Mellon University, May 2006.
10. *Commentary from Guidance for Writers on Wiley Handbook of Science and Technology for Homeland Security* (2006). John Wiley and Sons, Hoboken NJ.
11. Executive Office of the President, Office of Science and Technology Policy, Department of Homeland Security, Science and Technology Directorate (2004). *The National Plan for Research and Development in Support of Critical Infrastructure Protection*, Washington, DC, pp. 23–67 provides detail in each policy area (total pages 1–81).
12. The Institute for Information Infrastructure Protection www.theI3P.org.
13. *Critical Infrastructure Protection Workshop for Academic and Federal Laboratory R&D Providers* (2005). Science and Technology Directorate, Department of Homeland Security, Washington, DC, June 29, 2005.
14. *IEEE Special Session on Integration and Interoperability of National Security Information Systems* (2006). Cambridge, MA, June 8–9, 2006.
15. Kean, T. H., Hamilton, L. H., Ben-Veniste, R., Kerrey, B., Fielding, F. F., Lehman J. F., Gorelick, J. S., Roemer, T. J., Gorton, S., Thompson, J. R. (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, W.W. Norton and Company, Inc., New York, pp. 423–428 (total pages).
16. U.S. Department of Homeland Security (2005). *Interim National Infrastructure Protection Plan*, Washington, D.C., February 2005, pp. 38–39 (total pages 1–35).
17. U.S. Department of Defense (2005). *Strategy for Homeland Defense and Civil Support*, Washington, D.C., June 2005 pp. 36–38 (total pages 1–40).
18. National Science and Technology Council (2006). Interagency Working Group on Cyber Security and Information Assurance. *Federal Plan for Cyber Security and Information Assurance Research and Development*, National Science and Technology Council, Washington, April 2006.
19. Voeller, J. (2006). OSTP, December 2006.

## FURTHER READING

US Department of Justice. *Computer Crime and Intellectual Property Section* www.cybercrime.gov.

US Government Accountability Office (2001). Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform. *Homeland Security: Key Elements of Risk Management* Statement of Raymond J. Decker, Director Defense Capabilities and Management, October 12, 2001. www.house.govInternational CIIIP Directory, based on the G-8 CIIP Experts Initiative. E-mail ciip-directory @niscc.gov.uk for more details.

Other US Government documents: *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets; National Strategy for Homeland Security; National Strategy to Secure Cyberspace*.

David, M. (2002). *Concepts for Enhancing Critical Infrastructure Protection Relating Y2K to CIP Research and Development*, Santa Monica.

National Infrastructure Security Co-ordination Center (NISCC) www.nisc.gov.uk.

# THREATS AND CHALLENGES TO HOMELAND SECURITY

DAVID M. WEINBERG
*Practical Risk LLC, Rio Rancho, New Mexico*

## 1 THREAT SPECTRUM

This survey article is not meant to be exhaustive in detail or citations. Rather, it highlights some conventional threats and challenges and also attempts to tease the reader to consider some less conventional threats. This is done to stimulate the interest of the research community, and to play their role in one of the most complicated issues facing the United States and its people.

Within the context of governmental homeland security, the word *threat* has different meanings to different people and organizations. This article attempts to look at threat in conventional and some unconventional ways. Similarly, the term *challenges* carries much semantic heft, and it too will be considered in terms of conventional ways and otherwise.

Threat is commonly taken to mean that set of activities and purposes aimed at doing harm. Although this definition may be thought to specifically refer to the threat of terrorism, it actually applies to natural hazards and catastrophic accidents as well. A discussion of threat can be broad indeed.

Conventionally, terrorism threat is generally dissected into two components: namely, intent (to perform an act) and capability (resources, including intellectual, to accomplish the act). Recent work by Williams [1, 2] adds a third dimension (or metric), at least to radical jihadist terrorism, namely, authority. Within the Department of Homeland Security (DHS), some workers also break capability into subcomponents such as the intellectual capability to conceive and design what is needed for an attack and the capability to infiltrate the nation, organize all necessary manpower and material logistics, and remain undetected until the attack is executed.

Clearly, the topic of threat includes getting into our adversary's head. This topic is being addressed by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) [3]. Therefore, for the purposes of this article, it is preferable to start this discussion with something a bit simpler than *threat* and examine things that could cause harm in a somewhat more generic sense.

## 2 TYPES OF THREATS AND CHALLENGES

Terrorism attacks can generally be broken into those that are physical attacks (i.e. 9/11), virtual attacks (i.e. computer hacking and viruses), and a category best described as "other". Physical attacks represent a broad spectrum of possible attack modes

(often referred to as *threats* or *threat vectors*) that include the likes of much of what is seen in the media on an all-too-frequent basis. These attacks include improvised explosive devices (IED), a mode faced repeatedly by our troops in Iraq, backpack bombs such as used in the London and Madrid bombings, and suicide vests seen worldwide. An IED's big brother is a vehicle or vessel borne improvised explosive device (VBIED), differing from the IED in its delivery mechanism, size, and potential for destruction. These two attack modes or threat types make up the greatest statistical population of terrorist attacks across the world [4, 5]. Less often experienced within the homeland are other physical attacks that include assassinations and kidnapping, although we have seen these modes perpetrated by terrorists carried out on US citizens abroad.

These conventional physical attacks represent a type-of-attacks spectrum, namely from the somewhat impersonal attack on a group to the very personal attack on an individual. In both cases, there is some individual or group that has conspired to directly harm the homeland and/or its citizens by using a specific designed-for-purpose weapon.

As a class, such threats are fairly predictable in their effect, and to some degree, in their standard practices and procedures. While various types of attacks are "pigeonholed" below for convenience of discussion, it is acknowledged that such summarization may contribute to artificially discretizing what is a continuous, multidimensioned spectrum. For brevity and simplicity, neither multiple attacks, simultaneous or those along a predetermined timeline, are addressed. The reader is referred to other portions of this volume to investigate some of the complications raised by these attack scenarios.

## 2.1 Conventional Physical Attacks

Attacks can be direct or indirect. Protection and prevention against terrorist acts is a problem not unlike the "inverse problem" in conventional deterministic modeling. Given a result, some (perhaps very large) set of paths exist to go from the initial condition to the observed result (each path representing one determined path). The security problem faced, of course, is that all paths cannot be interdicted, so judgments must be made regarding the various paths and actions taken to disrupt a most likely path.

Evaluation of multiple paths is not unlike the approach taken by law enforcement and counterterrorism by "thinking like the criminal/terrorist", and defining what set of things must be brought together for the act to be realized. It becomes a problem in inductive logic whereby the system of reasoning extends deductive logic to less-than-certain inferences [6]. In this example, a sequence of events leading to the result are believed to support the conclusion, but do not ensure that this conclusion is right. Unfortunately, inductive approaches can miss the unanticipated event [7], sometimes with horrific consequences such as 9/11.

The predictability of such types of direct physical attacks, however, is hampered not only by the number of possible attack paths needed to be considered for interdiction but also by the ingenuity of the adversary. Adversarial ingenuity is demonstrated frequently by their design, and use of less well-known weapons (i.e. peroxide-based explosives, the root cause of our inability to take containers of liquids on airplanes, home-built armor-piercing explosively formed projectiles (EFPs) used in Iraq, and ability to quickly adapt to countermeasures) presents an enormous challenge to the nation.

Subsequent to 9/11, a federal directive was promulgated throughout the rail and chemical sectors to cease shipments of chlorine gas fearing that a rail car might be attacked in a populous area killing or injuring many. A few days later, the directive was lifted

because high-density population areas needed chlorine to purify drinking water supplies. Within about 90 days of the attack on the Pentagon, the Blue Plains Wastewater Treatment Plant in Southwest Washington, DC, converted its process so that large tanks of chlorine and sulfur dioxide (an equally hazardous gas) would be essentially eliminated from the plant site and switched to an alternative technology. These examples illuminate preventive actions against what many call indirect attacks because terrorists could use existing infrastructure against the nation. During its first 4 years, the DHS spent significant resources identifying terrorist-created chemical releases as an indirect attack mode with the result that a new organization was created to define and ensure security standards across the chemical industry.

The existence of standards across a sector, however, does not necessarily correlate to security. For instance, chemical contamination of a foodstuff could cause as much damage and panic as the release of a noxious plume from some manufacturing plant. Equally insidious, counterfeit materials (parts or substances) used in sensitive applications can also constitute threats to people, or in some cases, economic well being. In an open society, tracking materials—and people—from origin to endpoint creates a sociological problem, which the nation continues to struggle with.

## 2.2 Nonconventional Physical Attacks

The attacks described above are classed as being conventional in nature because the means of executing them are reasonably straightforward. Similarly, the tactics used and results obtained from these attacks are conventional. There are, however, less conventional types of attacks of importance to the nation. At the forefront, of course, is that group of attacks termed *weapons of mass destruction/effect* (WMD/E). Those attacks are covered elsewhere in this volume and are not discussed here.

Another unconventional, but not unknown, attack is that class considered denial of use attacks. These scenarios encompass a myriad of agents dispersed into, on, or around infrastructure important to continuity of operations. The anthrax attacks in 2001 using the US Postal Service's Trenton Processing and Distribution Center as a delivery system is one example of such denial of use attack. Unfortunately, in the case of the 2001 attacks, 5 of the 22 citizens exposed to the spores succumbed. Subsequently, then-Senator Tom Daschle's office suite in the Hart Building on Capitol Hill was found to have anthrax contamination causing building evacuation and shutdown of the government mail service until decontamination efforts could clean the premises for occupancy. The Trenton postal facility was not reopened until March 15, 2005, some three and a half years after the contamination was discovered. Had this attack been to a "critical" commercial facility (i.e. one that is essential to the nation and without substitute), it is questionable whether the corporate enterprise or the country could have survived such a lapse in service. Another scenario that could result in denial of use is that of a radiological dispersion device (RDD). In this scenario, radionuclides from any number of sources could be dispersed using explosive or aerosol means and could result in denial of use for years, even decades depending on the material used.

Biological and RDD attacks are not necessarily aimed at creating many casualties. Rather the economic hardship and/or the fear created within the population that works in or near the facility thereby preventing the facility from performing its necessary function may be the true goal. Although such attacks of a neighborhood retail facility may cause no great harm to the nation or inconvenience to the population, there are many facilities

that if shut down for extended periods of time can seriously impact the national economy (Wall Street) or national security (single-source for critical military component).

Two other nonconventional attack types being faced by the nation include virtual (cyber) attacks and attacks being staged by hostile nation-states. The former of these is dealt with extensively elsewhere in this volume, and the latter lies outside the scope of the volume. Neither is discussed here.

Other nonconventional attacks that seem farfetched, but nonetheless could wreak havoc throughout America also exist. They are called *attacks* here for the purpose of continuity, but they actually represent broad challenges as well. The first of these types constitutes a form of economic attack by currency, trade, or resource manipulation. These attacks could emerge from nation-states, but could also come from other, even transnational groups bent on controlling some particular part of the commercial or financial market. One example that happened, but was notably nonnefarious, was the over $300b investment in high-profile commercial American real estate by the Japanese in the 1980s. In the early 1990s, market forces reduced the value of these investments by as much as 50% [8]. While this example is one of arguably benign global investing, the question posed becomes "What if intentions are nefarious?"

One such example is clearly illustrated by the 1960 formation of the Organizations of Exporting Petroleum Countries (OPEC) and subsequent withholding of oil exports to the United States in the early 1970s and 1980s. Although academicians continue to argue over the root causes of the embargos, the net result was an energy crisis in the United States that, at least in part, was driven by a political stance taken to punish the alleged wrongdoer. Other technical and geopolitical events eventually nullified the problem, but as a nation, the problem has still not gone away; we are more dependent on foreign oil imports (by over a factor of two) than we were when the embargoes were first exercised 30 years ago. How can the United States protect itself from such economic attacks? "Energy Independence", while making a catchy bumper sticker, is as demonstrably lacking in substance as "Financial Independence". The effects of globalization are rooted deep in American society, and our interdependencies on both external supplies of energy and money create a formidable challenge in a world of highly heterogeneous cultures.

Another nonconventional attack that lays well beyond media headlines constitutes an equally formidable challenge. Simply put, it is the attack, perhaps self-inflicted, that the nation faces with respect to its intellectual infrastructure. Most readers can recall at least one article within the last year chiding "education in this country" for poor scores in science and math, relative to the rest of the world. It is similarly recognized that American colleges and universities are "educating the world". The implications of failing elementary and secondary education for its citizens and excellence at the college level attracting students from across the globe are not straightforward. However, two examples might be useful in stimulating research into how the nation can address this challenge.

Corporate recruiters are always looking for the "best and brightest" regardless of the particular type of expertise they represent. For jobs within the United States, significant resources must be spent if the desired employee is not a US citizen. For jobs within the government that require a security clearance, US citizenship is even more important. Looking at technical fields, the percentage of US graduate students who are US citizens has been decreasing for decades (except for a brief reversal following 9/11 [9]). A recent article [10] states that:

> "International students, especially at the graduate level, are considered an important brainpower infusion to the United States. In certain fields like engineering and physical sciences, foreign students account for more than 40 percent of total students at the graduate level, according to CGS (*Council of Graduate Studies*).
>
> 'There is not a strong domestic pipeline in those disciplines,' said Catharine Stimpson, dean of New York University's Graduate School of Arts and Sciences. 'The U.S. has a strong dependence on international talents.'"

The implications of US dependence on offshore intellectual infrastructure are discussed at length by Canton [11]. As the scientific and technical challenges to homeland security evolve, finding qualified personnel will represent sociological and educational challenges as difficult as anything in engineering or the sciences. Like the national physical infrastructure, our intellectual infrastructure is sufficiently intertwined with that of other nations that makes unilateral solutions (intellectual independence) impossible. From a threat, perspective, denial of access to information or knowledge can be an effective attack not dissimilar to denial of use.

## 3 ORIGIN OF THREATS

Within the scope of an overview article, exhaustive enumeration of all of the various sources of threats that play a role in homeland security would be redundant to other articles in this volume, and could go on for volumes in themselves. For greatest simplicity, four general types of threat considered here are international terrorism, domestic terrorism and hate groups, natural hazards, and catastrophic accidents. Three are anthropogenic, hence to some degree they can be defended or prevented, but the results of all four must be considered in the context of response and recovery.

### 3.1 International Terrorists

According to the Memorial Institute for the Prevention of Terrorism, there are over 1200 international terrorist groups [12], all of whom have agendas at odds with normal political intercourse. Although national attention has highlighted Al-Qaeda since 9/11, other groups are also "on the radar". Specific motivational differences between the groups are not of importance to this article. Rather, it is important to understand what kinds of attacks against what kinds of infrastructures may be posed by the transnational terrorists. As mentioned earlier, intent and capability are two venerable types of information needed to judge how realistic a threat from a particular group may be. Also mentioned earlier is the newer concept of authority, at least for radical Muslim jihadists. For more insight into this aspect, the reader is referred to the work of Williams cited below. It may be that his concept could be extended to other groups as well. Simply put, the execution of any particular terrorist event depends on someone effectively saying "Go". Williams shows the role played by fatwas, legal and religious justifications, and speeches given by radical Muslims intent on causing harm. However illogical, that role—choice of target type, what is and is not acceptable behavior during the execution of the attack, and the weapons used (each providing important insights to potential defenders)—can also be

seen in historical criminal behaviors (i.e. anecdotal prohibition of violence on family members by the Mafia). Getting this kind of insight is an immense challenge for the nation if only because these reasonings and rationalizations are dynamic even within the groups themselves. Complexity is not a reason to avoid trying to understand these drivers, but developing an institutional understanding of another culture can take decades.

### 3.2 Domestic Terrorists and Hate Groups

The April 19, 1995, bombing of the Alfred P. Murrah Federal Building in Oklahoma City by disaffected military veterans brought national attention to a threat nexus that had largely been ignored by the public since publicity of the Symbionese Liberation Army, the Black Panthers, and others in the 1970s. Timothy McVeigh and Terry Nichols' attack graphically demonstrated how ill-prepared the country was for dealing with violent acts perpetrated by its own internal terrorists.

Organized domestic terrorist groups such as the Aryan Nation, the Klu Klux Klan, and the New Order reside in the twilight between a "conventional" terrorist group and a "conventional" hate group. The line separating the two may be dim. However, radicalization by Muslim jihadists and others in homeland prisons is a growing and morphing threat, which is not necessarily racially based. Without dwelling on fine distinctions between domestic terror and hate groups, the result of their actions can still terrorize segments of our society or citizens within a particular region. All this compounds the problem of operating cells of transnational groups (e.g. Al-Qaeda, Al-Fuqra, and Aum Shinrikyo) that may form alliances of convenience with domestic groups, including criminal enterprises, possibly with or without their explicit knowledge. Groups such as the Animal Liberation Front and Earth Liberation Front often raise parochial headlines, but are not broadly thought of as national threats.

### 3.3 Naturally Occurring Challenges

In the simplest terms, natural hazards can be classed into those that are to some extent predictable allowing the population to take some preparatory measures, and those that "come out of the blue". The former would include floods, hurricanes, tornados, some biological events, and wildfires (initiated by lightning strikes). The latter would consist of earthquakes, some biological events, and some volcanic eruptions. Man has been living with and fearing the vicissitudes of Mother Nature for millennia. But, only recently has technology developed to the extent that some of these threats can be prevented (in rare cases) or engineered around to reduce consequences. Medicinal prophylaxis is arguably the most illustrious example of man's ability to prevent a threat from causing harm to health. Certain structures such as levees and dams can mitigate catastrophic impacts but do not prevent threats to them: often making them critical facilities. Similarly, preparations for hurricanes and tornadoes may mitigate impacts, as does buildings designed for earthquakes; but such natural hazards are unique (no two will be exactly alike in consequence or response) and will occur as long as natural processes continue. As demonstrated too well, the national response to Hurricane Katrina was reminiscent of the response to the tragedy of 9/11.

Interruptions to the global integration of economies [13] caused by natural disasters and the continuing interweaving of physical and commercial infrastructure (i.e. chemical feedstocks from Mexico and oil and gas energy from Canada), not only represent serious

challenges to homeland security professionals, but also pose a great scientific challenge. Clearly, knowledge-based actions have been shown to have saved lives through weather modeling. Scientific efforts and innumerable data collection efforts have saved lives by evacuating some remote Oregon areas prior to the eruption of Mt St Helens. However, such apparently academic pursuits are rarely seen (or funded) as homeland security efforts; yet the products of these research fields provide much information in the effort to prevent serious consequences of these threats.

### 3.4 Catastrophic Accidents

In ways similar to natural hazards, catastrophic accidents create impacts that might be indistinguishable from terrorist attacks. Such accidents could include the rupture of rail tank cars filled with toxic chemicals, the core meltdown at a nuclear power plant, a space shuttle crashing, equipment wear/burn-out with catastrophic failure, and so on. Unfortunately, all of these examples did (or nearly did) happen in recent history, but fortunately none occurred in large US population centers. For all intents and purposes, the possibility of the "event that never happened" spawned the field of probabilistic risk assessment (PRA) back in the 1970s when the government and private industry had to develop ways to plan for the risk of such events. The pursuit of PRA and fault-tree analyses by statisticians and engineers over the past three decades has helped reduce the likelihood of such catastrophic events by creating engineering and public safety standards that have prevented Bhopal- or Chernobyl-type events here. These disciplines continue to offer insights into the nation's homeland security.

## 4 PREVENTION AND PROTECTION

In J. Cummings' article in this volume, he refers to Merriam-Webster's online dictionary for some important definitions [14]. Prevention is defined in several, interlinked ways. Simply put, the DHS seeks to ensure that attacks on the homeland and its people do not occur. Often this is thought to be primarily a function of the intelligence and counter-errorism agencies; those aspects are covered elsewhere in the Handbook. Protection is essentially defined as shielding from an event or attack. Taking these definitions and the threat spectrum discussed above as the context for the technical challenges the nation faces, four activities evolve that provide focus for security professionals, namely; detect the threat, deter the attack, defend against its outcomes, and/or devalue the target. Much is written elsewhere in the Handbook regarding the first three of these, but the last one, devaluing the target (for the attacker) brings into play resiliency and redundancy.

Redundancy is an important and useful way to devalue any given target. However, redundancy is largely an asset-by-asset approach that provides protection from a single-point-of-failure situation. While this approach has been taken by some parts of the private sector, it is not physically or economically feasible to create redundancy for many of the nation's most important infrastructure assets. A large hydroelectric dam is where it is in part because of unique geography. Refineries are extremely expensive and, considering issues as divergent as pipeline connectivity and environmental regulation, cannot easily be duplicated.

Resiliency is a concept that applies to individual assets and to systems or networks of assets. Simply put, resiliency is a design property that allows the asset, network, or

system to "fail gracefully", or in such a way as to allow consequences of the failure to be minimized. Consider the automobile tire that you can drive on even after it is ruptured. Self-healing materials and networks are under intense study now, and will continue to play a growing role in homeland security. Greater sophistication in modeling and simulation is also giving rise to designing ways such that systems may actually heal themselves or fail gracefully. However, resiliency must become even broader. We recognize that the interdependencies of the nation's infrastructure are far-reaching and mostly poorly understood. Work in this arena is addressed in the Handbook section titled System and Sector Interdependencies, and the reader is referred to that section for more details.

## 5 CHALLENGES TO DHS

Some challenges to the DHS and the nation are scattered within the context of the threat spectrum. Many of these challenges are obvious and straightforward, such as sensors for detecting harmful substances or organisms, materials that can provide more and better protection by strengthening facilities while keeping costs reasonable, and software tools to frustrate cyber attacks before they can damage our physical and/or economic infrastructure. Technical challenges related to catastrophic accidents mimic those for natural hazard and terrorism attacks when it comes to physical infrastructure protection. Conventional attacks, by terrorists, nature, or accidents, all require advances in a variety of scientific and engineering endeavors. Less conventional, however, are the security considerations and approaches that will be needed to protect new technologies as they are deployed throughout our infrastructure. There are also two other challenges that the DHS faces as an institution that represents and works for the nation.

### 5.1 Defining the Unacceptable

In some ways, this problem is reminiscent of the problem faced by the Environmental Protection Agency since its inception "How clean is clean?" Within an attack context, it becomes "How bad (number killed or hurt, dollars lost, people traumatized, etc.) is bad?", and "What constitutes acceptable losses?" As painful as these questions are to contemplate, they must be considered.

Since its inception, the DHS has provided billions of dollars to state, local, tribal, and territorial governments in the form of grants to make the nation safer from terrorism attacks. Both 9/11 and Hurricane Katrina brought public attention to the simple fact that very large-scale events are a national issue requiring a national response. But at what price and for how long? There is no politically correct answer to the question of how many casualties are acceptable, but unfocused funding and unnecessary preventative processes and material are equally unacceptable.

The DHS Secretary, Michael Chertoff stated that "risk management must guide our decision making as we examine how we can best organize to prevent, respond and recover from an attack". To allocate resources, money, material, or personnel, the DHS must prioritize. However, prioritization, like triage, requires that choices be made regardless of how uncomfortable they may be. For many reasons, classical statistics cannot help in the prediction of terrorist attacks although they have proven useful, at least to the insurance industry, to help planning for natural events. There remains, however, the paradox of quantitative (defensible but often technically intricate) versus qualitative (what seems

right, albeit possibly quite subjective) solutions within the political environment where there will be winners and losers for federal resources. Making those choices is a significant challenge for the DHS.

### 5.2 Communicating to the Public

In today's era of 24/7 global news, Edward R. Murrow once said "The newest computer can merely compound, at speed, the oldest problem in the relations between human beings, and in the end the communicator will be confronted with the old problem, of what to say and how to say it." This concept is particularly pertinent to homeland security in general. In simple terms, most people ask two questions: "How likely is something bad to happen?" and "If that bad thing happens, how bad will it be?"

Insight into how the government and private industry has attempted to communicate answers to these questions in the past is, sometimes humorously, documented by Lewis [15]. Most people have great difficulty in fathoming just how likely any number of bad things really are. Schneier said [16], "I think terrorist attacks are much harder than most of us think. It is harder to find willing recruits than we think. It is harder to coordinate plans. It is harder to execute those plans. It is easy to make mistakes. Terrorism has always been rare, and for all we have heard about 9/11 changing the world, it is still rare." Even a casual review of terrorism incidents as compared to violent crimes proves him out. Communicating the risk of both man-made and natural catastrophic events remains a major challenge to the DHS and the nation as a whole.

## 6 RESEARCH NEEDS

The complexities of our nation's infrastructure belie simple listings of technological needs. The same complexities require bringing together very complicated components, systems, and results. Such complications and the challenges they bring forms most of this Handbook. For this author's part, however, there are three major categories of research needs that will help move us closer to a more secure nation.

The first of these includes more sophisticated modeling and simulation (M&S) of extremely rare events, terrorist systems, and networks, and outcomes from conventional and unconventional attack modes. Thanks to massive increases in computational capabilities, M&S can now be done for problems that only a decade ago were intractable. However, M&S is not reality, nor will it ever replace all of the possibilities that reality represents. That said, M&S does provide important tools into understanding phenomena (physical, virtual, and even psychological) that otherwise could simply not be gathered.

For instance, today's blast models are based on materials with energy equivalent to trinitrotoluene (TNT). The damage done to structures is modeled with a characteristic pressure wave caused by a certain amount of that explosive located at a specified distance from the modeled structure. However, despite the number of plots accomplished and foiled that utilized "bathtub" or peroxide-based explosives, little is known about their explosive characteristics against a variety of target types. It is infeasible to run experiments on all possible combinations of conventional and other explosives and targets. Therefore, more work is needed to better define envelopes of behaviors enabling better-informed protective decisions to be made. Similar statements can be made regarding impact of natural hazards on man-made structures. Some level of experimentation has

been done, but many of the historical impacts do not translate directly to today's infrastructure and their interdependencies. In this author's opinion, the M&S of the nation's infrastructure interdependencies is the single greatest and perhaps most difficult M&S infrastructure security challenge facing the nation. It is a problem of such complexity and across so many orders of magnitude that it will take decades to master.

Knowledge management is a second category of research needs. Information overload has become a major challenge in today's technological world. While new sensors and other data are collected (see the Sensing and Detection section of this volume), how we translate the data first into information and then into knowledge are pushing security professionals (and their IT systems) to their limits. Managing all of that in a retrievable way has become a significant and expensive challenge. Within the last decade, IT architectures began evolving from strictly hierarchical to more relational ones. More work needs to be done in this and associated areas in the pursuit of data, information, and knowledge. It is only when easily accessible broad knowledge across many disciplines is fused with judgment that decision makers can plot the best path for their enterprise or the nation.

More research in the social and psychological sciences constitutes the third area of great need for the DHS and the nation. There are two over-arching drivers for these areas to be addressed. First, great good can be accomplished by extensive and excellent scientific advances in all sorts of technologies. While supporting science at large, how these advances can be used to support the making of federal policy, in fact, provides the true return on investment for the government. Second, inasmuch as the government's role is to establish and execute the political will of the nation through policy, gathering data on what the nation wants, needs, and how willing they are to accept it is a supremely difficult task. In some measure, the challenge of communication feeds this research need as well, because policy is fed by communication, which in turn needs to be communicated back to the nation. Within infrastructure protection, a clear understanding of the risks run, and therefore the protection and prevention activities required to address that risk, must be communicated to the consumer, for in the end, it is the consumer that will have to live with the decisions driven by those risks, or less desirably, the perception of those risks. Alfred Hitchcock, who knew something about creating terror in people's minds stated: "There is no terror in a bang, only in the anticipation of it." By being psychologically and socially prepared for the bang, regardless of it being man-made or natural, the impact of the event can be reduced.

## 7 CONCLUSIONS

The extent of this Handbook's Table of Contents illustrates that homeland security is as complex as life itself. Invigorated by the terror attacks of 9/11, homeland security has expanded to include any and all catastrophic events. Total protection from and prevention of catastrophes is not achievable. However, their impacts to the nation can be partially mitigated by technology, partially by barriers (including regulation and legislation), and to a significant degree by knowing and understanding the risk, which includes threat, the knowledge and understanding of which must be objective, and not be used for fear mongering. In hindsight, the 9/11 attacks are understandable, perhaps even predictable. The perpetrator's ability to execute an attack must be seen as the target of protection and prevention technology. It is within our nation's ability to impact the execution of

an event, be it from terrorists or man-made mistakes, and by so doing prevention and protection will make their contribution to homeland security.

## REFERENCES


1. Williams, J. F. (2007). Authority and the role of perceived religious authorities under Islamic Law in terrorist operations. *Proceedings Federalist Society—Georgia State University, Atlanta*.
2. Williams, J. F. (2007). Al-Qaida strategic threats to the international energy infrastructure: authority as an integral component of threat assessment. *Proceedings Carlton University—Ottawa Center for Infrastructure Protection, Ottawa Canada*.
3. National Consortium for the Study of Terrorism and Responses to Terrorism (START). http://www.start.umd.edu/, 2008.
4. Memorial Institute for the Prevention of Terrorism. http://www.mipt.org/IncidentTacticModule.jsp, 2007.
5. National Consortium for the Study of Terrorism and Responses to Terrorism. http://209.232.239.37/gtd1/charts/weapon_type_pie.gif andhttp://209.232.239.37/gtd2/charts/weapon_type.gif, 2008.
6. *Stanford Encyclopedia of Philosophy*, http://plato.stanford.edu/entries/logic-inductive/, 2008.
7. Taleb, M. N. (2007). *The Black Swan—The Impact of the Highly Improbable*. Random House, New York, p. 366.
8. Pristin, T. (2005). Commercial real estate; echoes of the 80's: Japanese return to U.S. market. *The New York Times* http://www.nytimes.com/2005/01/26/business/26prop.html.
9. Kujawa, A. (2005). *Foreign Student Enrollment at U.S. Graduate Schools up in 2005*, http://www.america.gov/st/washfile-english/2005/November/20051107160749aawajuk0.8633234.html.
10. Du, W. (2007). *Foreign Student Enrollment Rebounds in U.S.; MSNBC*, http://www.msnbc.msn.com/id/20393318/.
11. Canton, J. (2006). *The Extreme Future —The Top Trends That Will Reshape the World in the Next 20 Years*. Plume, New York, p. 371.
12. Memorial Institute for the Prevention of Terrorism. http://209.232.239.37/gtd2/browse.aspx?what=perpetrator, 2008.
13. Friedman, T. L. (2005). *The World is Flat*. Farrar, Straus, and Giroux, New York, p. 660.
14. Merriam-Webster online dictionary. http://www.merriam-webster.com/, 2008.
15. Lewis, H. W. (1990). *Technological Risk*. WW Norton & Company, New York, p. 353.
16. Schneier, B. (2006). *The Scariest Terror Threat of All*, http://wired.com/politics/security/commentary/securitymatters/2006/06/71152.


## FURTHER READING


Chalk, P., Hoffman, B., Reville, R., and Kasupski, A.-B. (2005). *Trends in Terrorism*. RAND Corporation, Santa Monica, CA, p. 75.

Garcia, M. L. (2006). *Vulnerability Assessment of Physical Protection Systems*. Elsivier, Amsterdam, p. 382.

Haimes, Y. Y. (2004). *Risk Modeling, Assessment, and Management*. John Wiley & Sons, New York, p. 837.

Jenkins, B. J., Crenshaw, M., Schmid, A. P., Weinberg, L., Ganor, B., Gorriti, G., Gunartna, R., and Ellis, J. O., Eds. (2007). *Terrorism: What's Coming—The Mutating Threat*. Memorial Institute for the Prevention of Terrorism, Oklahoma. website: http://www.terrorisminfo.mipt.org/pdf/Terrorism-Whats-Coming-The-Mutating-Threat.pdf9.

Kline, M. (1967). *Mathematics for the Nonmathematician*. Dover Publications, New York, p. 641.

Mueller, J. (2006). *Overblown*. Free Press, New York, p. 259.

Post, J. M. (2005). *The Al-Qaeda Training Manual; USAF Counterproliferation Center, Maxwell Air Force Base*, U.S. Government Printing Office 2005-536-843, p. 175.

*Presidential Decision Directive 63: Protecting America's Critical Infrastructures*. The White House, May 28, 1998, http://www.fas.org/irp/offdocs/pdd-63.htm.

Ridgeway, J. (2004). *It's All for Sale*. Duke University Press, Durham & London, p. 250.

Roberts, P. (2005). *The End of Oil*. Houghton Mifflin Company, New York, p. 399.

Sauter, M. A., and Carafano, J. J. (2005). *Homeland Security*. McGraw-Hill, New York, p. 483.

Schneier, B. (2006). *Beyond Fear*. Springer, New York, p. 295.

*Securing Our Homeland*. Department of Homeland Security Strategic Plan, Washington, DC, (http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf).

# TERRORIST ORGANIZATIONS AND MODELING TRENDS

IRMAK RENDA-TANALI

*University of Maryland University College, Adelphi, Maryland*

CHRISTOPHER D. HEKIMIAN

*DXDT Engineering and Research, LLC, Hagerstown, Maryland*

## 1 INTRODUCTION

The US Joint Tactics, Techniques and Procedures (JTTP) for Antiterrorism, Joint Publication 3-07.2 as cited in [1] states: The terrorist organization's structure, membership, resources, and security determine its capabilities and reach". Any method of analysis and understanding that can be directed against the broad threat posed by terrorist organizations (TOs) can contribute to mitigation strategies. Moreover, since TO activities are often covert, and government secrets regarding intelligence pertaining to TOs are closely guarded, knowledge, understanding, and analytical tools may be the only assets that analysts have to direct toward terrorism threat mitigation. Understanding the structures

and modes of operation of terrorist groups is a key enabler in the assessment and mitigation of the terrorism threat. Organizational structures of terrorist groups that may appear complex during initial assessments may be more understandable when laid out in systematically modeled formats. This article focuses on existing and ongoing efforts related to terrorist data analysis and modeling aspects that deal with terror risk mitigation.

## 2 SCIENTIFIC OVERVIEW

The research in support of understanding the construct and operation of TOs can be categorized into (i) studies that focus on definition/conceptual issues; (ii) case studies of particular regions, countries, movements, and events; (iii) counterterrorism and crisis management; (iv) terrorism data analysis and modeling, and other related topics. This article deals with terrorism data analysis and modeling. Discussion of an overview of the seminal thinkers and works on terrorism studies were provided by Hopple in reference 2.

Although there is no universally agreed upon definition of *terrorism*, various definitions exist and have been adopted by organizations worldwide. Therefore it is helpful to disclose the definition up front with the disclaimer that other definitions may or may not be equally valid for the discussion at hand. Key researches on the current bases for classification and categorization of TOs have been summarized in unclassified military documents that are referenced in this article. Other sources on the topic include US Congressional reports and other government and academic reports. The RAND organization provides a large amount of recent research on the operation and function of TOs and has been cited multiple times in this article. A large amount of current research pertaining to the organizational structures of TOs and how those structures tend to affect operations and vulnerabilities are available in military and academic reports and journal articles by Fatur (2005), Shapiro (2005), and Hoffman (2004). There are a wide range of organization modeling methods and scholarly research, including case studies, dissertations, and theses, and articles have been cited in each section of this article. The work of Barry Silverman of University of Pennsylvania, in modeling terrorist behavior, and of Kathleen Carley of Carnegie-Mellon, in network organization modeling, is at the forefront of the advancement of these methods and their application. The reader is encouraged to obtain these documents to find more detailed information on those topics that are beyond the scope of this article.

## 3 TERRORIST ORGANIZATIONS

### 3.1 Terrorism Definitions

The definition of what constitutes “terror”, “terrorism”, and hence a “terrorist” or “terrorist organization”, is a matter of significant debate. Some embrace the position that one man’s terrorist is another man’s freedom fighter. In fact, there is a plurality of reasonable definitions suitable to provide context and focus to discussions on homeland security. For example, a study conducted by the Federal Research Service of the United States Library of Congress [3] presents the following definition for terrorism:

> [T]he calculated use of unexpected, shocking and unlawful violence against noncombatants . . . and other symbolic targets perpetrated by a clandestine member(s) of a sub-national group . . . for the psychological purpose of publicizing a political or religious cause and/or intimidating or coercing a government(s) or civilian population into accepting demands on behalf of the cause." (Reference 3, p. 12)

Ganor [4] further restricts the definition given above by stipulating that the targets must be civilian and attacked to attain political aims.

Given a definition of terrorism, a terrorist group can be defined as an organizational structure that employs terrorism as a means to further its goals. Terrorist groups can be defined as organizations based on the following criteria set forth by Crenshaw (Reference 5, p. 466):

- The group has a defined structure and processes by which collective decisions are made.
- Members of the organization occupy roles that are functionally differentiated.
- There are recognized leaders in positions of formal authority.
- The organization has collective goals which it pursues as a unit, with collective responsibility for its actions.

A report by the National War College entitled *Combating Terrorism in a Globalized World* [6], states:

> "Collectively, terrorist organizations pose the single greatest threat to American and international peace and prosperity" (Reference 6, p xix). Through links with other TOs, organized crime, drug traffickers, and state and corporate sponsors, TOs constitute a kind of *de facto* nation, complete with the ability to conduct war [6].

The potential targets of terrorist attacks can be summarized as

- the direct victims of the attack;
- members of society who are threatened by the prospect of being victims of similar attacks;
- the wider audience of the act who are intended to receive the message that the TO is a force to be reckoned with;
- government entities whose hand the terrorists are trying to force.

## 4 TERRORIST ORGANIZATION CONCEPTS

In a broad sense, TOs can be visualized in terms of a set of concentric rings. In the center of the rings is the leadership of the organization. The area just outside the leadership area represents the operations cells, where the responsibility for tactical planning and execution of operations resides. The area outside the operations ring represents the network of those sympathetic to the organization's cause. The sympathizers provide financial support to the organization either directly or indirectly [7].

The following sections describe key concepts associated with TOs, including TO members, TO funding sources, organizational learning for TOs, and TO functions and capabilities.

### 4.1 TO Members

Members of TOs may typically fall into one of the four general classifications [8]:

1. Leaders, providing direction and policy.
2. Cadres, planning and conducting operations and maintaining logistics, intelligence operations, and communications.
3. Active supporters, engaging in political and fund-raising activities.
4. Passive supporters, sympathizers based on shared end goals or through fear. "[P]assive supporters can be useful for political activities, fund-raising or through unwitting or coerced assistance in intelligence gathering or other nonviolent activities" (Reference 8, p. 3–2).

Members of TOs may progress upward through the power structure by earning the trust of leadership over time or through other factors such as familial or tribal relationships. Trust is likely to be earned through participation in risky operations. After a member has proven to be dedicated to the cause and capable, they are more likely to be rewarded with a leadership role. Typically, leaders are less likely to be involved directly with terrorist tactical operations [9].

### 4.2 TO Funding

TOs typically rely on any combination of six basic sources of funding [9]:

1. direct contributions from private individuals;
2. donations from charitable institutions;
3. government sponsors;
4. legitimate businesses;
5. contributions from members;
6. profits from criminal enterprises (robbery, kidnapping, hijacking, extortion, trafficking, gambling, black market, etc.).

A TO may be state supported. Sometimes the support exists due to intimidation or extortion. Some governments may support the terrorist's cause ideologically, but disagree with some of the methods employed by the TO. Most financial support for TOs originates from nongovernment sources [10].

### 4.3 Organizational Learning in TOs

A study of organizational learning within terrorist groups sets forth that in order for terrorist groups to endure, they must adapt to conditions around them (e.g. threats, technology, and societal factors) and within them (e.g. compromise of key organizational elements) [11]. The greater the ability of a TO to learn, the more effective it can be in choosing targets, identifying vulnerabilities for the maximum desired impact of attacks, and avoiding and confounding counterterrorism efforts [11]. Learning within the TO, and the ability to convey knowledge and information in a timely manner, affects the ability of the organization to adapt and survive [11]. The type of organizational structure of a TO and its communication resources will impact the ability of a TO to learn,

share knowledge, and adapt. According to Hopmeier [12], this is evolution, which TOs do much better than governments or counterterror organizations, because their response time is much smaller and their "bureaucratic inertia" is less due to the smaller size.

### 4.4 TO Size

TOs can be of various degrees of maturity and capability. However, the nature of terrorism is such that a large organization is not required to complete a large scale attack that is successful from the terrorist's perspective (e.g. the bombing of the Alfred E. Murrah federal building in Oklahoma City) [8]. TOs are often interconnected such that mutual aid is provided among them. Examples of such aid might be the supply of weapons, ammunition, or training; referral or vetting of personnel; sharing of safe havens; and of course, the exchange of intelligence. In effect, even a small TO may be able to make use of information and resources that they otherwise would not have access to without the support of a greater terrorist community [6].

Emergent terrorist groups can act as proxy or under guidance from larger organizations with more experience and resources. Smaller groups can be absorbed by larger organizations. Several small, hierarchical organizations might coalesce into a larger networked one. Conversely, a smaller organization might splinter off from a larger one. The splintering may occur due to strategic reasons or over disagreements over transitions of power. Each method of formation carries with it implications with respect to the organizational structure, experience level, and capabilities of the resulting organizations [8].

### 4.5 TO Functions

A 2005 RAND organization report says:

> "In order to act effectively, a TO must be able to organize people and resources, gather information about its environment and adversaries, shape a strategic direction for actions of its members, and choose tactics, techniques and procedures for achieving strategic ends" (Reference 11, p. 95).

Generally, TOs must address certain key functions, including [11]

- training
- logistics
- communications
- fund-raising
- collaboration/interface with other TOs or sponsors
- intelligence
- operational security
- tactical operations
- recruiting
- indoctrination.

Large organizations are also likely to have medical services that are organic to their structure. Well-funded organizations may participate in social services within their regions

of influence. Distributing food, providing jobs, and organizing educational and youth activities are all ways of developing and strengthening ties within the communities upon which they rely for cover, support, and new recruits [11].

### 4.6 TO Categories and Classifications

The military guide to terrorism in the twenty-first century [8] categorizes TOs as follows:

- structure—including hierarchical and networked (such as chain, hub, and flat networks);
- government affiliation—including nonstate supported, state supported, and state directed (operating as an agent of a government);
- motivation—separatist, ethnocentric, nationalistic, revolutionary;
- ideology—including political (for example, right wing, left wing, and anarchist); religious; social (for example, animal rights, abortion, environment, and civil rights);
- international scope—for example, domestic; international (i.e. regional and routinely operational in multiple countries within a specific region); transnational (i.e. transcontinental or global or routinely operational in multiple countries and in multiple regions).

A US Congressional Research Report from 2004 [13] identifies even more characteristics associated with [foreign] TOs. These additional characteristics are included in the following list:

- goals and objectives
- favored tactics
- primary areas of operation
- links with other groups
- business associations
- composition of the organization membership
- nonterror activities.

To understand the motivations and actions of TOs more thoroughly, some researchers have found it useful to categorize them as either *political* or *fanatic* [7]. *Political* TOs tend to use terrorism as a means to achieve political goals. On the other hand, *fanatic* groups tend to be more interested in violence as an end in itself. These groups may have lost sight of their political goals or may be locked in a cycle of revenge, or may have more criminal interests [7].

Most TOs are politically or religiously motivated such that they can benefit from the association with some legitimate or otherwise popular cause [6]. *US Department of State list of Designated Foreign Terrorist Organizations* includes religious as well as various national separatist organizations and ideologically inspired organizations. TOs focusing on racial separatism, opposition to abortion, animal rights, and environmental issues are not uncommon in many of the westernized nations [14].

## 4.7 Organizational Structures of TOs

The two general categories of structure for TOs are networked and hierarchical. Terrorist groups may be structured as a combination of the two types.

Hierarchical organizations are characterized by well-defined vertical command and control structure. The lower level functional elements of hierarchical organizations are usually specialized (e.g. logistics, operations, and intelligence) as opposed to being stand-alone elements whose capabilities span those same specialties. The latter type is more characteristic of networked organizations [8].

Hierarchical organizational structures are characterized by leadership, that is, centralized in terms of authority. Although the centralized leadership structure provides more organizational control over doctrine, motivation, and operations, these structures are usually more dependent on communication channels, structured logistics, and disciplined membership. These dependencies represent additional vulnerability to successful penetration or counterterror operations [7].

A terrorist network that is of distributed (decentralized) structure tends to be more capable of operation when key leadership is eliminated [15]. However, since terrorist activities are often covert and because modern information and communication systems are susceptible to being intercepted and analyzed, significant challenges to communications and the transfer of funds exist throughout these kinds of TOs. Owing to inexperience, fear of compromise or of leaving an evidence trail, record keeping is likely to be done sparingly or not at all in some cases, adding to the uncertainty and unaccountability of actions within the networked organization [9].

TOs that are bound by broader beliefs, such as religious, environmental, or moral, do not require the type of coordination that politically motivated organizations do. Consequently, networked structures of more or less self-sufficient operational cells distributed geographically are suitable to conduct their operations over a wide area and in cooperation with other like-minded organizations. The leadership of such organizations or of a particular "movement" can set broad goals, and networked TOs can independently choose targets and act against them in a manner that they see fit. The whole organization will expect to benefit in terms of influence and publicity and the attainment of its collective goals [8]. If a network becomes excessively distributed, it tends to lose much of its organizational aspects and instead becomes more of an idea or concept [16].

A correlation has been identified between the general structure of a TO and its ideology or motivating principles [8]. For example, Leninist or Maoist groups tend toward hierarchical structure (implying centralized leadership). Hierarchical groups are better suited for coordination and synchronization with political efforts. Larger organizations tend to adopt a networked, cellular structure at some point to reduce the risk of security breaches and counterintelligence failures [8].

## 4.8 TO Enabling Factors

According to the National War College report, the "most prominent contributing factors that enable terrorism to flourish" are (Reference 6, p. 54)

- poverty and economic and social inequities;
- poor governance with economic stagnation;
- illiteracy and lack of education;

- resentment to the encroachment of western values;
- unpopular foreign policies among potential target countries.

## 5 MODELS

A current trend in terrorist threat mitigation is to employ technology in the form of analytical tools as models, simulations, and data mining software to derive understanding about TOs where hard intelligence resources are limited or nonexistent.

A general knowledge of the prevalent models of terrorist organizational structures can be expected to lead to a better understanding of the threat, functionality, capabilities, and vulnerabilities of the organization [8]. The following sections discuss, in general terms, the most current analytical methods employed against the modeling and analysis of TOs.

### 5.1 Network Models

To conduct network analysis on a terrorist group, one typically represents the members of the group as nodes and the links between the nodes are representative of associations such as chain of command or resource dependencies [17]. The relative number of links emanating from a node tends to suggest a leadership position within a network, or otherwise, a key resource node [17]. When there are many short paths passing through a member, a gatekeeper role is likely. A gatekeeper acts as a facilitator between subgroups of a network [17]. Nodes (members) that are not linked are likely to exist in separate subgroups [7].

Organizational network modeling programs are available that can automatically identify the links per node of a network and present the results graphically in a top-down (hierarchical) fashion or in a rose form where the most influential nodes are located in the center of the diagram. The same programs can be used to identify subgroups within the network [18].

The *NetBreaker* modeling and analysis tool developed by Argonne National Laboratory [19] takes as input a list of known organization members (and their functions, if known), along with any unknown members and any known or hypothesized interactions involving the group. The interim analysis result is a set of all the possible terrorist networks that could include the input set. The interim analysis is based on validated network formation rules. Subsequent questions and rules are applied to reduce the size of the interim solution set, thereby honing in on the most likely actual structure of the organization. This kind of analysis is useful for identifying key functionaries in the network and for identifying vulnerabilities so that counterterror efforts can be more keenly focused.

The information required as input to network modeling tools is more likely to be found in a centralized terror network. Compromised elements of a centralized terrorist network will tend to lead, ultimately, to other elements. However, centralized structures can be expected to operate through well-established leadership chains and have well-organized communication and logistics channels. Distributed networks tend to be more difficult to identify or eliminate since leadership communication and logistics channels can be expected to be shorter. For distributed networks where elements act with more autonomy and with greater independence, it tends to be more difficult to identify dependencies between network elements.

Network modeling methods can be useful for determining what subgroups exist within a network. Moreover, the following information may be uncovered [20]:

- Whether subgroups are subordinate to one another.
- Whether the subgroups exist within a common logistics chain.
- Whether the subgroups have members in common.
- Whether the subgroups rely on one another for operational or financial support.
- Whether the overall network is centralized or distributed in form.
- What roles do members or subgroups play?

Clues to the structure of TOs can be uncovered that may lead to insights as to where limited counterterrorism resources can be directed for the most effect. For example, if a network is found to be more of a centralized structure, penetrating or destroying the nucleus of the network would tend to offer the greatest impact against the network as a whole. Similarly, when chain-like dependencies and linkages to subgroups are identified, whole operational cells (subgroups) could be effectively cut off and temporarily isolated with a "surgical" application of counterterror operations [17].

### 5.2 Network Influence Models

Influence models are derived from network models. They are based on an assumption that for the most part, members with more links attached to them have influence over those members with fewer links. The degree of influence is taken as a degree of importance of an individual to the organization as a whole [18]. Influence diagrams are intended to capture the interrelationship of factors pertinent to a given decision at a snapshot in time. Therefore, unlike causal and Bayesian models that are discussed in the following section, they have the weakness of being insensitive causal factors and decision-making processes [21].

### 5.3 Causal and Markov Modeling

Causal modeling of TOs is a method of identifying precursor conditions and/or actions that lead to some other condition or action on behalf of the TO. Some of the questions that causal modeling would address might be as follows [2]

- What conditions lead a TO to evolve from a nationally focused one to a transnational organization?
- How do national characteristics manifest in TOs?
- How do large events, including natural disasters, likely to affect TOs?
- What is the relationship between political activity and terrorism activities?

Causal models can be built based on a Markov chain construct where actions, conditions, and decision points are modeled in a flow chart fashion. Transition from one node in the Markov chain to another will occur based on a probability determined by the current state of model (i.e. what conditions are currently prevailing within the TO), and not based on precursor conditions that led the TO to the current state. Known information can be compared with a validated causal model to identify the patterns associated with specific terrorist activities and threats [22].

### 5.4 Bayesian Models

Bayesian models built on the Markov technique are used to answer high-level questions regarding a TO based on more conditions that can affect the transition of state. The types of questions that are answered might include the following: Will the organization merge with another? Will it attack a specific target? Will it escalate an attack? The Bayesian aspect of the modeling method addresses the decision-making processes and reactions within the organization that are conditioned upon previous actions and the current state of affairs. The Markovian aspect of the model defines the basic processes associated with operating a TO or planning or carrying out a terrorist attack. Bayesian (probabilistic) decisions are derived at different states along a chain of Markov-modeled events based on the plurality of conditions. The combined result of the Bayesian and Markov modeling is a complex model that can be used as a test bed for antiterrorism policy [23] and as a foundation for agent-based models such as those described in Section 5.6.

### 5.5 Dynamic Organizational Theory

Although the structure of TOs may hold clues to the strengths and/or vulnerabilities of it, understanding the dynamic aspects of the organization is also of great interest. The dynamic aspects might reveal under what conditions certain key functions such as training, recruiting, and funding become critically challenged or significantly enabled. Any probabilistic rules governing the likely responses of the organizational behavior to counterterror, bureaucratic, or societal stimuli are of interest to those planning antiterror strategies or conducting risk mitigation [24].

DeGhetto sets forth that organization theory (i.e. the study of organizational dynamics) and, specifically, organizational decline theory can be used effectively against TOs [25]. The agent-based modeling (ABM) methods described in the following section provide a means for testing counterterror strategies such as those outlined in DeGhetto's thesis [25].

Terrorist group decline factors, as identified by Kent Layne Oots, are the lack of entrepreneurial leadership, recruitment, ability to form coalitions with other groups, political and financial outside support, internal and external competition, and internal cohesiveness [26]. Preemption, deterrence, backlash, and burnout are the main factors for terrorist group decline, as identified by Gurr and Ross [27]. Another factor might be the failure of legitimate or illegitimate commercial ventures that the organization might be involved in.

### 5.6 Agent-Based Models and Complex Adaptive Systems

A system modeled as a set of independently simulated, interacting, and adaptive "agents" is referred to as a *complex adaptive system (CAS)*. Modeling a TO as a CAS is often effective in bringing out the dynamic aspects of the organization. The agents that comprise a CAS are themselves models of dynamic entities such as people or other groups or organizations.

The rules that govern agent behaviors are typically based on a large set of empirical and/or random variables [24]. Basic agent rules might govern movement, trading behavior, combat, interaction with the environment, cultural behaviors, and interaction between sexes and noncombatants [28].

In a sense, with ABM, a model of a relevant portion of the world, with as many relevant factors and conditions represented as possible, is developed. Within that world,

a TO is modeled as a CAS comprising many free-acting agents (perhaps sharing the same goal or motivations) that are programmed to behave and respond like real people. The combined result of the agents responding independently to conditions, other agents, and stimuli is an emergent and unpredictable higher level organizational behavior [24].

ABM in the context of a dynamic network model allows internal reactions and regrouping of a TO to be anticipated when one or more members are compromised or eliminated. The capability also can be used to help identify terrorists or to identify hidden dependencies on critical personnel or resources [29].

ABM provides a kind of "flight simulator" functionality that can serve as a test bed for tying various tactical and policy approaches in response to the terror threat and under a wide range of conditions [30]. Simulations based on ABM are also useful to determine the limits of an organization's capabilities.

### 5.7 Human Behavior Models

In ABM, modeled agents can have individual human characteristics, including personality traits such as temperament, dedication to the group, and ambition. These traits provide input to behavioral models. The actions and roles of the agents are subject to rules of social interaction and broader guiding principles [19].

A human behavior model developed by Barry Silverman et al., University of Pennsylvania, includes, for example, over 100 interdependent submodels of anthropological, physiological, medical, societal, cultural, religious, and political factors. The models have been incorporated into sophisticated, game-like simulations with life-like avatars, each with specific personalities and motivations. The models can be used to train in counterterror operations and to help identify terrorists based on interactions with others and patterns of behavior [29].

### 5.8 Population Dynamics Models

High-level modeling of TOs in terms of the size of the organization is taking place at the University of Maryland, Center for Technology and Systems Management (CTSM). Terrorist population dynamics (TPD) models rely on data pertaining to the growth and contraction of terrorist network population over a given time interval to estimate factors such as current terrorist population size, typical rates of growth and contraction of the TO, and correlations of TO size with activities and societal forces acting outside of the TO [31].

## 6 RESEARCH DIRECTIONS

The effectiveness of the modeling and analytical methods described in this article is limited by the quality and accuracy of information that the models are provided with and are based on. Increasingly, models and historical data are turned to fill the gaps of knowledge about TOs that are the result of otherwise poor intelligence. Models can be expanded but the ability to validate the models based on known facts about TOs will continue to be a challenge.

Case studies directed toward validation of the methods will always be valuable. A common set of metrics is needed to base evaluations of models and their specific applications. These metrics will allow a host of model and analytical techniques to be evaluated against each other in the context of a wide range of questions, TOs and conditions.

Areas for continued research include the hybridization of some of the methods described in the article. Review of the literature indicates that TO dependencies on resources such as arms, real properties, various kinds of communications, and transportation can be more rigorously modeled, perhaps revealing new insights or points of vulnerability. The flow of specific commodities within a TO can provide clues to the timing, nature, and scale of pending attacks.

A recurring theme in the literature is that TOs inevitably persist under challenged conditions that are often exclusive to covert, illegal, and largely unpopular organizations. The notion that TOs do not face at least the same problems with other large organizations, including bureaucracy, conflict, fraud, poor morale, attrition, and financial hardship, is not founded based on the research. Consequently, the opportunity exists to aggravate and exploit some of these factors to mitigate the threat posed by TOs [25] [9].

## REFERENCES


1. US Joint Chiefs of Staff. *Joint Tactics, Techniques and Procedures (JTTP) for Antiterrorism*, U.S. Government Joint Chiefs of Staff 3-07.2. (Revised first draft). 2004 Apr 9. (FOUO-Referenced in [7], pp. 3–1.
2. Hopple, G. W. (1982). Transnational terrorism: prospectus for a causal modeling approach. *Terrorism Int. J.* **6**(1), 73–100.
3. Library of Congress, Federal Research Center. (1999). *The Sociology and Psychology of Terrorism: Who Becomes a Terrorist and why*. Report. Washington (DC), 1999 Sept. 186. There are other standard definitions. One compendium is provided by the Terrorism Research Center Inc, URL: http://www.terrorism.com.
4. Ganor, B. (2002). Defining terrorism: is one man's terrorist another man's freedom fighter? *Police Pract. Res.* **3**(4), 287–304.
5. Crenshaw, M. (1985). An organizational approach to the analysis of political terrorism. *Orbis* **29**(3), 465–489.
6. National War College Student Task Force on Combating Terrorism. (2002). *Combating Terrorism in a Globalized World*. Report. National War College, Washington, DC, 2002 Nov. 88 pages.
7. Franck, R. E., and Melese, F. (2004). Exploring the structure of terrorists' WMD decisions: a game theory approach. *Def. Secur. Anal.* **20**(4), 355–372.
8. U.S. Army Training and Doctrine Command. (2005). *A Military Guide to Terrorism in the Twenty-First Century; TRADOC DCSINT Handbook*, Number 1 Chapter 3: Terrorist group organization, Leavenworth, KS, 3-1–3-12. Available from http://www.fas.org/irp/threat/terrorism/index.html; Internet; accessed Jan. 28, 2007.
9. Shapiro, J. (2005). The greedy terrorist: a rational-choice perspective on terrorist organizations' inefficiencies and vulnerabilities. *Strateg. Insights* **4**(1), 13.
10. Mickolus, E. (2005). How do we know if we are winning the war against terrorists? Issues in measurement. *Stud. Conflict Terrorism* **25**(3), 151–160.
11. Jackson, B. A., Baker, J. C., Cragin, K., Parachini, J., Trujillo, H. R., and Chalk, P. (2005). *Aptitude for Destruction: Volume 2: Case Studies of Organizational Learning in Five Terrorist*

*Groups*. RAND Corporation, Santa Monica, CA, p. 216, available from: http://www.rand.org/pubs/monographs/2005/RAND_MG332.pdf, accessed 2007 Feb. 24.

12. Hopmeier, M.. Unconventional. (2007). *Terrorism Expert*, Interview by phone. 2007 Mar. 18.
13. Cronin, A. R., Aden, H., Frost, A., and Jones, B.. Congressional Research Service [CRS]. (2004). Foreign terrorist organizations. Report for Congress. Library of Congress; 2004 Feb. 6. 111. Available from: http://www.fas.org/irp/crs/RL32223.pdf, accessed ~2007 Feb. 24.
14. National Defense University (US) [NDU]. (2002). *Chemical, Biological, Radiological, and Nuclear Terrorism: the Threat According to the Current Unclassified Literature*. Center for the Study of Weapons of Mass Destruction. ISN Publishing House, p. 46, available from: http://www.isn.ethz.ch/pubs/ph/details.cfm?v21=94077&lng=en&id=26595, accessed 2007 Feb 24.
15. Fatur, R. B.. (2005). *Influencing transnational terrorist organizations: using influence nets to prioritize factors*, [masters thesis]. Air Force Institute of Technology Wright-Patterson AFB OH School of Engineering and Management, 2005 June. 94 p. A523634.
16. Hoffman, B. (2004). The changing face of Al Qaeda and the global war on terrorism. *Stud. Conflict Terrorism* **27**(6), 549–560.
17. Xu, J., and Chen, H. (2005). Criminal network analysis and visualization. *Commun. ACM* **48**(6), 101–107.
18. Brams, S., Mutlu, H., and Ramirez, S. L. (2006). Influence in terrorist networks: from undirected to directed graphs. *Stud. Conflict Terrorism* **29**(7), 679–694.
19. North, M. J., Macal, C. M., and Vos, J. R.. (2004). Terrorist organizational modeling. *Argonne National Laboratory: NAACSOS Conference*, Pittsburgh, PA, 2004 June 27; n.d., p. 4 http://www.casos.cs.cmu.edu/events/conferences/2004/2004_proceedings/North_Michael.doc., accessed Feb 24, 2007.
20. McAndrew, D. (1999). The structural analysis of criminal networks. In *The Social Psychology of Crime: Groups, Teams, and Networks, Offender Profiling Series, III*, D. Canter, and L. Alison, Eds. Darthmouth, Aldershot.
21. Clemen, R. T., and Reilly, T. (2001). *Making Hard Decisions with Decision Tools*. Duxbury Resource Center, Belmont, CA, p. 752.
22. Coffman, T. R., and Marcus, S. E.. (2004). Dynamic classification of groups through social network analysis and HMMs. *IEEE: Aerospace Conference 2004*, BigSky, MO, 2004 Mar. 6, IEEE, 2004, p. 8.
23. Tu, H., Allanach, J., Singh, S., Pattipati, K. R., and Willett, P.. (2005). *Information Integration via Hierarchical and Hybrid Bayesian Networks [Internet]*. Storrs, CT: [cited 2007 Feb. 24]. p. 14, available from: http://servery.engr.uconn.edu/cyberlab/Satnam/docs/HHBN.pdf.
24. Elliott, E., and Kiel, L. D. (2004). A complex systems approach for developing public policy toward terrorism: an agent-based approach. *Chaos Solitons Fractals* **20**, 63–68.
25. DeGhetto, T. H. (1994). *Precipitating the decline of terrorist groups: a systems analysis*, [master's thesis]. Naval Postgraduate School, Monterey, CA, Mar. 24. 89 p.
26. Oots, K. L. (1989). Organizational perspectives on the formation and disintegration of terrorist groups. *Terrorism* **12**(3), 139–152.
27. Ross, J. I., and Gurr, T. R. (1989). Why terrorist subsides: a comparative study of Canada and the United States. *Comp. Polit.* **21**(4), 405–426.
28. Epstein, J. M. (1989). Agent-based computational models and generative social science. *Complexity* **4**(5), 41–60.
29. Goldstein, H.. (2006). *Modeling Terrorists*. IEE Eng Spectrum [serial on the Internet]. 2006 Sept. [cited 2007 Jan. 30]; Available from: http://spectrum.ieee.org/print/4424.
30. Holland, J. H. (1995). *Hidden Order: How Adaptation Builds Complexity*. Helix Books, Reading, MA.

31. Kaminskiy, M., and Ayyub, B. (2006). Terrorist population dynamics model. *Risk Anal.* **26**(3), 747–752.

## FURTHER READING

Ackoff Center for Advancement of Systems Approaches. (2007). Available from: http://www.acasa.upenn.edu/. See for more information on agent-based social behavior models at University of Pennsylvania.

Center for Computational Analysis of Social and Organizational Systems (CASOS). (2007) http://www.casos.cs.cmu.edu/terrorism/projects.php. See for more information on social network modeling efforts at Carnegie Mellon University.

Farey, J. D. (2003). Breaking Al Qaeda cells: a mathematical analysis of counterterrorism operations (a guide for risk assessment and decision making). *Stud. Conflict Terrorism* **26**, 399–411.

Gunaratna, R. (2005). The prospects of global terrorism. *Society* **42**(6), 31–35.

Gunaratna, R. (2005). Responding to terrorism as a kinetic and ideological threat. *Brown J. World Aff.* **11**(2), 243.

Johnston, R. (2005). *Analytic culture in the U.S. intelligence community*. The Center for the Study of Intelligence. CIA, Pittsburgh, PA, p. 184, available from: http://www.fas.org/irp/cia/product/analytic.pdf, accessed~n.d.

Klerks, P. (2001). The network paradigm applied to criminal organizations: theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands. *Connections* **24**(3), 53–65.

Krebs, V. E. (2001). Mapping networks of terrorist cells, *Connections* **24**(3), 43–52.

Newman, M., Barabasi, A. L., and Watts, D. J. (2006). *The Structure and Dynamics of Networks*. Princeton University Press, Princeton, NJ.

# RISK COMMUNICATION—AN OVERLOOKED TOOL IN COMBATING TERRORISM

DAVID ROPEIK

*Risk Communication, Ropeik & Associates, Concord, Massachusetts*

## 1 THE NEED

The terrorist attacks on September 11, 2001, killed approximately 3000 people, directly. But the death toll was higher. 1018 more Americans died in motor vehicle crashes

October through December 2001 than in those 3 months the year before, according to researchers at the University of Michigan's Transportation Research Institute. As those researchers observe " . . . the increased fear of flying following September 11 may have resulted in a modal shift from flying to driving for some of the fearful" [1]. 1018 people died, more than one-third the number of people killed in the attacks of September 11, in large part because they perceived flying to be more dangerous and driving less so, despite overwhelming statistical evidence to the contrary.

As much as 17% of Americans outside New York City reported symptoms of post-traumatic stress two months after the September 11, 2001, attacks [2]. Even 3 years later, a significant number of Americans were still suffering serious health problems as a result of that stress. In a random sample of 2000 Americans, people who reported acute stress responses to the 9/11 attacks, even if they only watched the events on television, had a 53% increased incidence in doctor-diagnosed cardiovascular ailments like high blood pressure, heart problems, or stroke for up to 3 years following the attacks. The impact was worse among those who continued to worry that terrorism might affect them in the future. These people were three to four times more likely to report a doctor-diagnosed cardiovascular problem [3].

The Oxford English Dictionary defines terrorism as "the action or quality of causing dread". But that definition is inadequate. The dread caused by terrorism is just an intermediate outcome. More important are the health effects that result from such fear. Terrorism injures and kills both directly—from the attacks themselves—and indirectly, from what has been called the social amplification of risk, from the behaviors and stress that our worries produce [4]. Risk communication is an underutilized tool for combating those effects and minimizing the harm that terrorism can cause.

## 2 RISK COMMUNICATION DEFINED

The term *risk communication* arose largely as a result of environmental controversies in the 1970s, when public concern was high about some relatively low threats to human and environmental health. Scientists, regulators, and the regulated community described this public concern as irrational, and in their frustration they looked for ways to make people behave more rationally (as defined by those experts), especially about issues such as air and water pollution, nuclear power, and industrial chemicals. The goal of early risk communication was rarely to enlighten people so that they might improve their health. It was frequently to reduce conflict and controversy, an effort to talk people out of opposing some product or technology of which they were afraid. One researcher defined risk communication as "a code word for brainwashing by experts or industry" [5].

But risk communication has evolved. This article will use the following definition:

> "Risk communication is a combination of actions, words, and other messages responsive to the concerns and values of the information recipients, intended to help people make more informed decisions about threats to their health and safety."

That definition attempts to embody the ways that risk communication has matured over the past two decades. The consensus among experts in the field now rejects the one-way "We'll teach them what they need to know" approach. A National Research Council effort to move the field forward produced this definition in 1989. "*Risk communication is*

*an interactive process of exchange of information and opinion among individuals, groups, and institutions. It involves multiple messages about the nature of risk and other messages, not strictly about risk, that express concerns, opinions, or reactions to risk messages or to legal and institutional arrangements for risk management*" [6]. In other words, risk communication should be considered a dynamic two-way street. Both sides get to talk, and both sides have to listen, and respond to input from the other.

More fundamentally, and intrinsic to the idea of the two-way street, is the growing acceptance among risk communication experts that risk means something different to the lay public than to scientists and regulators. "Risk" is perceived as more than a science-based rational calculation by the general public. Other attributes, like trust, dread, control, and uncertainty, also factor into the judgments people make about what they are afraid of.

As risk communication has evolved, more and more experts in the field agree that both the science-based view of experts and the affective view of risk among the general public are valid, and both must be respected and incorporated if communications about risk is to be effective.

This evolution is summed up in Risk Communication and Public Health, edited by Peter Bennett and Kenneth Calman:

> " . . . there has been a progressive change in the literature on risk:
>
> - *from* an emphasis on 'public *misperceptions*', with a tendency to treat all deviations from expert estimates as products of ignorance or stupidity
> - *via* empirical investigation of what actually concerns people and why
> - *to* approaches which stress that public reactions to risk often have a rationality of their own, and that 'expert' and 'lay' perspectives should inform each other as part of a two-way process" [7].

The evidence that illuminates what actually concerns people and why, requires discussion at some length. A solid body of careful research from a number of fields has established that the lay public's perception of risk is based on a dual process of fact-based analysis *and* intuitive, affective factors. The Greek Stoic philosopher Epictetus said "People are disturbed, not by things, but by their view of them." Understanding the roots of what shapes those views allows the true dialogue of modern risk communication to take place.

## 3 THE BIOLOGY OF FEAR

Neuroscientists have found that what we consciously describe as fear begins in a subcortical organ called the amygdala. Critically for risk communication, in very simplified terms, information is processed in the amygdala, the part of the brain where fear begins, *before* it is processed in the cortex, the part of the brain where we think. We fear first and think second [8]. That alone suggests that risk communication that merely attempts to communicate the facts, without factoring in the emotional issues involved, will not be as successful.

There is also neuroscientific evidence suggesting that as we process information, we fear *more*, and think *less*. Neural circuits have been identified that lead from the

amygdala to parts of the cortex, circuits which, in essence, trigger a "fight or flight" response (accelerated heart rate, hormonal responses, etc.). The pathways coming back into the amygdala from the thinking "rational" cortex have also been identified. And there are more circuits out of the amygdala, the organ that stimulates a fear response, than there are circuits coming back in from the "thinking" brain, which could moderate that response.

So when we encounter information that might pose a threat, we generally fear first and think second, and fear more and think less. This basic description of the way the human brain is physically wired has fundamental implications for risk communication and dramatically reinforces the importance of findings from social science, which explain why risk means one thing to experts and another to the lay public.

## 4 RISK PERCEPTION PSYCHOLOGY

Some of what we are commonly afraid of seems instinctive: snakes, heights, the dark, and so on. But how do we subconsciously "decide" what to be afraid of, and how afraid to be, when the threat does not trigger an instinctive reaction; when we hear about a new disease, product, or technology, or when we try to gauge the risk of something against its benefits, or when we witness an act of terrorism? How does the human mind translate raw data into our perceptions of what is risky and what is not?

The answers can be found in two literatures, both critically relevant to risk communication. The first is the study of how people generally make judgments of any kind, including judgments about risk, under conditions of uncertainty. The second is the specific study of the psychology of risk perception, which has identified more than a dozen affective attributes that tend to make some threats feel more worrisome than others, even when our apprehension is not consistent with the scientific data.

### 4.1 General Heuristics and Biases

The discovery of systematic heuristics and biases—mental shortcuts—that we use to make choices under uncertainty, when we do not have all the facts, or all the time we need to get all the facts, or all the intellectual ability to fully understand the facts we have, was led by, among others, Daniel Kahneman, who was awarded the 2002 Nobel Gold Medal in Economics for his work. Kahneman and others identified a number of mental processes that simplify decision making when time or complete information is not available. This field has direct relevance for risk communication, as noted in a seminal paper on risk perception: "When laypeople are asked to evaluate risks, they seldom have statistical evidence on hand. In most cases, they must make inferences based on what they remember hearing or observing about the risk in question." "These judgmental rules, known as heuristics, are employed to reduce difficult mental tasks to simpler ones" [9].

Here are a few of the heuristics and biases relevant to risk perception, and therefore to risk communication.

- *Availability.* " . . . people assess the . . . the probability of an event by the ease with which instances or occurrences can be brought to mind" [10]. The risk of terrorism in the United States is statistically quite low. But apprehension has been elevated since September 11, 2001, in part because such an event is more "available" to our

consciousness. The availability heuristic explains why, when a risk is in the news (flu vaccine issues, an outbreak of food poisoning, child abduction, etc.), it evokes more fear than when the same risk is around, at the same level, but just not making headlines.

- *Framing.* The way a choice is presented can distort the judgment that results. Imagine you are the mayor of a city of 1 million people and a fatal disease is spreading through your community. It is occurring mostly, but not exclusively in one neighborhood of 5000 residents. With a fixed amount of money, you can either (i) save 20% of the 5000 residents in that neighborhood, or (ii) save 0.2% of the entire city of 1 million. What do you do?

  A sizable number of people in risk communication classes I teach choose option (i), which produces a greater percentage effectiveness, but condemns 1000 people to death. Reframed, the choice would be: you can spend a fixed amount of money and save 1000 people or 2000. Presented that way, the choice is obvious. But the framing of the question in terms of percentages skews the judgment. Understanding the importance of framing is a key to better risk communication.
- *Anchoring and adjustment.* People estimate probabilities based on an initial value and adjusting from there. In one experiment, two groups of high school students estimated the sum of two numerical expressions that they were shown for just 5 s, not long enough for a complete computation. The first group was shown $9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1$. Their median estimate was 2250. The median estimate for the second group, shown the same sequence, but in ascending order—$1 \times 2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9$—was 512 [11]. Knowledge of the anchoring effect is another tool for better risk communication.
- *Representativeness.* This is "the tendency to regard a sample as a representation of the whole, based on what we already know" [12]. Consider two people:
  - A white woman who is shy and withdrawn, with little interest in people, a strong need for order and structure, and a passion for detail.
  - A young man of middle-eastern complexion who is passionate, but sullen, quick to anger, bright, and unconcerned with material possessions.

Which one is the librarian, and which one is the terrorist? Without complete data by which to make a fully informed choice, the representativeness heuristic gives you a simple mental process by which to take the partial information and fit it into the preexisting category it represents. This suggests that risk communication must consider the patterns of knowledge and information people already have, on which they will base their response to what the communicator says.

### 4.2 Risk Perception Characteristics

Work in a related field, the specific study of the perception of risk, has identified a number of attributes that make certain risks feel more worrisome than others.

These risk perception factors are essentially the personality traits of potential threats that help us subconsciously "decide" what to be afraid of and how afraid to be. They offer powerful insight into why "risk" means different things to the lay public than it does to experts. A few of these factors have particular relevance to terrorism.

- *Trust.* When we trust *the people informing us* about a risk, our fears go down. When we trust *the process* deciding whether we will be exposed to a hazard, we will be less afraid. When we trust *the agencies that are supposed to protect us*, we will be less afraid. If we do not trust the people informing us, the process determining our exposure to a risk, or the people protecting us, we will be more afraid.

  Trust comes from openness, honesty, competence, accountability, and respecting the lay public's intuitive reasoning about risk.
- *Risk versus Benefit.* The more we perceive a benefit from any given choice, the less fearful we are of the risk that comes with that choice. This factor helps explain why, of more than 400,000 "first responders" asked to take the smallpox vaccine in 2002, fewer than 50,000 did. They were being asked to take a risk of about one in a million—the known fatal risk of the vaccine—in exchange for ZERO benefit, since there was no actual smallpox threat. Imagine, however, there was just one confirmed case of smallpox in a US hospital. The fatality risk of the vaccine would still be one in a million, but the benefit of the shot would suddenly look much greater
- *Control.* If you feel as though you can control the outcome of a hazard, you are less likely to be afraid. This can be either physical control as when you are driving and controlling the vehicle, or a *sense* of control of a process, as when you feel you are able to participate in policy making about a risk through stakeholder involvement, participating in public hearings, voting, and so on.

  This is why, whenever possible, risk communication should include information not just about the risk ("Terrorists have attacked the food supply"), but also offer information about what people can do to reduce their risk ("Boil milk before you drink it"). Specifically as regards food-related terrorism, information about how people can participate in a food recall is of particular value, by giving people a sense of control.
- *Imposed versus voluntary.* We are much less afraid of a risk when it is voluntary than when it is imposed on us, as is the case in terrorism, agricultural, or otherwise.
- *Natural versus human-made.* If the risk is natural, we are less afraid. If it is human-made, we are more afraid. A radiologically contaminated conventional explosive—a "dirty bomb"—will evoke much more fear than radiation from the sun, which will cause far more illness and death. A natural foodborne pathogen such as *E. coli* O157:H will likely produce less concern than a "militarized" pathogen such as anthrax, regardless of their scientific risk profiles.
- *Dread.* We are more afraid of risks that might kill us in particularly painful, gruesome ways than risks that kill us in more benign fashion. Ask people which risk sounds worse, dying in a fiery plane crash or dying of heart disease, and they are likely to be more afraid of the plane crash, despite the probabilities.

  This factor helps explain why the United States has a "War on Cancer", but not "War on Heart Disease". Cancer is perceived as a more dreadful way to die, so it evokes more fear, and therefore more pressure on government to protect us, thought heart disease kills far more people annually.
- *Catastrophic versus chronic.* We tend to be more afraid of things that can kill a lot of us in one place at one time, such as a plane crash, than heart disease or stroke or chronic respiratory diseases or influenza, which cause hundreds of thousands more

deaths, but spread out over time and location. This factor makes foodborne illness outbreaks much more frightening than the chronic presence of foodborne illness, which sickens one American in four per year.

- *Uncertainty.* The less we understand about a risk, the more afraid we are likely to be, as is the case with terrorism, particularly a terrorist attack on the food supply, where there will likely be many unknowns. When uncertainty exists because all the facts are not in, the fear that results must be acknowledged and respected.
- *Is the risk personal.* Understandably, a risk that we think can happen to us evokes more concern than a risk that only threatens others. As a demonstration of this, consider how the attacks of September 11 made terrorism a risk not just to Americans living somewhere else, but to Americans at home. Suddenly we realized "this could happen to ME!" We began referring to the United States as "The Homeland". We could probably take the "H" and the "O" out of the word. What we are really saying is that now terrorism could happen in the "MEland".

  This factor explains why numbers alone are ineffective as risk communications. One in a million is too high if you think you can be the one.
- *Personification.* A risk made real by a person/victim, such as news reports showing someone who has been attacked by a shark or a child who has been kidnapped, becomes more frightening than one that is statistically real, but only hypothetical.

There are a few important general qualifications about the heuristics and biases mentioned earlier, and the risk perception factors listed immediately above. Often, several of these factors are relevant for any given risk. A terrorist attack on the food supply will certainly evoke issues of trust, dread, and control, among other factors. The availability heuristic will certainly affect how afraid we are.

Also, while the research suggests that these tendencies are universal, any given individual will perceive a risk uniquely depending on his or her life circumstances, that is, age, gender, health, genetics, lifestyle choices, demographics, education, and so on. This means that although it is good risk communication practice to consider the emotional concerns of the audience, not everyone in a large audience shares the same concerns. As the National Research Council report suggests, "For issues that affect large numbers of people, it will nearly always be a mistake to assume that the people involved are homogeneous . . . . It is often useful to craft separate messages that are appropriate for each segment" [13].

## 5 RECOMMENDATIONS

In general, by understanding and respecting the psychological reasons for people's concerns (or lack of concerns in the case of terrorism preparedness), risk communication strategies can be devised that take these factors into account and shape messages that are more resonant with people's perceptions. That in turn, increases the likelihood that the messages will be more trusted, better-received, which increases the impact they will have.

However, as the National Research Council report noted, " . . . there is no single overriding problem and thus no simple way of making risk communication easy" [14]. So although this article provides suggestions on fundamentals, it cannot offer a detailed how-to guide to risk communication.

But there are several widely accepted general recommendations:

*Include risk communication in all risk management policy making and action. Far more is communicated by what you do than what you say*. "Risk communication . . . must be understood in the context of decision making involving hazards and risks, that is, risk management" (NRC) [15]. Consider the example cited a few pages ago of the failed Bush administration smallpox vaccination policy. Had the risk perception factor of "risk versus benefit" been considered when the policy was being discussed, officials might not have chosen a policy unlikely to meet its objectives since it asked people to take a risk (albeit low) for ZERO benefit. In other words, the policy itself, not the press releases about it, carried implicit, but very clear risk communication information that had a lot to do with how people responded.

Information that affects how people think and feel about a given risk issue is conveyed in nearly all of the management actions an agency or a company or a health official takes on that issue. All risk management should include consideration of the risk perception and risk communication implications of any policy or action under review. Quite specifically, this means that *organizations should include risk communication in the responsibilities of senior managers, not just of the public relations or communications staff*. As the NRC report suggests, risk managers cannot afford to treat risk communication as an afterthought that comes at the end of the process after risk assessment has been done and policy set.

Recognize that *the gaps between public perception and the scientific facts about a risk can lead to behaviors that can threaten public health. These gaps are part of the overall risk that must be managed*. Whether people are more afraid of a risk than they need to be or when they are not afraid enough, this perception gap is a risk in and of itself and must be included in dealing with any specific risk issue and in all risk management and public health efforts.

Consider the example or the fear of flying post 9/11. One of the messages of the federal government was, paraphrasing, "Live your normal lives or the terrorists win. Go shopping." Had they considered the importance of the feeling of control to people's perceptions, perhaps the message might have suggested "Live your normal lives or the terrorists win. For example, flying seems scary right now. But if you choose not to fly and drive instead, because having a sense of control makes driving safer, remember that driving is much riskier, and if you die behind the wheel, the terrorists have won." Such a message might have saved the lives of some of those who made the choice to drive instead of fly.

*Trust is fundamentally important for effective risk communication, and it is on the line with everything you do*. " . . . messages are often judged first and foremost not by content but by the source: 'Who is telling me this, and can I trust them?' If the answer to the second question is 'no', *any* message from that source will often be disregarded, no matter how well-intentioned and well delivered" (Bennett and Calman) [16].

Trust is determined in part by who does the communicating. When the anthrax attacks took place in the fall of 2001, the principal government spokespeople were the Attorney General, the Director of the FBI, and the Secretary of Health and Human Services, and not the head of the CDC or the US. Surgeon General—doctors likely to be more trusted than politicians. Had risk communication been included in the considerations of senior managers as the anthrax issue was beginning to develop, and incorporated into the deliberations of how to manage the overall anthrax risk, the more trusted officials would have done the majority of the public speaking, which might have done more to

help the public keep their concern about the risk of bioterrorism in perspective. This lesson should be applied to any risk communication in connecting with agroterrorism.

But trust is more than just who does the talking. Trust also depends on competence. If people believe that a public health or safety agency is competent, they will trust that agency to protect them, and be less afraid, than if they doubt the agency's ability. When the first mad cow case in the United States was found in 2003, the US Department of Agriculture and Food and Drug Administration were able to point to a long list of regulatory actions they had taken for years to keep the risk low. So the *actions* taken by those agencies, years before the news conferences and press releases about that first case, had risk perception implications by establishing trust and thus affecting the public's judgment about the risk and their behavior. This helps explain why beef sales in the United States after that first case was discovered were effectively unchanged.

Trust is also heavily dependent on honesty. Of course, honesty means many things. In some instances, it can mean apologizing or taking responsibility for mistakes. When leaks developed in underground tunnels that are part of a major transportation project in Boston, press attention and public criticism focused on the contractor responsible for the tunnels until the chairman of the company said at a tense public hearing "We apologize for our mistakes" [17] (Note that the apology was made 'sincere' by the fact that it came from the head of the company, and the fact that the company offered to pay for repairs.). Criticism of the company dropped substantially thereafter.

Another example of honesty is avoiding the desire to over-reassure. Again, the way the USDA handled mad cow disease illustrates one example. In the years prior to that first sick cow being found, top officials never promised there was ZERO risk of mad cow disease, either in animals or in humans, just that the risk was very low. Had they followed the initial inclination of some senior USDA officials and promised that the risk was ZERO, that single first case would probably have provoked more public concern because people might have feared that the government's overassurance was not honest and could not be trusted.

And, obviously, honesty means not covering things up or telling untruths or half-truths. Being caught keeping secrets is almost always worse than revealing the information, even if damaging, first. Remember the framing heuristic mentioned above. How people think about an issue is based in part on the first way it is presented. Even if information is damaging, revealing it first gives the communicator the opportunity to "paint the first picture" of how people will think about the matter.

*Adopting risk communication into intrinsic risk management requires fundamental cultural change*. Sharing control, admitting mistakes, acknowledging the validity of the public's intuitive risk perception, not keeping secrets, being open and honest ... these are all countercultural to political, legal, and scientific organizations and people, the kinds of organizations and people who will be in charge of dealing with terrorist threats to the food supply. These are countercultural suggestions in a litigious society. They are countercultural to the myth of the purely rational decision-maker. As risk communication researcher and practitioner Peter Sandman has observed, "What is difficult in risk communication isn't figuring out what to do; it's overcoming the organizational and psychological barriers to doing it" [18].

Nonetheless, countless examples demonstrate how adoption of the principles of risk communication are in the best interests of most organizations, public safety officials, politicians, as well as the interest of public health. In the case of terrorism, they help officials with more effective risk management to protect public health. They increase

support for an agency's overall agenda or a company's brand and products, political support for a candidate or legislation, and they reduce controversy and legal actions. While these benefits may not be readily quantifiable, and only realized over the long term, they are real, well-supported by numerous examples, and argue strongly for the cultural change necessary for the adoption of best practice risk communication principles.

Finally, *if at all possible within constraints of time and budget, any specific risk communication should be systematically designed and executed, including iterative evaluation and refinement*. "We wouldn't release a new drug without adequate testing. Considering the potential health (and economic) consequences of misunderstanding risks, we should be equally loath to release a new risk communication without knowing its impact" [19].

*Risk communication messages and strategies specific to each plausible terrorist scenario should be developed in advance, and tested and revised to maximize effectiveness*. Being prepared for purposeful contamination of the food supply, with various agents, at various points of entry in the farm-to-fork system, is vital to protecting public health in such events.

## 6 CONCLUSION

The human imperative of survival compels us to make rapid decisions about the threats we face. But this decision-making process is almost always constrained by a lack of complete information, a lack of time to collect more information, and a lack of cognitive abilities to understand some of the information we have. In response, humans have evolved a dual system of reason and affect to rapidly judge how to keep ourselves safe. In many cases these judgments work to protect us. But sometimes they can lead to behaviors that feel right, but actually raise our risk, whether we are more afraid of a relatively low risk or not afraid enough of a relatively big one. Great harm to public health can occur in such cases. To mitigate this threat, it is critical that an understanding of risk perception and its application to effective risk communication become an intrinsic part of how organizations deal with the threat of terrorism.

## REFERENCES

1. Sivak, M., and Flanagan, M. (2004). Consequences for road traffic fatalities of the reduction in flying following September 11, 2001. *Trans. Res. Part F* **7**(4-5), 301–305.
2. Silver, R. C., Holman, E. A., McIntosh, D., Poulin, M., and Gil-Rivas, V. (2002). Nationwide longitudinal study of psychological responses to September 11. *JAMA* **288**, 11235–11244.
3. Holman, E. A., Silver, R. C., Poulin, M., Andersen, J., Gil-Rivas, V., and McIntosh, D. (2008). Terrorism, acute stress, and cardiovascular health, a 3-year study following the September 11th attacks. *Arch. Gen. Psychiatry* **65**(1), 73–80.
4. Pidgeon, N., Kasperson, R., and Slovic, P., Eds. (2003). *The Social Amplification of Risk*, Cambridge University Press, Cambridge, UK.
5. Jasanoff, S. (1989). Differences in national approaches to risk assessment and management. *Presented at the Symposium on Managing the Problem of Industrial Hazards: the International Policy Issues*, National Academy of Sciences, Feb. 27.
6. *Improving Risk Communication*, (1989). National Research Council, National Academy Press, p. 21.

7. Bennett, P., and Calman, K., Eds. (1999). *Risk Communication and Public Health*, Oxford University Press, New York, p. 3.
8. This very simplified synthesis of LeDoux's work comes from Ledoux, J. (1998). *The Emotional Brain: the Mysterious Underpinnings of Emotional Life*, Simon and Schuster, New York.
9. Slovic, P., Fischhoff, B., and Lichtenstein, S. (2001). A revised version of their original article appears. In *Judgment Under Uncertainty: Heuristics and biases*, D. Kahneman, P. Slovic, and A. Tversky, Eds. Cambridge University Press, Cambridge, UK, pp. 463–489.
10. Kahneman, D., Slovic, P., and Tversky, A., Eds. (1982). *Judgment Under Uncertainty: Heuristics and biases*, Cambridge University Press, Cambridge, UK, pp. 11–12.
11. Kahneman, D., Slovic, P., and Tversky, A., Eds. *Judgment Under Uncertainty: Heuristics and biases*, Cambridge University Press, Cambridge, UK, pp. 14–15.
12. Kahneman, D., Slovic, P., and Tversky, A., Eds. (1982). *Judgment Under Uncertainty: Heuristics and biases*, Cambridge University Press, Cambridge, UK, p. 24.
13. *Improving Risk Communication*, (1989). National Research Council, National Academy Press, p. 132.
14. *Improving Risk Communication*, (1989). National Research Council, National Academy Press, p. 3.
15. *Improving Risk Communication*, (1989). National Research Council, National Academy Press, p. 22.
16. Bennett, P., and Calman, K. (1991). *Risk Communication and Public Health*, Oxford University Press, Oxford, UK, p. 4.
17. *Big Dig Firm Apologizes, Considers Fund for Repairs*, (2004). Boston Globe, Dec. 3, p. 1.
18. Sandman, P. *The Nature of Outrage (part1)*, www.psandman.com.
19. Morgan Granger, M., Fischhoff, B., Bostrom, A., and Altman, C. (2002). *Risk Communication A Mental Models Approach*, Cambridge University Press, Cambridge, UK, p. 180.

# CROSS-CUTTING THEMES AND TECHNOLOGIES

## RISK MODELING AND VULNERABILITY ASSESSMENT

# TERRORISM RISK: CHARACTERISTICS AND FEATURES

BILAL M. AYYUB

*Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland*

## 1 INTRODUCTION

Risk is associated with all projects, business ventures, and activities taken by individuals and organizations regardless of their sizes, natures, and time and place of execution and utilization. Acts of violence including terrorism can be considered as an additional hazard source. These risks could result in significant losses, such as economic and financial losses, environmental damages, budget overruns, delivery delays, and even injuries and loss of life. In broad context, risks are taken even though they could lead to adverse consequences because of potential benefits, rewards, survival, and future return on investment. Risk taking is a characteristic of intelligence for living species since it involves decision making that is viewed as an expression of higher levels of intelligence. The chapter defines and discusses terrorism risk and its characteristics and features.

## 2 TERMINOLOGY

Definitions that are needed for risk analysis are presented herein [1].

Several definitions are available for the term *terrorism*, though without a globally accepted one. The following are selected definitions:

- US Code of Federal Regulations: " . . . the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives" (28 C.F.R. Section 0.85).
- Current US national security strategy: "premeditated, politically motivated violence against innocents".

- United States Department of Defense: the "calculated use of unlawful violence to inculcate fear; intended to coerce or intimidate governments or societies in pursuit of goals that are generally political, religious, or ideological".
- British Terrorism Act 2000 defines terrorism so as to include not only attacks on military personnel but also acts not usually considered violent, such as shutting down a website whose views one dislikes.
- 1984 US Army training manual says "terrorism is the calculated use of violence, or the threat of violence, to produce goals that are political or ideological in nature".
- 1986 Vice-President's Task Force: "Terrorism is the unlawful use or threat of violence against persons or property to further political or social objectives. It is usually intended to intimidate or coerce a government, individuals, or groups or to modify their behavior or politics."
- Insurance documents define terrorism as "any act including, but not limited to, the use of force or violence and/or threat thereof of any person or group(s) of persons whether acting alone or on behalf of, or in connection with, any organization(s) or government(s) committed for political, religions, ideological or similar purposes, including the intention to influence any government and/or to put the public or any section of the public in fear".

A *hazard* is an act or phenomenon posing potential harm to some person(s) or thing(s), that is, a source of harm, and its potential consequences. For example, uncontrolled fire is a hazard, water can be a hazard, and strong wind is a hazard. In order for the hazard to cause harm, it needs to interact with person(s) or thing(s) in a harmful manner. Hazards need to be identified and considered in projects' life cycle analyses since they could pose threats and could lead to project failures.

*Threat* is any indication, circumstance, or event with the potential to cause the loss of or damage to an asset. Threat can also be defined as the intention and capability of an adversary to undertake actions that would be detrimental to assets.

*Reliability* can be defined for a system or a component as its ability to fulfill its design functions under designated operating and/or environmental conditions for a specified time period. This ability is commonly measured using probabilities. Reliability is, therefore, the occurrence probability of the complementary event to failure.

For a failure event, *consequences* can be defined as the degree of damage or loss from some failure. Each failure of a system has some consequence(s). A failure could cause economic damage, environmental damage, injury or loss of human life, or other possible events. Consequences need to be quantified in terms of failure—consequence severities using relative or absolute measures for various consequence types to facilitate risk analysis.

*Risk* originates from the Latin term *risicum* meaning the challenge presented by a barrier reef to a sailor. The Oxford dictionary defines risk as the chance of hazard, bad consequence, loss, and so on. Also, risk is the chance of a negative outcome. Formally, risk can be defined as the potential of losses for a system resulting from an uncertain exposure to a hazard or as a result of an uncertain event. Risk should be identified based on risk events or event scenarios. Risk can be viewed as a multidimensional quantity that includes event-occurrence probability, event-occurrence consequences, consequence significance, and the population at risk; however, it is commonly measured as a pair of

the probability of occurrence of an event, and the outcomes or consequences associated with the event's occurrence. Another common representation of risk is in the form of an exceedence probability function of consequences.

*Probability* is a measure of the likelihood, chance, odds, or degree of belief that a particular outcome will occur. A conditional probability is the probability of occurrence of an event based on the assumption that another event (or multiple events) has occurred.

*An asset* is any person, environment, facility, physical system, material, cyber system, information, business reputation, or activity that has a positive value to an owner or to society as a whole.

The occurrence probability ($p$) of an outcome ($o$) can be decomposed into an occurrence probability of an event or threat ($t$) and the outcome-occurrence probability given the occurrence of the event ($o|t$). The occurrence probability of an outcome can be expressed as follows using conditional probability concepts:

$$p(o) = p(t)p(o|t) \tag{1}$$

In this context, threat is defined as a hazard or the capability and intention of an adversary to undertake actions that are detrimental to a system or an organization's interest. In this case, threat is a function of only the adversary or competitor, and usually cannot be controlled by the owner of the system. The adversary's intention to exploit his capability may, however, be encouraged by vulnerability of the system or discouraged by an owner's countermeasures. The probability $p(o|t)$ can be decomposed further into two components: success probability of the adversary and a conditional probability of consequences as a function of this success. This probability $p(o|t)$ can then be computed as the success probability of the adversary times the conditional probability of consequences given this success. The success probability of the adversary is referred to as the *vulnerability of the system* for the case of this threat occurrence. *Vulnerability* is a result of any weakness in the system or countermeasure that can be exploited by an adversary or competitor to cause damage to the system and result in consequences.

The *performance* of a system or component can be defined as its ability to meet functional requirements. The performance of an item can be described by various elements, such as speed, power, reliability, capability, efficiency, and maintainability. The design and operation of system affects this performance.

A *system* is a deterministic entity comprising an interacting collection of discrete elements and commonly defined using deterministic models. The word *deterministic* implies that the system is identifiable and not uncertain in its architecture. The definition of the system is based on analyzing its functional and/or performance requirements. A description of a system may be a combination of functional and physical elements. Usually functional descriptions are used to identify high information levels on a system. A system can be divided into subsystems that interact. Additional details in the definition of the system lead to a description of the physical elements, components, and various aspects of the system. Methods to address uncertainty in systems architecture are available and can be employed as provided by [3].

Risk-based technologies (RBT) are methods or tools and processes used to assess and manage the risks of a component or system. RBT methods can be classified into risk management that includes risk assessment/risk analysis and risk control using failure prevention and consequence mitigation, and risk communication. Risk assessment consists

of hazard identification, event-probability assessment, and consequence assessment. Risk control requires the definition of acceptable risk and comparative evaluation of options and/or alternatives through monitoring and decision analysis. Risk control also includes failure prevention and consequence mitigation. Risk communication involves perceptions of risk, which depends on the audience targeted. Hence, it is classified into the media, the public, and the engineering community.

*Safety* can be defined as the judgment of risk tolerance (or acceptability in the case of decision making) for the system. Safety is a relative term since the decision of risk acceptance may vary depending on the individual making the judgment. Different people are willing to accept different risks as demonstrated by different factors such as location, method or system type, occupation, and lifestyle. The selection of these different activities demonstrates an individual's safety preference despite a wide range of risk values. It should be noted that *risk perceptions* of safety may not reflect the actual level of risk in some activity.

*Risk assessment* is a technical and scientific process by which the risks of a given situation for a system are modeled and quantified. Risk assessment can require and/or provide both qualitative and quantitative data to decision makers for use in risk management. Risk analysis is the technical and scientific process to breakdown risk into its underlying components. Risk assessment and analysis provide the processes for identifying hazards, event-probability assessment, and consequence assessment. The risk assessment process answers three basic questions: (i) What can go wrong? (ii) What is the likelihood that it will go wrong? (iii) What are the consequences if it does go wrong? Answering these questions requires the utilization of various risk methods as discussed in this section. A summary of selected methods is provided in Table 1. A typical overall risk analysis and management methodology can be expressed in the form of a workflow or block diagram consisting of the following primary steps:

1. definition of a system based on a stated set of analysis objectives;
2. hazard or threat analysis, definition of failure scenarios, and hazardous sources and their terms;
3. data collection in a life cycle framework;
4. qualitative risk assessment;
5. quantitative risk assessment; and
6. management of system integrity through countermeasures, failure prevention, and consequence mitigation using risk-based decision making.

Methods to support these steps are described in various articles of this section on "Risk Modeling and Vulnerability Assessment".

Risk can be assessed and presented using matrices for preliminary screening by subjectively estimating probabilities and consequences in a qualitative manner. A risk matrix is a two-dimensional presentation of likelihood and consequences using qualitative metrics for both the dimensions as given in Tables 2–4 and Figure 1 with risk subjectively assessed as high (H), medium (M), and low (L). The articles on "Quantitative representation of risk" and "Qualitative representation of risk" describe other methods for representing risk.

*A countermeasure* is an action taken or a physical capability provided whose principal purpose is to reduce or eliminate one or more vulnerabilities or to reduce the frequency of attacks. *Consequence mitigation* is the preplanned and coordinated actions or system

**TABLE 1 Risk Assessment Methods**

| Method | Scope |
|---|---|
| Safety/review audit | Identifies equipment conditions or operating procedures that could lead to a casualty or result in property damage or environmental impacts |
| Checklist | Ensures that organizations are complying with standard practices |
| What-If | Identifies hazards, hazardous situations, or specific accident events that could result in undesirable consequences |
| Hazard and operability study (HAZOP) | Identifies system deviations and their causes that can lead to undesirable consequences and determine recommended actions to reduce the frequency and/or consequences of the deviations |
| Preliminary hazard analysis (PrHA) | Identifies and prioritizes hazards leading to undesirable consequences early in the life of a system. It determines recommended actions to reduce the frequency and/or consequences of the prioritized hazards. This is an inductive modeling approach |
| Probabilistic risk analysis (PRA) | Quantifies risk, and was developed by the nuclear engineering community for risk assessment. This comprehensive process may use a combination of risk assessment methods |
| Failure modes and effects analysis (FMEA) | Identifies the components (equipment) failure modes and the impacts on the surrounding components and the system. This is an inductive modeling approach |
| Fault tree analysis (FTA) | Identifies combinations of equipment failures and human errors that can result in an accident. This is an deductive modeling approach |
| Event tree analysis (ETA) | Identifies various sequences of events, both failures and successes that can lead to an accident. This is an inductive modeling approach |
| The Delphi Technique | Assists to reach consensus of experts on a subject such as project risk while maintaining anonymity by soliciting ideas about the important project risks that are collected and circulated to the experts for further comment. Consensus on the main project risks may be reached in a few rounds of this process [3]. |
| Interviewing | Identifies risk events by interviews of experienced project managers or subject-matter experts. The interviewees identify risk events based on experience and project information |
| Experience-based identification | Identifies risk events based on experience including implicit assumptions |
| Brain storming | Identifies risk events using facilitated sessions with stakeholders, project team members, and infrastructure support staff |

features that are designed to reduce or minimize the damage caused by attacks (consequences of an attack), support and complement emergency forces (first responders), facilitate field-investigation and crisis management response, and facilitate recovery and reconstitution. Consequence mitigation may also include steps taken to reduce short- and long-term impacts, such as providing alternative sources of supply for critical goods and services. Mitigation actions and strategies are intended to reduce the consequences (impacts) of an attack, whereas countermeasures are intended to reduce the probability that an attack will succeed in causing a failure or significant damage.

**TABLE 2 Likelihood Categories for a Risk Matrix**

| Category | Description | Annual Probability Range |
|---|---|---|
| A | Likely | ≥0.1 (1 in 10) |
| B | Unlikely | ≥0.01 (1 in 100) but <0.1 |
| C | Very unlikely | ≥0.001 (1 in 1,000) but <0.01 |
| D | Doubtful | ≥0.0001 (1 in 10,000) but <0.001 |
| E | Highly unlikely | ≥0.00001 (1 in 100,000) but <0.0001 |
| F | Extremely unlikely | <0.00001 (1 in 100,000) |

**TABLE 3 Consequence Categories for a Risk Matrix**

| Category | Description | Examples |
|---|---|---|
| I | Catastrophic | Large number of fatalities and/or major long-term environmental impact |
| II | Major | Fatalities and/or major short-term environmental impact |
| III | Serious | Serious injuries and/or significant environmental impact |
| IV | Significant | Minor injuries and/or short-term environmental impact |
| V | Minor | Only first aid injuries and/or minimal environmental impact |
| VI | None | No significant consequence |

**TABLE 4 Example Consequence Categories for a Risk Matrix in 2003 Monetary Amounts (US $)**

| Category | Description | Cost |
|---|---|---|
| I | Catastrophic loss | ≥$10,000,000,000 |
| II | Major loss | ≥$1,000,000,000 but <$10,000,000,000 |
| III | Serious loss | ≥$100,000,000 but <$1,000,000,000 |
| IV | Significant loss | ≥$10,000,000 but <$100,000,000 |
| V | Minor loss | ≥$1,000,000 but <$10,000,000 |
| VI | Insignificant loss | <$1,000,000 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Probability category | **A** | L | M | M | H | H | H |
| | **B** | L | L | M | M | H | H |
| | **C** | L | L | L | M | M | H |
| | **D** | L | L | L | L | M | M |
| | **E** | L | L | L | L | L | M |
| | **F** | L | L | L | L | L | L |
| | | **VI** | **V** | **IV** | **III** | **II** | **I** |
| | Consequence category | | | | | | |

**FIGURE 1** Example risk matrix.

Risk management entails decision analysis for a cost-effective reduction of risk within available resources. The benefit of a risk mitigation action can be assessed as follows:

$$\text{Benefit} = \text{unmitigated risk} - \text{mitigated risk} \tag{2}$$

The benefit minus the cost of mitigation can be used to justify the allocation of resources. The benefit-to-cost ratio can be computed, and may also be helpful in decision making. The benefit-to-cost ratio can be computed as

$$\text{Benefit-to-cost ratio } (B/C) = \frac{\text{Benefit}}{\text{Cost}} = \frac{\text{Unmitigated risk} - \text{Mitigated risk}}{\text{Cost}} \tag{3}$$

The cost in Eq. (3) is the cost of the mitigation action or countermeasure. Ratios greater than one are desirable. In general, the larger the ratio, the better the mitigation action. Internal rate of return can be used instead of benefit-to-cost ratios [1]. Assuming $B$ and $C$ random variables with normal probability distributions, a benefit–cost index ($\beta_{B/C}$) can be defined as follows:

$$\beta_{B/C} = \frac{\mu_B - \mu_C}{\sqrt{\sigma_B^2 + \sigma_c^2}} \tag{4}$$

where $\mu$ and $\sigma$ are the mean and standard deviation. In the case of lognormally distributed $B$ and $C$, benefit–cost index can be computed as

$$\beta_{B/C} = \frac{\ln\left(\frac{\mu_B}{\mu_C}\sqrt{\frac{\delta_C^2+1}{\delta_B^2+1}}\right)}{\sqrt{\ln[(\delta_B^2+1)(\delta_C^2+1)]}} \tag{5}$$

where $\delta$ is the coefficient of variation. The probability of not realizing the benefits ($P$) can be computed as

$$P = 1 - \Phi(\beta_{B/C}) \tag{6}$$

where $\Phi$ is the cumulative distribution function of the standard normal. In the case of mixed distributions or cases involving basic random variables of $B$ and $C$, the advanced second moment method or simulation method can be used [1]. In cases where benefit is computed as revenue minus cost, benefit might be correlated with cost requiring the use of other methods [1].

The following are four primary ways available to deal with risk within the context of a risk management strategy:

- risk reduction or elimination;
- risk transfer, for example, to a contractor or an insurance company;
- risk avoidance; and
- risk absorbance or pooling.

*Risk communication* can be defined as an interactive process of exchange of information and opinion among stakeholders such as individuals, groups, and institutions. It often involves multiple messages about the nature of risk or expressing concerns, opinions, or reactions to risk managers or to legal and institutional arrangements for risk management. Risk communication greatly affects risk acceptance and defines the acceptance criteria for safety.

## 3 TERRORISM RISK ANALYSIS

Terrorism can be assessed at various levels, starting with a facility and its assets, a region, a sector, and a national territory. For example, considering risk analysis for an asset requires examining several threat-asset scenarios [4, 5]. Each individual risk for a scenario can be evaluated as the product or combination of a specific defined consequence, expressed as a numerical range (e.g. dollars) and the probability range that the specific consequence will occur. This results in a mean value for the risk, and can be reevaluated to produce upper and lower bounds using uncertainty analysis techniques [3]. For asset screening, qualitative measures of probability and consequence can be combined on a risk matrix. For most postulated adversary actions, there is a spectrum of possible outcomes (consequences), each with an associated probability range. Terrorism risk analysis can be performed using a scenario-based approach. The probability range associated with a specific consequence range is the product of the frequency of attacks by adversaries and a series of individual conditional probability ranges associated with the chain of events that occur after the attack. These probability ranges are determined based on the various capabilities that the asset has for dealing with or avoiding the adversary action. These capabilities may be consequence mitigation systems or threat response or avoidance actions (countermeasures), which can be pictured as nodes along an event tree. The consequence ranges associated with a successful attack by an adversary on an asset, combined with the probability range associated with each consequence, define the risk range. The risks associated with each of these probability range/consequence range pairs can be added (given that they are measured in the same units, e.g. dollars) to obtain the risk for a postulated adversary action. Similarly, the overall risk for a spectrum of postulated adversary actions is the sum of the risks for each individual action. Figure 2 schematically shows the relationship of risk, in terms of the above features, and the spectrum of potential countermeasures and consequence mitigation strategies. Figure 3 presents a primary structure of risk analysis for critical assets. The figure shows a threat block on the left that targets asset or sector vulnerabilities protected by existing countermeasures. If a threat materializes and succeeds, it might lead to failures that might pass through existing consequence mitigation measures leading to consequences.

## 4 UNIQUE FEATURES OF TERRORISM RISK ANALYSIS

Terrorism risk analysis includes some features of typical probabilistic risk analysis (PRA) methods, in which probability and consequence ranges are determined numerically. However, it relies heavily on many of the features of traditional qualitative approaches

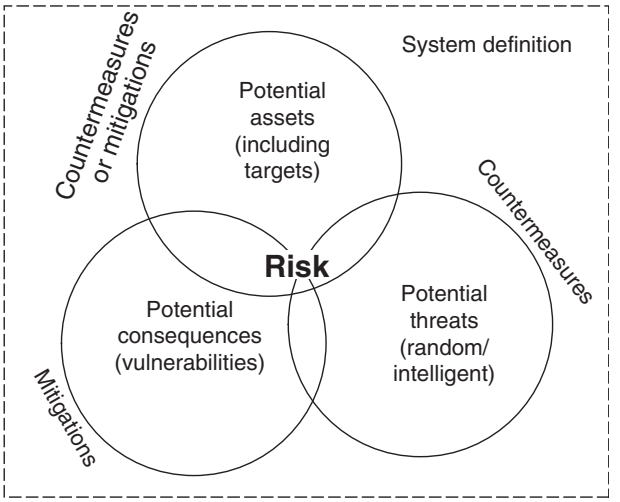



**FIGURE 2** Schematic of the approach to risk analysis.

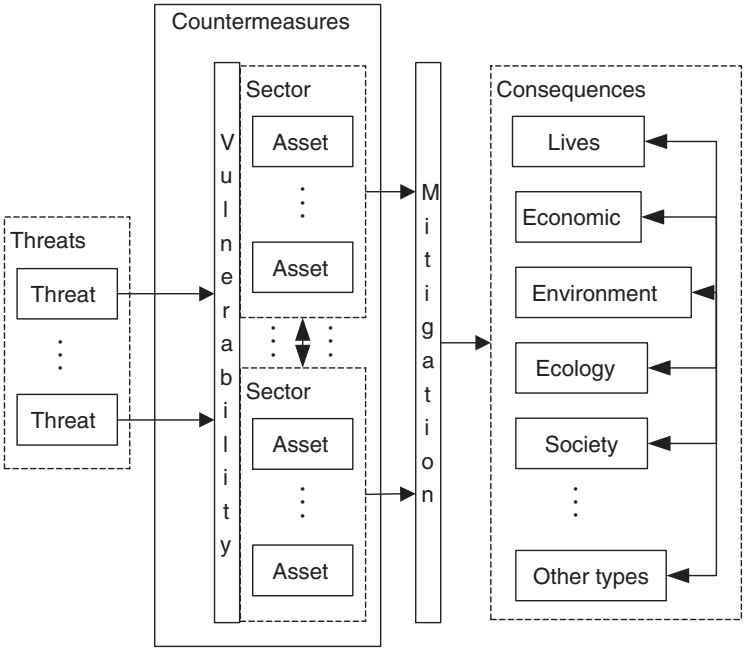



**FIGURE 3** A primary structure for risk analysis.

to balance the time and resources required to do the analysis with the need for numerical risk measures that can be used to inform resource allocation decisions. Some of the unique features of risk analysis related to assets, threats, and countermeasures and consequence mitigation are summarized in Table 5.

**TABLE 5 Unique Features of Risk Analysis for Asset Protection from Adversary Threats**

| Features | Unique Characteristics |
|---|---|
| Risk analysis framework | Should be performed accounting for the perspectives of adversaries as well as the perspectives of defenders. And as a multilevel analysis ranging from an asset, to multiassets, to a sector, and to multisectors to sufficiently account for interdependencies that may affect the risks pertinent to the decision being made |
| Asset (target) features | Include attractive assets, critical assets, soft assets, assets with vulnerabilities that are sufficiently known to adversaries |
| Assets (targets) selected by adversaries | Include high consequence assets (or scenarios) with high probability of success |
| Threat features | Include the dynamic nature of threats, threat types and probabilities; their nonrandomness but deliberateness using design basis threats; possibly being of unknown or unknowable types |
| Threat–asset dependencies | Include dynamically responding to asset protection using countermeasures and consequence mitigation |
| Ingenuity of adversaries | Include converting assets to threats by capitalizing on the efficiency of infrastructures, for example:<br>Transportation efficiency by converting airplane assets into explosive weapons<br>Mail efficiency by using mail items for bioagent delivery<br>Other efficient infrastructure systems include power and information systems |
| Capabilities of adversaries | Include the ability to select targets and accurately deliver the weapon to them and the ability to adapt to countermeasures to redirect the weapon to another target |
| Asset vulnerabilities | Include identifying targets outside the system boundaries to exploit system vulnerabilities through system dependencies |
| Consequences | Are broadly defined to include public health, economic loss, loss of vital commodities, interruption of government operation, and national psyche |
| Asset and sector interdependencies | Include interdependencies in functionality and subsequently in consequences |
| Decision analysis | Includes trade-offs based on national security, safety, and economics |
| Information flow | Is a two-way flow of defenders acquiring knowledge about the adversaries; adversaries acquiring knowledge about the assets, countermeasures, and consequence mitigation plans |
| Countermeasures | Include countermeasures at the asset level and metacountermeasures at the multiasset, sector, and multisector levels. Countermeasures reduce the probability of selection of an asset as well as the probability of success of an attack |
| Consequence mitigation plans | Include mitigation at the local level and metamitigations at the state, regional, and national level. Mitigation actions reduce consequences |

## 5 ANALYSIS OBJECTIVES, ASSETS, AND SYSTEM BOUNDARIES

One of the first steps in a risk analysis is to define the objectives. The objectives may include

- understanding the nature of the risks to define and optimize the allocation of resources for countermeasures and consequence mitigation strategies;
- maximizing threat risk reduction benefits and utility to stakeholders; and/or
- understanding the nature of the risks for better communication with stakeholders.

Risk analysis requires a systems framework in order to achieve the stated objectives. Such a view of risk analysis requires structuring and formulating a problem or approaching a design with the following in mind:

1. The structure should be within a systems framework.
2. The approach should be systematic and should capture all critical aspects of the problem or decision situation.
3. Uncertainties should be assessed and considered.
4. An optimization scheme should be constructed for the utilization of available resources including maximizing benefits and utility to stakeholders. The definition of a system is therefore driven by a well-stated description of the objectives of the risk analysis.

After the objectives have been defined, the next step is to identify potential critical assets for further screening. This is done using judgment and experience. Taxonomy of potentially critical assets is provided in Table 6 for illustration purposes. The taxonomy is provided under selected headings and could be expanded hierarchically according to asset categories and sectors.

Identifying critical assets requires defining the features that define criticality. Categories of critical assets are relatively broad and inclusive. The criticality of an asset should be based on features such as the impact of total destruction of or significant damage to an asset on

- public service and the operation of government;
- the local, regional, and national economy;
- surrounding population;
- national security; and
- environment.

Note that critical assets are identified primarily on the basis of the consequences of a successful attack by an adversary rather than the probability that the attack will be successful. However, other asset features that should be considered include

- asset softness, that is, accessibility and inability to limit it;
- softness of targets within an asset; and
- other specific features of these targets.

**TABLE 6 Asset Taxonomy**

| Agriculture and Food | Information and Telecommunications | Banking and Finance |
|---|---|---|
| Supply | Public switched telecommunications network (PSTN) | Physical facilities (buildings) |
| Processing | Internet | Operations centers |
| Production | Switch/router areas | Regulatory institutions |
| Packaging | Access tandems | Physical repositories |
| Storage | Fiber/copper cable | Telecommunications networks |
| Distribution | Cellular, microwave, and satellite systems | Emergency redundancy service areas |
| Transportation | Operations, administration, maintenance and provisioning systems | **Chemical/Hazardous Materials Industry** |
| **Water** | Network operations centers | Manufacturing plants |
| Dams, wells, reservoirs, and aqueducts | Underwater cables | Transport systems |
| Transmission pipelines | Cable landing points | Distribution systems |
| Pumping stations | Collocation sites, peering points, and telecom hotels | Storage/stockpile/supply areas |
| Sewer systems | Radio cell towers | Emergency response and communications systems |
| Treatment facilities | **Energy** | **Postal and Shipping** |
| Storage facilities | **Electricity (Nonnuclear)** | Processing facilities |
| **Public Health** | Hydroelectric dams | Distribution networks |
| National strategic stockpile | Fossil-fuel electric power generation plants | Air, truck, rail, and boat transport systems |
| National institutes of health | Distribution systems | Security |
| State and local health departments | Key substations | **National Monuments and Icons** |
| Hospitals | Communications | National parks |
| Health clinics | **Oil and Natural Gas** | Monuments |
| Mental health facilities | Offshore platforms | Historic buildings |
| Nursing homes | Refineries | **Nuclear Power Plants** |
| Blood supply facilities | Storage facilities | Commercial owned/operated |
| Laboratories | Gas processing plants | Government owned/operated |
| Mortuaries | Product terminals | Physical facilities |
| Pharmaceutical stockpiles | Pipelines | Spent fuel storage facilities |
| **Emergency Services** | **Transportation** | Safety/security systems |
| Fire houses | Aviation | **Dams** |
| Rescue | Railways | Large |
| Emergency medical services | Highways | Small |
| Law enforcement | Trucking | Government owned |
| Mobile response | Busing | Private/corporate owned |
| Communications systems | Bridges | **Government Facilities** |

**TABLE 6 (*Continued*)**

| Agriculture and Food | Information and Telecommunications | Banking and Finance |
|---|---|---|
| **Defense Industry Base** | Tunnels | **National Security Special Events** |
| Supply systems | Borders | **Commercial Assets** |
| | Seaports | Prominent commercial centers |
| | Pipelines | Office buildings |
| | Maritime | Sports centers/arenas |
| | Mass transit | Theme parks |
| | | Processing/service centers |

The definition of the system and the establishment of system boundaries should be based on an analysis of its functional and/or performance requirements. A description of a system may be a combination of functional and physical elements. For example, the system to be considered for a particular highway bridge should include both its structural design characteristics (e.g. a steel span across a river that is a quarter mile wide) and its functional capability (e.g. carry 1000 vehicles per hour). A system may be divided into subsystems that interact with each other. For example, the elements of a petroleum refinery are highly interdependent, such that each unit might constitute a subsystem within a system under analysis. Additional detail leads to a description of the physical elements, components, and various aspects of the system. The analysis objectives drive the system definition and boundaries. Buffer zones should be included in the definition of the systems, so that their effect on threat success and consequence mitigation can be appropriately assessed.

## 6 UNIQUE FEATURES OF THREAT

The analysis of threats is generally the most uncertain part of risk analysis for homeland security. When considering events such as equipment failures, human errors, or natural disasters an extensive body of historical experience exists that can be used to establish the frequency or probability range of various initiating events. Although, unfortunately, there is also an extensive history of terrorist and other adversarial acts, the nature of these events is constantly changing, so historical experience provides less guidance in trying to predict the future. The following characteristics make terrorist and other adversarial threats unique relative to other risk contributors:

- Terrorist and other adversarial threats are focused rather than random events. This is often characterized as “intelligent versus random threats”. Accidents and natural disasters occur in a random pattern that is often statistically predictable. On the other hand, prediction of the frequency range of a specific adversary action against a specific target should be based less on historical data and more on an analysis of factors such as

  - prevailing political situation;
  - objectives and motivations of adversaries with access to or near the target;
  - attractiveness of the target to the adversaries;
  - number and type of adversaries with sufficient access to the target to carry out the threat;
  - weapons and other capabilities available to the adversaries;
  - local security surveillance level;
  - quality of intelligence information.
- Unlike accidents and natural disasters, adversaries are able to adapt to changing circumstances. This is often characterized as "dynamic versus static threats". For example,
  - hardening of a target by improving countermeasures that adversaries are aware of can drive them to select another target;
  - changing perceptions of the impact of damage to various targets and the effectiveness of various types of attacks can lead to changes in terrorist and other adversarial strategies;
  - terrorists/adversaries typically try to accumulate more material and capability than the minimum necessary to achieve their desired consequences.
- Even "unsuccessful" attacks can have a significant consequence. For example, an attempt to shoot down a commercial airliner in the United States could have a significant impact on the airlines and the US economy even if the attack is not successful.

Efficient systems for creating threats, delivering threats, and propagating consequences should be identified, such as transportation systems, mail systems, computer networks, and power systems. Adversaries could capitalize on the efficiencies of infrastructure systems to create/advance/transmit/propagate threats. Threats could be classified as threats by the system, through the system, and to the system.

Threats can be classified by type as shown in Table 7. Analyzing threats over a spectrum from low to high enables analysts to focus their attention and resources. Figure 4 shows such a threat spectrum based on threat magnitude measured in terms of its potential impact. Design basis threats can be used to address threats for which an individual asset owner is expected to provide countermeasures and/or consequence mitigation; whereas regional or national countermeasures are necessary for large-scale threats, for example, weapons of mass destruction. For the region in between these two extreme categories, risk-informed decision making should be used to decide on appropriate countermeasures and consequence mitigation strategies.

## 7 SECTION SCOPE AND OUTLINE

This article starts with a presentation of overall frameworks for analyzing and assessing risks for homeland security purposes, and for critical infrastructure and key resource protection. The article also includes various risk analysis methods, such as logic trees: event, fault, success, attack, probability, and decision trees; scenario analysis, cognitive maps,

**TABLE 7 Threat Types**

| Threat Type | Delivery Mode | Weapon/Agent | Quantity/Quality |
|---|---|---|---|
| Chemical | Outdoor dispersal | Ricin | Potent |
| | | Mustard gas | Potent |
| | Crop duster | VX | Potent |
| | | Chlorine gas | Potent |
| | Propelled missile | Any of the above | Potent |
| | Postal mail | Ricin | Potent |
| Biological | Outdoor dispersal | Anthrax | Potent |
| | | SARS | Potent |
| | Postal mail | Anthrax | Potent |
| | Food buffets | Hepatitis | Potent |
| | | Salmonella | Potent |
| | Missile | Any of the above | Potent |
| Radiological | Standard deployment | Dirty bomb | Strong |
| | | Radiological release | Strong |
| Nuclear | Standard deployment | Improvised nuclear device | 2 kt |
| | | Strategic nuclear weapon | 100 kt |
| Explosive | Standard deployment | Backpack bomb | 10 lb Trinitrotoluene (TNT) |
| | | Propelled missile | 50 t |
| | Truck | Fertilizer bomb | 200 lb |
| | | | 500 lb |
| | | | 1000 lb |
| | | | 4000 lb |
| | Boat | C4 | 200 lb |
| | Airplane | Jet fuel | 5000 ga |
| Sabotage | Physical | Cut power cable | Not applicable |
| | | Cut bolts | Not applicable |
| | | Improper operation or maintenance | Not applicable |
| | Cyber | Providing unauthorized access | Obvious |
| Cyber | Physical | Cut SCADA cable | Not applicable |
| | | Magnetic weapons | Power units |
| | Cyber | Worm virus | Obvious |

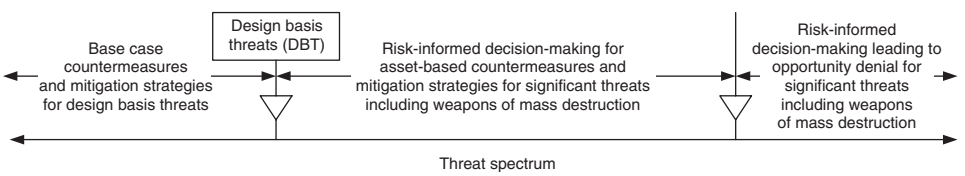



**FIGURE 4** Threat spectrum.

and concept maps; Bayesian networks; probabilistic risk assessment; game theory; and representation of risk. National interdependence models of infrastructure are discussed. High consequence threats, such as electromagnetic pulse, nuclear, biological, chemical, and high-grade explosives are discussed. Also, special chapters on bioterrorism, cyber security, risk perception, and soft failure modes are provided. Regulations and standards relating to risk analysis are discussed and their features are summarized. Also, methods for policy development are discussed.

The article covers various analytical steps needed for performing threat analysis, vulnerability assessment, consequence analysis with infrastructure interdependencies and social and psychological issues, systems analysis, multiobjective decision analysis including risk-based prioritization, and risk communication. Uncertainty modeling and analysis are also introduced and discussed. Countermeasures, including robustness, resilience and security, and consequence mitigation methods are discussed with a special presentation relating to deterrence and defeating surprise.

Experiences from terrorism risk analysis from the insurance industry including the economics of terrorism and risk transfer are discussed. Regional risk analysis and protection are also covered.

Terrorism risk analysis requires data and information. Data scarcity and unavailability require the use of expert opinion elicitation. Data sources for threat analysis are needed [2]. Treads in threats and their organizations and emergence, and terrorism databases are also discussed and covered. The legal aspects of information security needed for risk analysis are discussed.

## REFERENCES

1. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*, Chapman and Hall/CRC Press, FL.
2. Ayyub, B. M., and Klir, G. J. (2006). *Uncertainty Modeling and Analysis in Engineering and the Sciences*. Chapman and Hall/CRC Press, Boca Raton, FL.
3. Ayyub, B. M. (2001). *Elicitation of Expert Opinions for Uncertainty and Risks*. CRC Press, Boca Raton, FL.
4. Ayyub, B. M., McGill, W. L., and Kaminskiy, M., (2007). Critical asset and portfolio risk analysis for homeland security: an all-hazards framework, *Risk Anal. Int. J. Soc. Risk Anal.*, **27**(3), 789–801.
5. McGill, W. L., Ayyub, B. M., and Kaminskiy, M., (2007). A quantitative asset-level risk assessment and management framework for critical asset protection, *Risk Anal. Int. J. Soc. Risk Anal.*, **27**(5), 1265–1281.

## FURTHER READING

Kumamoto, H., and Henley, E. J. (1996). *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed. IEEE Press, New York.

Modarres, M. (1993). *What Every Engineer Should Know About Reliability and Analysis*. Marcel Dekker, Inc., New York.

Modarres, M., Kaminskiy, M., and Krivstov, V. (1999). *Reliability Engineering and Risk Analysis: A Practical Guide*, Marcel Decker Inc., New York.

# RISK ANALYSIS FRAMEWORKS FOR COUNTERTERRORISM*

JAMES SCOURAS
*Defense Threat Reduction Agency, Fort Belvoir, Virginia*

GREGORY S. PARNELL
*Department of Systems Engineering, United States Military Academy, West Point, New York*

BILAL M. AYYUB
*Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland*

ROBERT M. LIEBE
*Innovative Decisions Inc., Vienna, Virginia*

## 1 INTRODUCTION

Although there are numerous definitions of risk concepts in use in the risk analysis community, the great majority of these definitions recognize the same common elements. We focus on these essential elements to develop straightforward definitions of risk, risk analysis, risk assessment, risk management, threat, vulnerability, and consequence. To further clarify these terms, we also discuss the relationships among them. We also expand some of the classic questions addressed by risk assessment and risk management to more explicitly address terrorism.

A framework is a conceptual or procedural structure used to address complex issues. A risk framework can facilitate both internal and external risk communication and enable risk analysis involving diverse threats and multiple participants. We analyze a selection of risk frameworks to develop a set of tasks that would be included in a comprehensive framework and against which a particular framework could be evaluated: (i) identify goals and objectives, (ii) define system, (iii) assess threats, (iv) assess vulnerabilities, (v5) assess consequences, (vi) assess baseline risk, (vii) identify risk management options, (viii) analyze benefits and costs, (ix) make decisions, (x) communicate risks, (xi) implement risk management actions, and (xii) monitor risk management actions.

The United States is engaged in a global war on terrorism with domestic and international battlefronts. US military and civilian leaders have defined this conflict as the "Long War" to convey the expectation that the terrorist threat will be with us for years—possibly decades—and the war will require significant resources and resolve to win [1].

There is a consensus among analysts and policy makers that risk management provides the proper framework for defending against terrorism. We need to understand the threats, reduce our vulnerabilities, and prevent terrorists from achieving the

*The views expressed in this article represent those of the authors; they do not necessarily represent the views of any governmental or commercial entity.

consequences they seek with attacks on the United States and worldwide. The US Government Accountability Office (GAO) advocates adopting a risk management approach universally across the federal government [2]:

> After threat, vulnerability, and criticality assessments have been completed and evaluated in this risk-based decision process, key actions can be taken to better prepare ourselves against potential terrorist attacks. Threat assessments alone are insufficient to support the key judgments and decisions that must be made. However, in conjunction with vulnerability and criticality assessments, leaders and managers will make better decisions based on this risk management approach. If the federal government were to apply this approach universally and if similar approaches were adopted by other segments of society, we could more effectively and efficiently prepare in-depth defenses against acts of terrorism against our country.

This article focuses on risk frameworks, a first step toward coordinated risk management approaches. We begin with discussions of essential risk terminology and the relationships among basic concepts, as well as several important practical considerations in risk analysis. We then introduce the concept of a risk framework and summarize our research on 17 diverse frameworks. We illustrate two types of risk frameworks: procedural and methodological. On the basis of our research on the risk frameworks, we identify 12 risk framework elements. We then describe each of these elements and how they can be used to evaluate risk frameworks.

## 2 DEFINITIONS OF RISK ANALYSIS TERMS

It is important to begin with a clear understanding of the terminology of risk analysis. Here, we limit ourselves to definitions of risk, the major components of risk analysis, and the elements of risk assessment. There are a multitude of definitions in use for each of these terms. Our analysis of these definitions leads us to the observation that much effort can be expended in debating the nuances of alternative definitions to little avail. The definitions we propose are intended to be simple in that they convey the essential elements of the term, with as little extraneous baggage as possible.

*Risk* is the potential for loss or harm due to the likelihood of an unwanted scenario and its potential adverse consequences. There are two essential features of risk that are embedded in this definition. First, the consequences that contribute to risk are negative. (There is no short-term financial risk associated with winning the lottery.) Secondly, both the scenario (sequence of future states) and its associated consequences are uncertain. (There is no risk that governments will abandon taxation.) We use the term *likelihood* (rather than *probability*) to acknowledge that risk can be represented qualitatively or quantitatively.

*Risk assessment* is a systematic analytic process for describing the nature and magnitude of risk associated with a scenario, including consideration of relevant uncertainties. When we consider natural hazards (e.g. hurricanes) and engineered systems (e.g. nuclear reactor accidents), the risk assessment objective is to provide, to the extent practical, a scientific and analytically sound basis for answering the following questions: What can go wrong? How can it happen? What are the potential consequences if it does happen? How likely is it to happen? However, these questions do not emphasize the unique human aspect of the terrorist threat: terrorists are intelligent and motivated adversaries who can

adapt to their experiences, environment, and anticipations of the future. Thus, when we consider terrorism, we propose a set of more explicit questions:

1. What adversaries threaten US interests?
2. What are their motivations, capabilities, and intentions?
3. What vulnerabilities could be exploited in an attack?
4. What are the potential consequences of an attack?
5. How likely is an attack to occur?

*Risk management* is the process of constructing, evaluating, selecting, implementing, and monitoring actions to alter levels of risk. For natural and engineered system hazards, it addresses the questions:

1. What can we do?
2. What should we do?
3. What are the results of our actions? Again, the terrorist is an intelligent adversary, which requires we make explicit the need to answer an additional question:
4. What can be done to account for the response of an adaptive, intelligent adversary?

The goal of risk management is scientifically sound, cost effective, integrated actions, including providing information (i.e. risk communication) that transfer, mitigate, or accept risks while taking into account social, cultural, ethical, political, economic, and legal considerations. Because of these additional considerations, which can significantly constrain the risk management actions available and their evaluations, we refer to homeland security decisions as *risk informed*, rather than *risk based*.

It is worth noting that some risk professionals use the term *risk management* to encompass *risk assessment* and *risk control*, where *risk control* is what we have defined as risk management in this article [3]. This is a useful taxonomy of concepts, but (unfortunately) not as widely used in the community of risk analysts and practitioners.

As with many terms in English, *risk analysis* has more than one meaning. One definition has risk analysis encompassing the full spectrum of activities, processes, and phenomena related to risk, including all of risk assessment and risk management, as depicted in Figure 1a. This was the meaning intended when the term was used in this article. Although risk communication is often called out as an additional separate element of risk analysis, we do not do so here because it is integral to both risk assessment and risk management.

A related but distinct definition holds risk analysis to be the process of separating the whole of risk into its component parts (e.g. threat, vulnerability, and consequence). As such, it supports both risk assessment and risk management as depicted in Figure 1b.

A *threat* is a scenario that could result in loss or harm. Terrorist threats are intentional. More generally, the term *hazard* encompasses terrorist and other intentional threats, as well as unintentional events such as accidents (e.g. nuclear power plant failures) and natural phenomena (e.g. hurricanes). Risk management of counterterrorism must include consideration of all hazards (AH) because (i) nonterrorist threats might not pose the greatest risks or the greatest opportunities for risk mitigation with limited resources and (ii) many risk management actions (e.g. stockpiling vaccines) will reduce both terrorist and nonterrorist risks and should be evaluated on that broader basis.

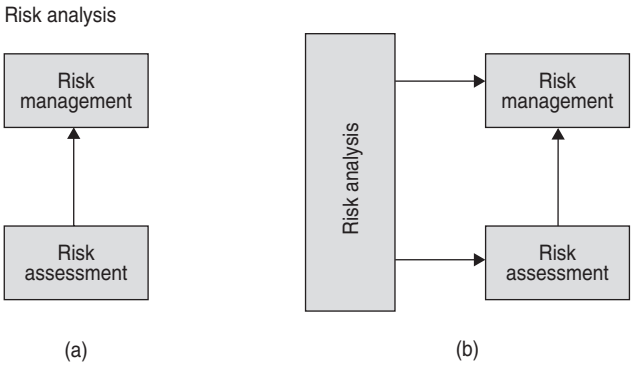



**FIGURE 1** Alternative taxonomies of risk analysis, risk assessment, and risk management: (a) risk analysis *encompasses* risk assessment and risk management and (b) risk analysis *supports* risk assessment and risk management.

A *vulnerability* is an attribute of a system that could be exploited by an adversary to cause loss or harm or, similarly, a weakness of a system that could result in loss or harm in the event of a terrorist attack, an accident, or a natural phenomenon.

A *consequence* is an adverse outcome. Consequences include the tangible and intangible, the quantifiable and unquantifiable: mortality, morbidity, economic loss, psychological and societal damage, and myriad other forms of loss and harm. Consequences can cascade through interdependent economic infrastructures and can persist, or even increase, far into the future.

## 3 RELATIONSHIPS AMONG THREAT, VULNERABILITY, AND CONSEQUENCE

Two depictions of the relationships among threat, vulnerability, consequence, and risk are shown in Figures 2 and 3.

Figure 2 shows risk in a Venn diagram at the intersection of threat, vulnerability, and consequence. This widely used representation is meant to convey that if any one of these elements is absent, there is no risk. For example, even with a recognized vulnerability and definite severe consequences of an attack that exploits that vulnerability, without a plausible threat there is no risk. As an illustration, there is (essentially) no risk of a UK nuclear attack against the United States, even though we are defenseless against such an attack and the consequences would be horrific.

Note that while our definition of risk has two components, likelihood and consequences, Figure 2 shows three—threat, vulnerability, and consequence. These are reconciled in probabilistic risk analyses with the following definitions:

$$\text{Risk} = \text{threat} \times \text{vulnerability} \times \text{consequence} \tag{1}$$

where threat is the probability of an attempted attack, vulnerability is the probability of successful attack, given an attempted attack, and consequence is the consequences of a successful attack.

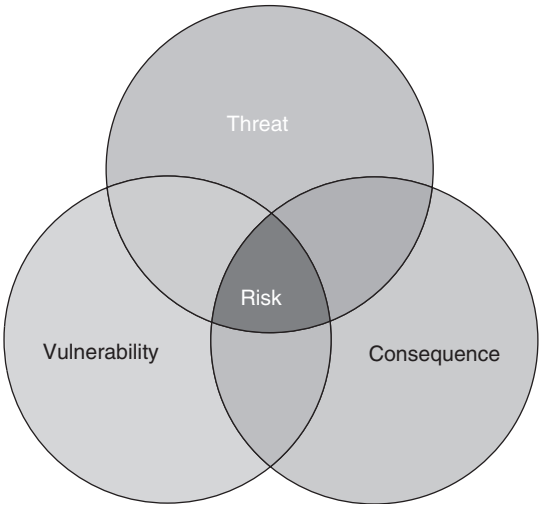



**FIGURE 2** Venn diagram representation of threat, vulnerability, consequence, and risk.

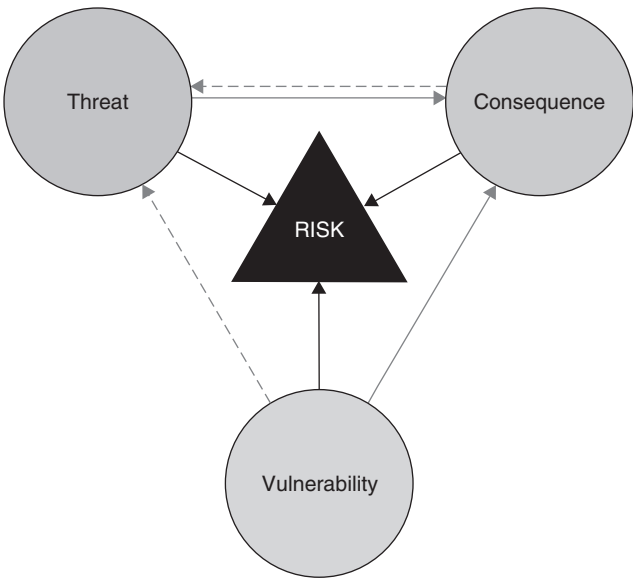



**FIGURE 3** Information flow among threat, vulnerability, consequence, and risk.

With these assignments, we can identify likelihood as the probability of a successful attack, the product of threat and vulnerability.

The Venn diagram representation of risk can be misleading. By its symmetry, it suggests that threat, vulnerability, and consequence are equal and independent elements of risk. Figure 3 breaks this symmetry by depicting the flow of information among threat, vulnerability, consequence, and risk, thereby making explicit their interdependencies.

The black arrows from threat, vulnerability, and consequence to risk indicate that all three elements contribute to risk. The solid red arrows indicate that both threat and vulnerability contribute to consequence. The dashed red arrows indicate that intelligent adversaries' (IA) perceptions of vulnerability and consequence influence their thinking, and thus the threat. (Readers are requested to refer the online version for color indication.) These arrows would not be present in an analysis of unintentional hazards.

## 4 INTRODUCTION TO RISK FRAMEWORKS

With this set of definitions and discussion, we now turn to the utility of, indeed *need for*, a risk framework to help assess and manage risk. We use the term *framework* to mean a conceptual or procedural structure used to address complex issues.

There is no doubt that the question of how to address the risks of terrorism qualifies as a complex issue. Terrorism is characterized by multiple adversaries with opaque motivations, diverse threats, learning, and adaption—all of which are evolving in uncertain ways over time. Counterterrorism must address multiple stakeholders with differing perceptions and priorities; profound uncertainties in threats; vulnerabilities of complex interdependent systems; myriad direct and indirect consequences; and the challenges of risk communication to diverse stakeholders.

In general terms, conceptual frameworks are simpler than procedural frameworks. Although both conceptual and procedural frameworks identify the major risk analysis tasks, conceptual frameworks may or may not explicitly specify an order to these tasks or the flow of information among them, and do not specify techniques or provide specifics with respect to data and measures. Procedural frameworks are more detailed and prescriptive than conceptual frameworks. Procedural frameworks do indicate the order of the tasks, the flow of information among them, can specify the techniques used to perform each task, and may or may not prescribe the data and measures used. Of course, many risk frameworks employ a mixture of features of both types of frameworks.

A risk framework makes a number of contributions to risk analysis. In particular, both conceptual and procedural frameworks serve as vehicles for risk communication. Internal risk communication among analysts, stakeholders, and decision makers requires a common terminology and understanding of the risk analysis process often undertaken by multiple participants from diverse disciplines across many public and private organizations. Even for highly conceptual frameworks, the process itself of developing a risk framework can be very helpful in hammering out differences in terminology and in refining the objectives, scope, and methodology of a risk analysis.

Moreover, for risk management decisions regarding policy, procedures, and the allocation of resources to gain acceptance and support, the results of risk analyses need to be communicated to stakeholders, the media, and the public. A graphical representation of a conceptual or procedural risk framework is an essential means toward this end.

The second major contribution of a risk framework applies more to procedural frameworks. The means of terrorist attack are diverse (e.g. biological, chemical, explosive, nuclear, and radiological), as are targets and consequences of attack. Since the goal of risk management is to effectively and efficiently allocate limited resources, risk analysis needs to compare risks across the full spectrum of possibilities. This requires the development of a risk framework that specifies the data to be collected, the techniques to be employed, and the measures to be used.

Finally, we observe that risk frameworks are either widely perceived to be useful or there is an unexplained compulsion to develop them. The ubiquity of risk frameworks is addressed in the following section.

## 5 SURVEY OF RISK FRAMEWORKS

In this section, we analyze a selection of common risk frameworks. These frameworks should be considered as an illustrative, rather than a representative sampling of all risk frameworks. One of our key screening criteria was clear evidence of use of the risk framework by public or private organizations. We offer the general observation that the variety of risk frameworks suggesting the development of a common risk framework for use throughout the homeland security enterprise is neither wise nor feasible.

Table 1 provides the following information about each risk framework: a reference number that includes the category of the framework, the framework name, the application area(s), the framework sponsor and/or developer, the user(s), and a reference (the full citation is provided in the references section). We have categorized the risk frameworks by the type of hazards they are designed to address: unintentional hazards (H), IA, and AH. The Coast Guard's Risk-Based Decision Making (RBDM) Guidelines is different from the other frameworks. RBDM has a list of 12 risk analysis techniques and 4 risk management techniques and provides information about when each of the techniques is appropriate.

Table 2 provides our analysis framework. We identify each task included in each of the frameworks and record the terminology used to describe it. By this process we have identified 12 distinct tasks that span the elements used in the 17 risk frameworks:

1. *Identify goals and objectives.* Identifying the goals and objectives of the risk framework is a useful task in problem framing. This can be achieved with a general objective (reduce risk of computer network attack) or multiple qualitative and quantitative objectives (see MORDA).
2. *Define system.* Another important framing or scoping task is defining the system. Because of the complex interconnections of systems, the system boundary may not be clear. For example, any component connected to the internet may be vulnerable to a cyber attack. Because of the system complexity, this task sometimes is required for critical asset identification. The assumption is that not all of the system is required to be considered—only the most critical assets.
3. *Assess threats.* This is a very important bounding task. Threats can be identified by specific sources (e.g. terrorist group T) or by classes of threats (domestic terrorist, foreign terrorist group, rogue nation–state, etc.). A common technique is the use of threat scenarios.
4. *Assess vulnerabilities.* Assessing the vulnerabilities is a very common task. This task usually requires significant understanding of the system (or at least the critical assets) and the full spectrum of the threats.
5. *Assess consequences.* Assessing consequences is a very common task. Identifying the potential types of consequences and their relationships is problematic. For example, will terrorist attacks of airplanes cause economic consequences of reduced discretional flying. If so, how much and for how long?

**TABLE 1 Surveyed Risk Frameworks**

| Reference Number | Name | Application(s) | Sponsor/Developer | User(s) | Reference |
|---|---|---|---|---|---|
| H-1 RBDM | Risk-Based Decision Making (RBDM) Guidelines | Marine safety prevention, preparedness, and response | Coast Guard | Public and private organizations (12 risk analysis tools and 4 risk management techniques) | Coast Guard, 2008 [4] |
| H-2 IRGC | IRGC Risk Governance Framework | Global risks (environmental, social, etc.) | International Risk Governance Council | International agencies | Renn, 2005 [5] |
| H-3 HVA | Highway Vulnerability Assessment | Highway vulnerabilities | Federal Highway Administration/SAIC | Highway administrators | SAIC, 2002 [6] |
| H-4 RFRM | Risk Filtering and Ranking Method | Highway infrastructures | State of Virginia/UVA | Highway administrators | Haimes et al., 2004 [7] |
| H-5 MRA | Revised Framework for Microbial Risk Assessment | Microbial risk assessment | United Nations/ILSI | Environmental protection offices | ILSI, 2000 [8] |
| H-6 DOT | DOT Hazardous Materials Transport | Transportation of hazardous materials | DOT/ICF Consulting | Public and private hazardous materials transporters | ICF, 2000 [9] |
| H-7 NASA | NASA | Safety and reliability of engineered systems | NASA | NASA risk analysts and risk managers | NASA, 2002 [10] |
| IA-1 RAMCAP | RAMCAP | Infrastructure critical asset protection | DHS/ASME | Public and private organizations | ASME, 2004 [11] |
| IA-2 FEMA | FEMA 452 | Terrorist threats against buildings | FEMA | Building developers and owners | FEMA, 2006 [12] |

| | | | | | |
|---|---|---|---|---|---|
| IA-3 DS | Digital Sandbox | Ranks relative risks for assets at a facility | Digital Sandbox | Public and private facility owners | Ware et al., 2002 Digital Sandbox, 2005 [13] |
| IA-4 ODP | ODP | Terrorist threat of WMD to facilities | Office of Domestic Preparedness | Federal, state, and local community organizations | ODP, 2003 [14] |
| IA-5 GAO | GAO Risk Management | Ports and other critical infrastructure | GAO | GAO to assess government frameworks | GAO, 2005 [15] |
| IA-6 MORDA | MORDA | Critical information systems | DoD/Innovative Decisions Inc. | DoD information assurance organizations | Buckshaw et al., 2005 [16] |
| IA-7 COMSEC | Canada COMSEC | Communications security | Canada | Information assurance organizations | Canada, 1999 [17] |
| AH-1 Orange Book | Orange Book | Risks to achieving organizational objectives | Her Majesty's Treasury | Public organizations in the United Kingdom | Her Magesty's Treasury, 2004 [18] |
| AH-2 CAPRA | CAPRA | Variety of hazards (safety, reliability, and security) | State of Maryland/University of Maryland | Public and private organizations | Ayyub, 2006 [19] |
| AH-3 Army | Army FM 100-14 | Operational missions and daily tasks | US Army | Army commanders and staff officers | Army, 1998 [20] |

**TABLE 2 Comparison of Risk Frameworks**

| Reference Number | Identify Goals and Objectives | Define System | Assess Threats | Assess Vulnerabilities | Assess Consequences | Assess Baseline Risk | Identify RM Options | Analyze Benefits and Costs | Make Decisions | Communicate Risks | Implement RM Actions | Monitor RM Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| H-1 RBDM | Some techniques | Some techniques | Boating safety hazards | Most techniques | Most techniques | Most techniques | Most techniques | Some techniques | Risk informed decisions | Not addressed | Four techniques identified | |
| H-2 IRGC | | Problem framing | Hazard identification | Exposure and vulnerability | Concern assessment (risk perception) | Risk characterization | Risk management | Option evaluation | Decision making | Center of framework | Implementation | |
| H-3 HVA | | Not addressed | Critical assets | Not addressed | Assess vulnerabilities | Assess consequences | Not addressed | Identify CM | Estimate CM cost | Review operational security planning | Not addressed | |
| H-4 RFRM | | Scenario identification and filtering | Bicriteria filtering Quantitative ranking | Multicriteria evaluation | Bicriteria filtering Quantitative ranking | Bicriteria filtering Quantitative ranking | Risk management | | Filtering | Interview survey | Operational feedback | |
| H-5 MRA | Water and foodborne pathogens | Not addressed | Pathogen characterization | Occurrence and exposure analysis | Health effects and dose response analysis | Exposure and host–pathogen profile | Not addressed | | | | | |
| H-6 DOT | Party involved | Hazmat transport activities | Conduct risk analyses with probabilities and consequences | | | | | Risk control points | Establish priorities, analyze cost/benefits, and decide | Party involved | Implement | Verify |

| H-7 NASA | Identify | | Analyze | | | | Plan | | | Communicate and document | Track | Control |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IA-1 RAMCAP | Critical assets: prepare for study | Define scope | Analyze threats | Analyze vulnerabilities | Analyze consequences | Analyze risks | Identify action strategies | Analyze benefits and costs | Make informed decisions | Communicate results for all steps | Implement results | Monitor risks |
| IA-2 FEMA | Terrorist attacks against buildings | Buildings | Threat identification and rating | Vulnerability rating | Asset value rating | Threat* asset value * vulnerability[a] | Mitigation options | Prioritize | Select mitigation options | Not addressed | | |
| IA-3 DS | Facility security | Asset assessment | Threat discovery and assessment | Vulnerability assessment | Asset assessment | Risk assessment | Mitigation option analysis | | Operations and security planning | Not addressed | Remediation program management | Trend analysis and auditing |
| IA-4 ODP | Not addressed | Criticality assessment | Threat assessment | Vulnerability assessment | Impact assessment | Risk assessment | Not addressed | | | | | |
| IA-5 GAO | Strategic goals, objectives, and constraints | | Risk assessment | | | | Alternatives evaluation | | Management selection | Not addressed | Implementation and monitoring | |
| IA-6 MORDA | Value models | Information system | Threat categories | Attack trees | Value models | Baseline risk | CM design options | Cost–benefit analysis | Optimization and decision making | Not addressed | Implement CM design options | Not addressed |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| Reference Number | Identify Goals and Objectives | Define System | Assess Threats | Assess Vulner-abilities | Assess Con-sequences | Assess Baseline Risk | Identify RM Options | Analyze Benefits and Costs | Make Decisions | Communicate Risks | Implement RM Actions | Monitor RM Actions |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| IA-7 COMSEC | Planning | Identify assets | Threat analysis | Identify vul-nerabilities | Assess con-sequences | Risk analysis | Identify safeguards | Not addressed | Avoid, transfer, accept, reduce | Not addressed | Implement and certify | Operations and main-tenance |
| AH-1 Orange Book | Not addressed | Risk environment/ context, extended enterprise | Identify risks | Assessing risks | | | Addressing risks | | | Communica-tions and learning | Not addressed | |
| AH-2 CAPRA | Identify | Define | Assess | Assess | Assess | Assess | Identify | Analyze | Benefit–cost analysis | Communicate | Evaluate | |
| AH-3 Army | Army mission objectives | Missions | Identify Hazards | Assess prob-abilities | Assess severity | Assess risk level and mission risk | Develop controls | Assess controls | Make decision | Not addressed | Implement | Supervise and evaluate |

[a]CM, countermeasures; RM, risk management.

6. *Assess baseline risk.* Assessing the baseline risk is not as common. However, without a baseline risk assessment, it is difficult to compare the costs and benefits of risk management options.
7. *Identify risk management options.* This task is used in all risk frameworks that address risk management. The quality and quantity of the risk management options are important considerations.
8. *Analyze benefits and costs.* Benefit–cost analysis is a common task. Organizations have limited budgets. Resources spent on risk management are not spent on providing products and services to generate profit (private organization) or provide value to citizens (public organization). Benefits and costs can be assessed qualitatively or quantitatively.
9. *Make decisions.* Decision making is a common risk management task. For all public organizations and many private organizations, decision makers are accountable to other individuals and organizations to obtain the most benefit for the resources.
10. *Communicate risks.* Risk communication requires the identification of stakeholders and development plans to provide timely information in a form that stakeholders will understand. Stakeholder participation earlier in the process tends to build understanding and confidence in the results.
11. *Implement risk management actions.* Implementing risk management options is not always included. Implementation requires the support of key stakeholders who have important roles in implementation.
12. *Monitor risk management actions.* Monitoring of risk management options to evaluate the extent to which they achieve risk mitigation objectives is seldom included in risk frameworks, but seems like an important task to ensure that benefits and costs were correctly assessed. In addition, this task is required to help identify the need for future actions.

These tasks constitute a comprehensive risk analysis framework. Although we do not advocate a one-size-fits-all common framework for the entire homeland security enterprise, we do believe that there is potential utility in developing a risk analysis framework with all these elements that could then be tailored to specific applications. Such tailoring could involve combining or eliminating tasks, alternative terminology, providing greater detail on certain tasks, and so on. At the very least, this list provides a basis to evaluate frameworks. If some tasks are not addressed, a justification should be provided.

We make the following additional observations:

*Risk problem identification.* In Table 2 we have two risk problem identification tasks: identify goals and objectives (of the study) and define the system. In contrast to decision analysis and systems engineering, stakeholder analysis is *not* a first task in the risk frameworks. Only one framework explicitly addresses the risk environment (UK Orange Book). We found that risk analysis goals and objectives are explicitly included in most, but not all, of the frameworks. In some frameworks, the scope is obvious by the name of the framework (COMSEC) or the framework application area (Federal Emergency Management Agency (FEMA) terrorist attack on buildings). In other frameworks, the scope and objectives must be determined (GAO, Orange Book, and Army). The most comprehensive frameworks seem to be the frameworks with the broadest scopes (Risk Governance Framework, RAMCAP, and Critical Asset and Portfolio Risk Analysis (CAPRA)).

*Risk assessment.* Most of the frameworks assess threats, vulnerabilities, and consequences. However, the definitions of these terms and the order of assessment is not the same. Several of the frameworks focus on critical assets; some have a methodology to identify the critical assets (Risk Filtering and Ranking Method, RFRM). Only one framework explicitly addresses dependencies (RAMCAP). A couple of frameworks emphasize the importance of learning about threats and vulnerabilities (Orange Book and IRGC).

*Risk management.* There is no common terminology or approach for risk management. Different terms are used including options, countermeasures, actions, plans, and strategies. The risk management tasks and techniques can also be quite different. Cost–benefit analysis is included in some frameworks (RAMCAP, DOT, and MORDA. Several of the frameworks address implementation and monitoring of risk management actions (IRGC, RFRM, DOT, NASA, DS, GAO, COMSEC, CAPRA, and Army). Only one framework (IRGC) explicitly addresses risk perceptions. Seven of the 17 frameworks included risk communication.

## 6 EXAMPLE RISK FRAMEWORKS

In this section we present an example of a conceptual and a procedural framework.

### 6.1 A Conceptual Framework: The Government Accountability Office Risk Management Framework

The GAO uses a procedural risk framework (Figure 4) with five tasks [15, 21]:

1. strategic goals, objectives, and constraints
2. risk assessment
3. alternatives evaluation
4. management selection
5. implementation and monitoring.

Although there is an ordering of these tasks, the cyclical representation in the GAO framework suggests an iterative process. This framework does not specify the specific analysis techniques or the outputs of the analysis. The GAO uses this framework to evaluate homeland security risk management programs.

We are particularly fond of this conceptual framework because it is relatively straightforward to draw a correspondence between its 5 steps and 11 of the 12 tasks that span all 17 frameworks surveyed. The one task not explicitly included in the GAO Risk Management Framework is *Communicate Risks*. We believe this framework would be improved were this task shown supporting the other five tasks from the center of the oval.

### 6.2 A Procedural Framework: Critical Asset and Portfolio Risk Analysis (CAPRA)

CAPRA provides a quantitative approach for all-hazards risk analysis [22, 23]. As we see in Figure 5, CAPRA specifies the analysis tasks, the analysis techniques, and the output of each task.

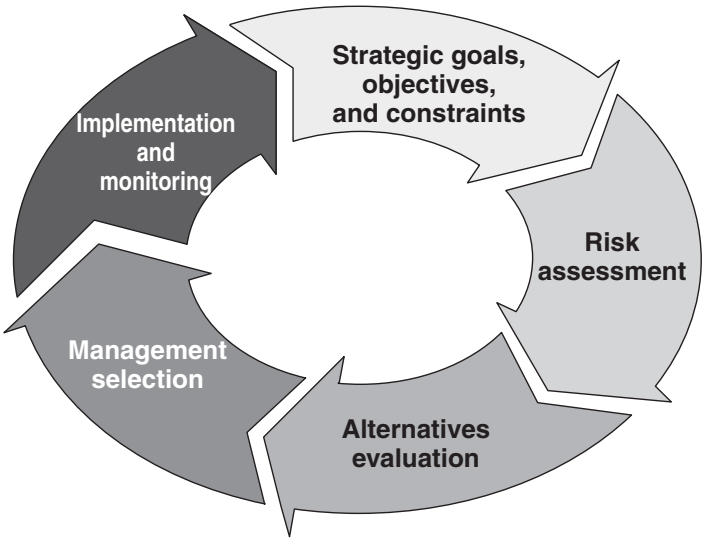



**FIGURE 4** GAO risk management framework.

In general, CAPRA is a five-phase process that identifies hazard scenarios that are relevant to the region or asset of interest, assesses the losses for each of these scenarios given they were to occur, allows for consequence-based screening, assigns a probability of success given a hazard as one, assesses the annual rate occurrence for each scenario, and provides results suitable for benefit–cost analysis. CAPRA produces *risk assessments* that can form the basis for identifying alternative risk mitigation strategies and evaluating them for their cost-effectiveness, affordability, and ability to meet risk reduction objectives.

The following provides a description of each phase:

- *Scenario identification.* characterizes the missions applicable to a region and identifies hazard and threat scenarios that could cause significant regional losses should they occur. For natural hazards, this phase considers the estimated annual rate of occurrence, and screens out infrequent scenarios. For security threats, this phase identifies relevant scenarios based on the inherent susceptibilities of a region's mission and lifeline services to a wide spectrum of threat types. The product of this phase is a complete set of hazard and threat scenarios that are relevant to the region under study.
- *Consequences and criticality assessment.* assesses the loss potential for each scenario identified for the region by considering the maximum possible loss, physical vulnerability of key missions and services, and effectiveness of consequence-mitigation measures to respond to and recover from a scenario. The results of this phase provide estimates of potential loss for each hazard and threat scenario, which are used to screen scenarios and determine those that warrant further analysis.
- *Security vulnerability assessment.* assesses the effectiveness of measures to deny, detect, delay, respond to, and defeat an adversary determined to cause harm to a

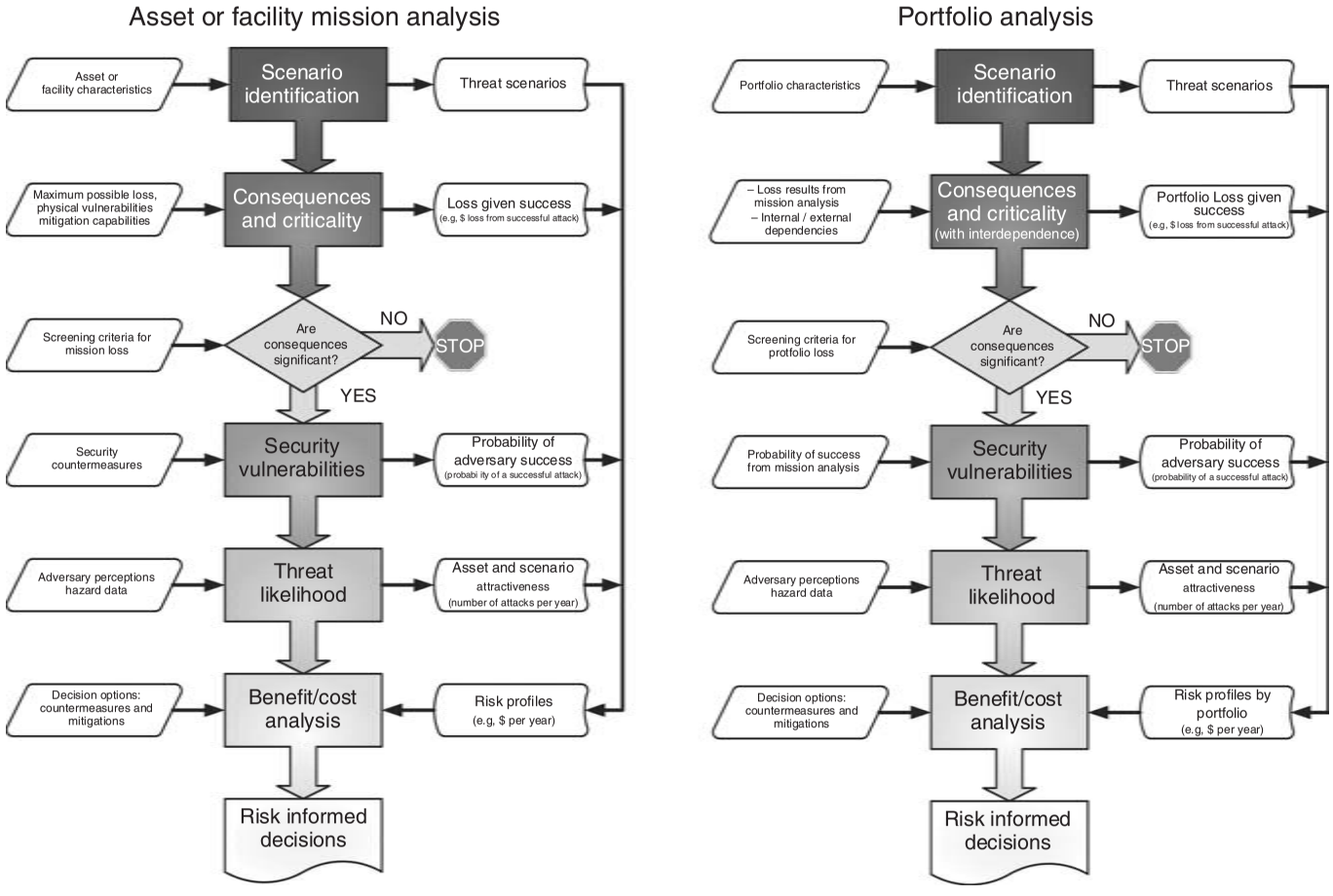



**FIGURE 5** Critical asset and portfolio risk analysis (CAPRA) [4].

region. The results from this phase provide estimates of the probability of adversary success for each threat scenario, which combined with loss yields an estimate of conditional risk.

- *Threat likelihood assessment.* assesses scenario attractiveness from the adversary's point of view. The results from this phase provide estimates of the annual rate of occurrence for each threat scenario.
- *Benefit/cost analysis.* assesses the cost-effectiveness of proposed countermeasures and consequence-mitigation strategies produced from the developing of strategy tables. The results from this phase provide benefit-to-cost ratios for each proposed risk mitigation strategy, which are used to inform resource allocation decisions.

## 7 A CONCLUDING THOUGHT

It is no exaggeration to characterize the terrorist threat, from a national perspective, as *existential*. The consequences of terrorist attacks, and potentially ineffective, inefficient, and counterproductive responses to those attacks could threaten our society in fundamental ways. In countering the terrorist threat, we must be at least as intelligent, resourceful, and adaptive as our adversaries have proven to be. Among other things, this requires the best risk analyses we can develop. Greater rigor in the use of terminology and risk frameworks is a useful first step.

## REFERENCES

1. Graham, B. and White, J. (2006). Abizaid credited with popularizing the term 'Long War'. *The Washington Post*, A08.
2. U.S. General Accounting Office (GAO) (2001). GAO-02-150T. *HOMELAND SECURITY Key Elements of a Risk Management Approach*, Washington, DC.
3. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*, Chapman and Hall/CRC Press, p. 39.
4. U.S. Coast Guard (2008). *Risk-based Decision-making Guidelines*. Coast Guard web site: http://www.uscg.mil/hg/g-m/risk/e-guidelines/RBDMGuide.htm, accessed January 21, 2008.
5. Renn, O. (2005). *Risk Governance: Towards an Integrative Approach*, International Risk Governance Council, Geneva, Switzerland.
6. Science Applications International Corporation (SAIC) (2002). *A Guide to Highway Vulnerability Assessment*, Vienna, VA.
7. Haimes, Y., Lambert, J., Horowitz, B., Kaplan, S., Pikus, I., Leung, F., and Mosenthal, A. (2004). *Risk assessment and management of critical highway infrastructure, Report to Virginia Transportation Research Council*, University of Virginia, Charlottesville, VA.
8. International Life Science Institute (ILSI) (2000). *Revised Framework for Microbial Risk Assessment*. An ILSI Risk Science Institute report. Washington, DC.
9. ICF Consulting (2000). *Risk Management Framework For Hazardous Materials Transportation*, report to US Department of Transportation, Fairfax, VA.

10. National Aeronautics and Space Agency (NASA) (2002). *NPR 8000.4 NASA Risk Management Directive*, Office of Safety and Mission Assurance, Washington, DC.
11. American Society of Mechanical Engineers (ASME) (2004). *Risk Analysis And Management For Critical Asset Protection: General Guidance*.
12. Federal Emergency Management Agency (FEMA) (2006). *FEMA 452. Risk Assessment: How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings*, Washington, DC.
13. Ware, B. S., Beverina, A. F., Gong, L., Colder, B. (2002). *A Risk-Based Decision Support System For Antiterrorism*. Digital Sandbox web site: http://www.dsbox.com/Documents/MSS A Risk-Based Decision Support System for Antiterrorism.pdf, accessed January 21, 2008.
14. Office of Domestic Preparedness (ODP) (2003). *Special Needs Jurisdiction Toolkit for Official Use Only*, Washington, DC.
15. U.S. Government Accountability Office (GAO) (2005). GAO-06-91. *RISK MANAGEMENT Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, Washington, DC.
16. Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., Wallner, J. M., and Saydjari, O. S. (2005). Mission oriented risk and design analysis of critical information systems. *Mil. Operat. Res*. **10**(2), 19–38.
17. Government of Canada (1999). *Threat and Risk Assessment Working Guide*, Communications Security Establishment, Ottawa, Ontario, Canada.
18. Her Majesty's Treasury (2004). *The Orange Book: Management of Risk Principles and Concepts*, London, UK.
19. Ayyub, B. M. (2006). *Guide on the protection of critical infrastructure and key resources for homeland security*, Center for Technology and Systems Management, University of Maryland.
20. Department of the Army (1998). *Risk Management. Field Manual 100-14*, Washington, DC.
21. U.S. Government Accountability Office (GAO) (2007). GAO-07-386T. *HOMELAND SECURITY Applying Risk Management Principles to Guide Federal Investments*, Statement of William O. Jenkins, Jr., Director Homeland Security and Justice Issues.
22. Ayyub, B. M., McGill, W. L., Kaminskiy, M. (2007). Critical asset and portfolio risk analysis for homeland security: an all-hazards framework. *Risk Anal. Int.J., Soc. Risk Anal*., **27** (3), 789–801. DOI: 10.1111/j.1539-6924.2007.00911.x.
23. McGill, W. L., Ayyub, B. M., and Kaminskiy, M. (2007). A quantitative asset-level risk assessment and management framework for critical asset protection. *Risk Anal. Int. J., Soc. Risk Anal*. **27**(5), 1265–1281. DOI: 10.1111/j.1539-6924.2007.00955.x.

## FURTHER READING

Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*, Chapman and Hall/CRC Press.

Haimes, Y. Y. (2004). *Risk Modeling, Assessment, and Management*, 2nd ed., John Wiley & Sons, Inc., Hoboken, NJ.

Parnell, G. S., Dillon-Merrill, R. L., and Bresnick, T. A. (2005). Integrating risk management with homeland security and antiterrorism resource allocation decision-making. In *The McGraw-Hill Handbook of Homeland Security*, D. Kamien, Ed., New York, pp. 431–461.

Scouras, J., Cummings, M. C., McGarvey, D. C., Newport, R. A., Vinch, P. M., Weitekamp, M. R., Colletti, B. W., Parnell, G. S., Dillon-Merrill, R. L., Liebe, RM, Smith, GR, Ayyub, B. M., and Kaminskiy, M. P. (2005). *Homeland Security Risk Assessment*. Volume I, An Illustrative Framework. RP04-024-01a. Homeland Security Institute, Arlington, VA.

# RISK ANALYSIS AND MANAGEMENT FOR CRITICAL ASSET PROTECTION

JERRY P. BRASHEAR AND J. WILLIAM JONES
*ASME Innovative Technologies Institute, LLC, Washington, D.C.*

## 1 INTRODUCTION

The current economic crisis and events of 9/11, Hurricane Katrina, terrorist attacks and natural disasters at home and abroad have heightened the nation's awareness of the risks to critical infrastructures. This awareness has stimulated the requirement that risks and risk-reduction options be assessed in ways permitting the direct comparisons needed for rational allocation of resources. Numerous risk methodologies are in use by individual firms and industries, but their results are generally not comparable with other firms or industry sectors or, in some cases, not even with other facilities within the sector. Most are qualitative or ordinal only, producing relative results that can be compared only locally, if at all. Moreover, several of the available methods require the assistance of specialized consultants and/or considerable amounts of time, money and personnel resources, which discourages their use and makes them costly to use on a regular basis. The RAMCAP Plus process—through the cost-effective application of common and consistent terminology, processes and metrics—provides an objective, repeatable basis for assessing risk, resilience, and the benefits and costs of improvements in a transparent, consistent, quantitative, and directly comparable manner.

## 2 ORIGIN AND DEVELOPMENT

Following the attacks of September 11, 2001, the American Society of Mechanical Engineers (ASME) convened more than one hundred industry leaders, at the request of the White House, to define and prioritize the requirements for protecting our nation's critical infrastructure. Their primary recommendation was to create a risk analysis and management process to support decisions allocating resources to initiatives that can reduce risk. This process would necessitate quantitative objectivity; common terminology; common metrics; and consistent processes for analysis and reporting, often tailored to the technologies, practices and cultures of the respective industries. This commonality would permit direct comparisons within and across industrial sectors, scales of analysis from asset to region to nation, and time for measuring trends and effectiveness as well as maintaining accountability. Such direct comparisons are seen as *essential* to supporting rational decision-making in allocating limited private and public resources to reducing risk and enhancing resilience of critical infrastructures.

Published by permission of ASME Innovative Technologies Institute, LLC.

In response to this recommendation, ASME assembled a team of distinguished risk assessment experts from industries and universities to develop a suitable methodology. The team defined a seven-step methodology that enables asset owners to perform assessments of their risks and risk-reduction options, relative to specific attacks. A series of reviews with infrastructure executives and engineers added the design criterion: to be useful, acceptable and useable by personnel at facilities of concern; the methodology must be *appropriate for self-assessment by on-site staff, in a relatively short period of time*. The original version was simplified and streamlined to meet this criterion. Throughout the experience with RAMCAP$^{TM}$, balancing practicality with scientific rigor has been a challenge—and still is.

The simplified version of RAMCAP [1] served as the basis for consistent sector-specific guidance documents for (i) nuclear power generation; (ii) spent nuclear waste transportation and storage; (iii) chemical manufacturing; (iv) petroleum refining; (v) liquefied natural gas offloading terminals; (vi) dams and navigational locks; and (vii) water and wastewater systems. In addition, ASME-ITI has prepared a version for higher education campuses, that is currently being tested. Experience in field testing these tailored processes, the devastation caused by recent natural disasters, and a growing appreciation of the range of threats to critical infrastructures caused the simplified process to evolve into the present RAMCAP Plus.

## 3 RISK AND RESILIENCE DEFINED

Consistent with the widely held definition that risk is the expected value of the consequences of an adverse event, that is, the combination of the event's likelihood and consequences, the National Infrastructure Protection Plan [2], and RAMCAP Plus [3] split the likelihood term into event likelihood and conditional vulnerability, given the event:

$$\text{Risk} = (\text{Threat}) \times (\text{Vulnerability}) \times (\text{Consequence}) \text{ or } R = T \times V \times C \qquad (1)$$

where

Risk = The probability of loss or harm due to an unwanted event and its adverse consequences. When the probability and consequences are expressed as numerical point estimates, the expected risk is computed as the product of those values.

Threat ($T$) = The likelihood that an adverse event will occur within a specified period, usually one year. The event could be anything with the potential to cause the loss of, or damage to, an asset or population.

Vulnerability ($V$) = The probability that, given an adverse event, the estimated consequences will ensue.

Consequence ($C$) = The outcomes of an event occurrence, including immediate, short and long-term, direct and indirect losses and effects. Loss may include human fatalities and injuries, economic damages and environmental impacts, which can generally be estimated in quantitative terms, and less tangible, nonquantifiable effects, including political ramifications, decreased morale, reductions in operational effectiveness or military readiness, etc. RAMCAP Plus estimates economic losses to the infrastructure owner and to the community served, and can readily be extended to states, multistate regions or the nation.

A second, closely related concept, resilience, is not an element in the risk equation, but is central to the purposes of risk management for critical infrastructures. *Resilience* is defined as the ability of an asset, system or facility to withstand an adverse event while continuing to function at acceptable levels or, if functioning is diminished, the speed by which an asset can return to the acceptable level of function (or a substitute function or service provided) after the event. Resilience as a concept is still being formalized, but candidate metrics include reductions in the duration and severity of service denial and/or economic losses to the community due to service denial. For the purposes of this article, resilience is defined in different ways for the asset owner and the community.

For the asset owner, the level of resilience for a particular asset–threat combination is

$$\text{Resilience}_{\text{Owner}} = \text{Lost net revenue} \times \text{Vulnerability} \times \text{Threat} \tag{2}$$

where

Lost revenue = The product of the *duration* of service denial (in days) and the *severity* of service denial (in physical units per day) and pre-event price of the service less variable costs avoided (in dollars per unit), all of which are essential parts of estimating the owner's financial loss, that is

$$\begin{aligned}\text{Lost net revenue} = {} & \text{Duration of denial} \times \text{Severity of denial} \\ & \times (\text{Unit price} - \text{Variable costs})\end{aligned} \tag{3}$$

For the community, the level of resilience for a particular asset–threat combination is

$$\text{Resilience}_{\text{Community}} = \text{Lost community economic activity} \times \text{Vulnerability} \times \text{Threat} \tag{4}$$

where

Lost economic activity in the community = The amount of decreases in both the losses of income, direct and indirect, throughout the economy of the metropolitan region due to denial of service. It is usually estimated as a function of the asset's lost revenue and the duration of the service denial, while using a static application of basic regional economic data and an input–output model, modified to reflect the resilience of the respective business sectors. Impacts on the number of jobs and employment levels are also often estimated in the same model [4–9].

The constituent elements of risk and resilience are treated as independent, single-point, "best" estimates; they are not means of underlying distributions of the estimates. More complete treatment of uncertainty and dependencies is being considered for the future.

## 4 THE RAMCAP PLUS PROCESS

The RAMCAP Plus process comprises seven steps (Figure 1). Taken as a whole, these steps provide a rigorous, objective, replicable, and transparent foundation for data-collection, interpretation, analysis, and decision-making.

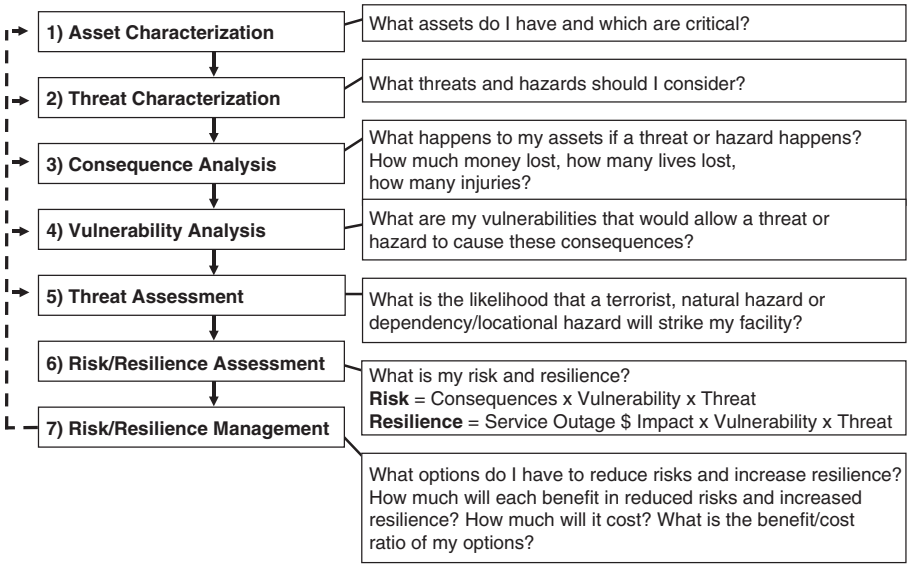



**FIGURE 1** The RAMCAP Plus process.

The figure also shows the iterative nature of the RAMCAP process. The feedback arrows imply that the assessment of risk-reduction and resilience enhancement benefits is a reiteration and modification of some or all of the same logical steps as the initial, baseline risk estimate. Enhancing security and resilience requires that the options being considered reduce consequences (including duration of service denial), vulnerability, and/or the likelihood of occurrence. The process estimates the changes attributable to a countermeasure or mitigation option.

*Benefits* are defined as the change in risk and/or resilience (the result of changing the elements in Eqs 1–3); and *costs* include the investment and operating costs of the option. With these estimates, the net benefit (benefit less costs) and benefit–cost ratio can be used to rank the options by the magnitude and efficiency of security or resilience improvement per dollar of cost. Reductions of other consequences (e.g. fatalities) can be either converted to dollar values using the value of a statistical life, or can be maintained as a separate indicator.

The feedback arrows also imply that the process is iterated for three additional concepts: (i) for each relevant threat for a given asset; (ii) for each asset critical to the mission of the organization; and (iii) over time as part of continuous improvement and evaluating periodic progress (e.g. annually) or as needed based on changing threat circumstances.

*Step 1. Asset characterization* analyzes the organization's mission and operational requirements to determine which assets, if damaged or destroyed, would diminish the facility's ability to meet its mission. Critical assets are identified and a preliminary estimate is made of the gross potential consequences from various threats or hazards, in ordinal terms (e.g. "very small" to "very large" in five to seven intervals). The assets evaluated include those that are directly engaged in performing the most important missions or functions, the assets that support these and the infrastructures on which they depend. These assets may include physical plants, cyber systems, knowledge bases, human resources, customers or critical off-site suppliers.

Since the number of assets owned by an organization can be substantial, the assessment team conducts an initial ranking to identify the high priority assets, screening out the rest. The term "asset" means components of an organization's system.

The assets that directly perform the organization's mission are usually fairly obvious, but the assets and systems on which they depend may be less so. For example, a water plant has systems through which water flows for treatment and distribution and many of these are critical, but these systems require electricity, chemicals, automated monitoring, water testing, skilled labor, and so on, which can also be critical because the assets directly performing the mission cannot operate without them.

The supporting assets, in turn, may be dependent on yet other assets, which are then seen as critical, for example, the electricity substation from which the plant draws its power. Whenever an alternative source of critical support is independently available, the supporting asset may not be critical, for example, an emergency generator with sufficient fuel to last through an event would make the substation noncritical. Noncritical assets are not considered further.

*Step 2. Threat characterization* is the identification and description of reference threat scenarios in enough detail to estimate vulnerability and consequences. As summarized in Table 1, there are a wide variety of threat scenarios. Each is specified in more detail in actual application [3].

One key to comparability of results is the use of a common set of reference threats. These threat scenarios are not "design basis threats," which imply that the organization must take steps to withstand the threat to continue operations. Rather, these are "benchmark" or "reference" threats that span the survivable range of possible threats across all critical infrastructure sectors. Five distinct types of reference threats have been defined as follows:

1. *Terrorism.* Attacks by enemies, as suggested by the U.S. Department of Homeland Security (DHS) based on analyses by DHS and others as an understanding of the means, methods, motivations and capacities of terrorists.
2. *Natural hazards.* Currently including hurricanes, floods, tornadoes and earthquakes, based on the physical location of the facility and federal data.
3. *Product or waste stream contamination.* Suggested by the water sector and also applicable to food and pharmaceuticals, to address concerns of intentional or accidental contamination.
4. *Supply chain hazards.* Immediate dependencies, mostly supply chain issues such as suppliers, labor, and customers included as an initial step toward dealing with dependencies on other organizations for critical elements of the organization's mission.
5. *Proximity hazards.* Potential to become collateral damage from events at nearby sites.

The organization decides which of the defined scenarios represent possible physical threats for the facility; some, such as a major marine attack in a desert, may be impossible. For those threats which are possible, the organization should summarily assess the consequences of a successful attack by each threat against each asset earlier defined as critical. A convenient way to do this is to array a matrix of the critical assets identified in the first step versus the possible threats and estimating ordinally according to a five- or seven-point ordinal scale (e.g. very low, low, moderate, high, and very high).

**TABLE 1 Summary of *RAMCAP Plus* Reference Threat Scenarios**

| Attack Type | Tactic/Attack Description | | | |
|---|---|---|---|---|
| Marine | M1 | M2 | M3 | M4 |
| | Small boat | Fast boat | Barge | Deep draft shipping |
| Aircraft | A1 | A2 | A3 | A4 |
| | Helicopter | Small plane (Cessna) | Medium, regional jet | Large plane long-flight jet |
| Land-based vehicle | V1 | V2 | V3 | V4 |
| | Car | Van | Mid-size truck | Large truck (18 wheeler) |
| Assault team | AT1 | AT2 | AT3 | AT4 |
| | 1 Assailant | 2–4 Assailants | 5–8 Assailants | 9–16 Assailants |
| Sabotage | S(PI) | S(PU) | S(CI) | S(CU) |
| | Physical-Insider | Physical-Outsider | Cyber-Insider | Cyber-Outsider |
| Theft or diversion | T(PI) | T(PU) | T(CI) | T(CU) |
| | Physical-Insider | Physical-Outsider | Cyber-Insider | Cyber-Outsider |
| Product contamination | C(C) | C(R) | C(B) | C(P) |
| | Chemical | Radionuclide | Biotoxin | Pathogenic |
| | C(W)—Weaponization of waste disposal system | | | |
| Natural hazards | N(H) | N(E) | N(T) | N(F) |
| | Hurricanes | Earthquakes | Tornadoes | Floods |
| Dependency and proximity hazards | D(U) | D(S) | D(S) | DI |
| | Loss of utilities | Loss of suppliers | Loss of employees | Loss of customers |
| | D(T) Loss of transportation | | D(P) Proximity to other targets | |

This establishes the sequence by which asset–threat pairs will be analyzed: examine the highest ranked and proceed to lower ranked until the consequences are acceptable.

*Step 3. Consequence analysis* is the identification and estimation of the *worst reasonable consequences* generated by each specific asset–threat combination. This step examines facility design, layout and operation in order to estimate fatalities, serious injuries and economic impacts.

RAMCAP Plus defines "economic impacts" for risk management at two levels: (i) the financial consequences to the organization and (ii) the economic consequences to the regional metropolitan community the organization serves. Economic consequences for communities larger than the metropolitan area, for example, the state, multistate region, or nation, may also be estimated using the same methods, as needed by decision-makers. For many critical infrastructures and facilities, interdependencies make the metropolitan region most relevant to decision-makers.

Financial consequences to the organization include all necessary costs to repair or replace damaged buildings and equipment, abandonment and decommissioning costs, site and environmental cleanup, net revenue losses (including fines and penalties for failing to meet contractual production levels but excluding avoided variable costs) while service is reduced, direct liabilities for casualties on and off the property and environmental damages. These costs are reduced by applicable insurance or restoration grants and must be corrected to account for tax effects for tax-paying organizations.

The primary concern for the public or community is the length of time, quantity and sometimes quality of critical service denied, and the direct and indirect economic consequences of service denial [5, 6]. When the service denial is short and/or customers are able to cope by such actions as conservation, substitution, redundancies, making up lost production later, the region is said to be "resilient" [7]. The public's objective is to enhance the resilience of critical infrastructures on which they depend.

RAMCAP Plus estimates the direct and indirect losses to the regional community by a modified input–output algorithm. While recognizing the classical critiques of input–output modeling of a major disruption of critical infrastructures, it remained necessary to quantify at least roughly the community impact, to guide public choices. To minimize the methodological problems without adding inordinate complexity, RAMCAP Plus adopted a model originally developed to fill a gap in the computational ability of HAZUS-MH [8], the Federal Emergency Management Agency's loss estimation software referred to as a *HAZUS patch* [9]. The algorithm can be applied to any estimate of infrastructure service disruption to compute direct and indirect losses of regional output, income and jobs.

Other consequences are identified and described qualitatively, and include impact on iconic structures, governmental ability to operate, military readiness, and citizen confidence in the organization, product, or the government.

*Step 4. Vulnerability Analysis* estimates the conditional likelihood that the estimated consequences will occur, *given* the occurrence of the specific threat or hazard. Vulnerability analysis involves an examination of existing security capabilities and structural components, as well as countermeasures and their effectiveness.

A variety of rigorous tools can be used to estimate vulnerability, such as those described in Table 2.

Direct elicitation often seems to be easier and less time-consuming, but the time to reason through each threat–asset pair can lead to long discussions and it is difficult to maintain logical consistency across a number of such judgments. Some RAMCAP sector-specific guidance documents provide prespecified structure of vulnerability logic, event or decision trees for users to populate with estimates of the required elements to enhance comparability and reliability.

*Step 5. Threat assessment* estimates the probability that a particular threat–terrorist, natural, contamination, dependency, or proximity–will occur in a given time frame (usually one year). The approach differs depending on the type of hazard, as characterized in Table 3.

Terrorism likelihood (and its contribution to contamination, proximity, and even dependency hazards) is the most difficult to estimate and is still being refined. In its most advanced formulation, it recognizes that terrorists are cognizant, near-optimizing adversaries in a contest perhaps best modeled by game theory. Because of RAMCAP's specification to keep the process simple and brief, however, simpler techniques of

**TABLE 2 Frequently Used Vulnerability Tools**

| Method | Description |
|---|---|
| Direct expert elicitation | Members of the evaluation team discuss the likelihood of success and their reasoning for their estimates; in its more formal form, a statistical "Delphi" processor Analytical Hierarchy Process can be used to establish a consensus. |
| Vulnerability logic diagrams (VLDs) | Plot of the flow of events from the time an adversary approaches the facility to the terminal event in which the attack is foiled or succeeds, considering obstacles and countermeasures that must be surmounted, with each terminal event associated with a specific likelihood estimate. This is frequently complemented with an estimate of the reaction time of a counterforce once the attack has been detected |
| Event trees (also called "failure trees") | Tree with branches for the sequence of events between the initiation of the attack and the terminal events. The evaluation team estimates the probability of each outcome. Multiplying the probabilities along each branch, from the initiating event to each terminal event, calculates the probability of each unique branch, while all branches together sum to 1.0. The sum of the probabilities of all branches on which the attack succeeds is the vulnerability estimate |
| Decision trees | Very similar to event trees except that the decisions by the adversary are modeled at each node in the unfolding tree to capture the adaptive behavior of the adversary; a sophisticated variant is to model the tree as a two-player game |
| Hybrids of these | Often used by the more sophisticated assessment teams |

**TABLE 3 Estimation of Hazard Likelihood**

| Hazard Type | Likelihood/Probability Estimation |
|---|---|
| Terrorist attack | Based on the terrorists' objectives and capabilities, (generally provided by intelligence and law enforcement agencies), and the attractiveness of the facility relative to alternative targets, the asset's expected value (vulnerability x consequences), and the cost/effectiveness of the attack |
| Natural hazards | Based on the historical federal frequency data for various levels of severity at the specific location of the asset. Can be adjusted if there is reason to believe that the future frequency or severity will differ from the past |
| Dependency hazard | Based on local historical records for the frequency, severity and duration of service denials as a baseline estimate of "business as usual," incrementally increased if they may be higher due to terrorist activity or natural events on required supply chain elements. Confidential conversations with local utilities and major suppliers can inform these estimates |
| Product contamination | Treated the same as terrorism and dependency likelihood, except additional consideration is given to accidental contamination of inputs and the vulnerability of critical processes to accidents |
| Proximity hazard | Based on asset's location relative to other assets that may incur adverse events leading to collateral damage, using the same logic in estimating terrorist and natural hazard threats |

approximation based on observable or previously estimated factors are used. RAND Corporation has contributed relative likelihood of attack based by metropolitan region and asset type [10]. The previously estimated conditional risk (consequences, times, vulnerability) aptly characterizes the expected value to the terrorist of the asset–threat pair, while the asset's size and prominence relative to other assets of the same type in the region can indicate attractiveness. The adversary might also consider the likelihood of preattack detection and the "cost" in resources. This approach is explained in reference [11].

Two additional analyses can assist in appraising the realism of this approach to terrorism likelihood:

1. *Comparison of terrorism risk with natural hazard risk.* uses a natural hazard risk that is accepted by the organization to deduce a terrorism threat likelihood equating the two risks. The analyst and decision-maker then judge whether the deduced likelihood is reasonable or not. If the likelihood in the deduced risk is equal to or less than the judged reasonable level, then the terrorism risk is as tolerable as the natural hazard risk and the likelihood is moot. If, on the other hand, the likelihood in the deduced risk is greater than the accepted level, the judgment of the reasonable level sets a minimum and the asset–threat pair's risk justifies taking the next steps.
2. *Investment break-even.* assumes the decision-maker's choices are simple "go/no-go" on individual options. This method can only be applied as part of Step 7 because it requires the calculation of a baseline risk, conceptual design and cost estimation of an investment option to materially reduce the risk, and an assessment of the risk with the option in place. Given the reestimated consequences and vulnerability and the option cost, the calculated "break-even" likelihood is the one that yields a net benefit of exactly zero and a benefit–cost ratio of 1.0. The decision-maker can then judge whether the "break-even" likelihood is plausible or not. If the decision-maker believes the actual likelihood exceeds the break-even, the option has value and results in a "go" decision, and vice versa.

*Step 6. Risk and resilience assessment* creates the foundation for prioritizing and selecting among risk-reduction and resilience enhancement options. The risk assessment step is a systematic and comprehensive evaluation of the previously developed estimates. The risk for each threat for each asset is calculated from the risk relationship expressed in Eq. (1).

Resilience, the ability to function despite and during a traumatic event or to restore functionality in very short time, is defined in different ways for the asset owner (Eq. 2) and community (Eq. 3), respectively, for each asset–threat pair.

*Step 7. Risk and resilience management* is the step that actually reduces risk and increases resilience. Having determined the risk and resilience of each important asset–threat pair, this step defines new security countermeasures and consequence-mitigation resilience options, and evaluates them to achieve a portfolio that yields an acceptable level of risk and resilience at an acceptable cost. The 10 actions described in Table 4 constitute this crucial step.

In essence, the value or benefit of the options is estimated by revisiting Steps 3, 4 and/or 5 and reestimating the (reduced) threat likelihood, vulnerability or consequences to calculate a new risk and resilience with the option in place. The reduction in risk and the increase in resilience are the benefit or value of the option, which can be compared

**TABLE 4 Risk and Resilience Management Actions**

| Activity Title | Activity Description |
|---|---|
| 1. Acceptance level | Establish whether the risk/resilience level is acceptable |
| 2. Design | Design potential countermeasures and consequence-mitigation options that would reduce risk and/or enhance resilience |
| 3. Costs | Estimate the investment and operating costs of each option |
| 4. Reestimation | Reestimate consequences, threat likelihood, and/or vulnerability, whichever is affected by the option |
| 5. Benefits | Recalculate risk and resilience, given the option, and subtract it from the risk without the option (the "do nothing" baseline option) to define the *benefit* of the option |
| 6. Combinations | Combine the options that affect multiple asset–threat pairs, for example, if a higher fence changes the vulnerability for an attack by one assailant, it may do the same for two to four. Add the benefits of the asset-pairs to compute the total benefit of the option |
| 7. Key metrics | Calculate the net benefits (less costs) (value) and the benefit–cost ratio (efficiency) of the option |
| 8. Rank and select | Select the options that have the highest net benefits and/or benefit–cost ratios and the lives saved, injuries avoided, considering both risk and resilience until resources are fully committed (less any reserved amounts) |
| 9. Manage | Manage the implementation and operation of the selected options, evaluate their effectiveness and make mid-course corrections for maximum effectiveness |
| 10. Recycle | Repeat the risk analysis cycle periodically or as needed given intelligence or changing circumstances, for example, new technologies and new facilities |

to the cost of implementing it and to the benefits of other options. Taking no action is always a baseline option against which all others are compared.

Net benefits measure the magnitude of the value added by the option, while the benefit–cost ratio measures of the amount of risk reduction per unit of cost, an efficiency test. For fatalities and serious injuries, examine the gross reductions and the expected number required to make the needed trade-offs. The full set of options should be as a portfolio to establish if equity and balance are maintained. Financial, human, and other resources are then allocated to implement and operate the selected options.

Choices among the options are virtually never made with a single metric, but rather a set of difficult trade-off decisions must be made. Some organizations apply explicit preferences to establish an initial portfolio of options and then adjust the selections as needed to balance the portfolio or program of risk-reduction and resilience enhancement measures. It is common to estimate a "value of statistical life" to roll human casualties into the dollar-denominated benefits. When this is done, RAMCAP Plus calls for displaying the casualty estimates separately as well, for decision-makers to consider.

Once these decisions are made, risk management extends to implementation of the chosen options, monitoring their effectiveness and taking corrective actions as needed. The risk management process is the essential part of continuous security and resilience improvement, repeated periodically (e.g. annual budget process) or as necessitated

by changes in the threats, vulnerabilities, consequences, technologies or the evolving development of the organization's systems.

In addition to investing in these options, risk can also be managed by acquiring insurance, entering into cooperative agreements, or simply accepting the calculated risk when it compares favorably with other risks such as financial or investment alternatives. Ideally, the organization would consider all these risk-reduction and resilience enhancement options collectively as a mixed portfolio of risk and resilience management.

## 5 BENEFITS OF USING THE RAMCAP PLUS PROCESS

Use of the RAMCAP Plus process generates a number of benefits or advantages to the organization using it, the sector or industry that adopts it, the communities served and the public policy toward infrastructure security and resilience. These are summarized in Table 5.

Several of the entries in Table 5 mention benefits that occur if the process becomes a voluntary consensus standard. As this article is being written, three voluntary consensus American National Standards are being developed based on RAMCAP Plus: one, an overarching standard applicable to any asset-based industry and the others, specifically tailored for water–wastewater utilities and higher education campuses. Three additional RAMCAP Plus standards are under consideration. These standards and others that will follow provide for continuous improvement of the process, *while* maintaining consistency and comparability. They cost the federal government little or nothing other than perhaps sector-specific guidance (SSG) development because they are maintained by volunteers in officially designated standards development organizations, of which ASME and ASME-ITI are two. These benefits result in dynamic, effective risk and resilience management that is driven by the private and public infrastructure organizations in true partnership with all other stakeholders' interests, including public and nonprofit concerns.

In summary, use of the RAMCAP Plus process yields significant benefits to the asset owners and industries who use it, to the communities they serve, and to the local, regional and/or national economies to which they contribute.

## 6 LOOKING TO THE FUTURE

RAMCAP Plus is a "living" tool, now in its third version [3], as new challenges and improved methods are incorporated. Even as this is published, a number of enhancements are being developed or evaluated, including the following:

- sector-specific guidance for additional sectors;
- software for more systematic, efficient application, and facilitation of more sophisticated techniques;
- explicit treatment of uncertainties in, and dependencies among, the key terms of risk and resilience instead of point estimates;
- adding wear, aging, technological obsolescence, and rise in sea level in coastal areas to the hazard set;
- augmenting the analysis of dependencies and interdependencies on the regional scale to track multistage "cascading failures" explicitly;

**TABLE 5 Using RAMCAP Plus and Its Standards Benefits All Levels of Decision-making**

| Beneficiaries | Benefits |
|---|---|
| Infrastructure organizations | • Cost-effective enhancement of security and resilience<br>• Rational allocation of resources across assets, facilities, sites, and lines of business<br>• More efficient management of capital and human resources<br>• Consistently quantified risk and resilience levels, potential net benefit and benefit–cost ratios of investment options<br>• Repeated application over time measures progress and trends while enabling accountability for execution<br>• Enhanced reliability in performance of the mission<br>• Ability to define risk and resilience levels quantitatively at the *community* level enables partnering with other firms and public agencies for large-scale solutions<br>• If adopted as industry voluntary consensus standard, it becomes the vehicle for incentives, such as preferred supplier status, lower insurance costs, higher credit ratings, and lower liability exposure |
| Whole industry or sector | • Ability to identify the assets with the greatest need and value of improvement<br>• Cross-facility comparisons reveal industry-wide vulnerabilities for collective action (e.g. R&D, new technology and standards)<br>• Direct comparison of the sector's risk and resilience level to other sectors for higher level resource allocation and policy-making<br>• If sector-specific guidance becomes a consensus standard, additional benefits can be incurred, e.g.,<br>◦ preferential treatment by insurers, financial rating services and customers<br>◦ potential affirmative defense in liability cases<br>◦ ability to substitute self-regulation by standards for bureaucratic regulation, and direct participation in federal regulatory, procurement or other federal actions |
| Metropolitan regional community | • Ability to estimate value of security and resilience investments to the region, a salient criterion in both private and public decisions<br>• Consistent terminology provides common language for meaningful dialogue between private organizations and government agencies<br>• Identification and valuation of "public goods" and shared-benefit programs; encourages public–private partnerships<br>• Cooperative decision-making based on comparability of risk, resilience, and benefit estimates for rational regional trade-offs<br>• If consensus standards become available, communities can designate the standards as the local codes of expected practice |

**TABLE 5 (*Continued*)**

| Beneficiaries | Benefits |
|---|---|
| | • Repeated application over time measures progress and trends while enabling accountability for regional execution |
| State, multistate regions and/or federal agencies | • All the metro regional community benefits, above<br>• Consistency, transparency and direct comparability needed to evaluate major public infrastructure and program investments<br>• Methods used to estimate economic losses to metropolitan regions can be extended to whatever scales are relevant to the decisions to be made—states, multistate regions or the national economy—in the same, directly comparable terms<br>• Rational allocation of resources to maximize the security and resilience enhancement within a finite budget<br>• If consensus standards are developed, the industry can self-regulate with public compliance audits; maintenance of the standards costs government nothing, *for as long as there is demand for the standard* |

- enhanced estimation of economic impacts on metropolitan, state, multistate, and national scales;
- modification to include valuing both existing and new infrastructures required by a growing population and economy in the same framework;
- adding new metrics of merit such as the upside gains from improved infrastructure, socioeconomic distribution of benefits, quantitative environmental impacts (including effects on global climate), and employment (during construction and subsequently as the improvements in infrastructure contribute to the economy);
- portfolio analysis to exploit correlations and dependencies in selecting collections of investment options.

As these and other enhancements are made, they will be incorporated into the tools and standards that constitute the RAMCAP program.

## REFERENCES

1. ASME Innovative Technologies Institute, LLC. (2006). *RAMCAP: The Framework, Version 2.0*. ASME-ITI, Washington, DC.
2. U.S. Department of Homeland Security. (2006). *National Infrastructure Protection Plan*. DHS, Washington, DC.
3. ASME Innovative Technologies Institute, (LLC). (2009). *All-Hazards Risk and Resilience: Prioritizing Critical Infrastructures Using the RAMCAP Plus$^{SM}$ Approach*. ASME Press, New York.
4. Rose, A. (2006). Economic resilience to disasters: toward a consistent and comprehensive formulation. In *Disaster Resilience: An Integrated Approach*, D. Paton, and D. Johnston, Eds. Charles C. Thomas, Springfield, IL, pp. 226–248.

5. Rose, A. (2004). Economic principles, issues, and research priorities in natural hazard loss estimation. In *Modeling the Spatial Economic Impacts of Natural Hazards*, Y. Okuyama, and S. Chang, Eds. Springer, Heidelberg, pp. 13–36.
6. Rose, A., and Liao, S. (2005). Modeling regional economic resilience to disasters: a computable general equilibrium analysis of water service disruptions. *J. Reg. Sci.* **45**(1), 75–112.
7. Rose, A., Oladosu, G., and Liao, S. (2007). Business interruption impacts of a terrorist attack on the water system of Los Angeles: customer resilience to a total blackout. In *Economic Costs and Consequences of Terrorist Attacks*, H. Richardson, P. Gordon, and J. Moore, Eds. Edward Elgar, Cheltenham, pp. 291–316.
8. Federal Emergency Management Agency (FEMA). (2006). *HAZUS-MH: Multi-hazard Loss Estimation Methodology*. National Institute of Building Sciences, Washington, DC.
9. Multi-Hazard Mitigation Council (MMC). (2005). *Mitigation Saves: The Benefits of FEMA Hazard Mitigation Grants*. National Institute of Building Sciences, Washington, DC.
10. Willis, H. H., LaTourrett, T., Kelly, T. K., Hickey, S., and Neil, S. (2007). *Terrorism risk modeling for intelligence analysis and infrastructure protection*, l, RAND Center for Terrorism Risk Policy.
11. Brashear, J. B. (2009). *Approximating Terrorism Threat Likelihood*. ASME Innovative Technologies Institute, LLC, Washington, D. C. (in press).

# LOGIC TREES: FAULT, SUCCESS, ATTACK, EVENT, PROBABILITY, AND DECISION TREES

ROBIN L. DILLON-MERRILL
*McDonough School of Business, Georgetown University, Washington, D.C.*
GREGORY S. PARNELL
*Department of Systems Engineering, United States Military Academy, West Point, New York*
DONALD L. BUCKSHAW
*Innovative Decisions, Inc., Vienna, Virginia*

## 1 INTRODUCTION

This article provides an introduction to logic trees. Six types of logic trees are described, compared, and illustrated in this article: fault trees, success trees, attack trees, event trees, probability trees, and decision trees. Probabilistic risk analysis (PRA) models may include fault trees, success trees, attack trees, and event trees [1]. Decision analysis

models generally include probability trees and/or decision trees [2]. We illustrate the different models using bioterrorism examples. Table 1 provides a summary of the different logic tree models. The table includes the uses, mathematical foundation, data required, advantages, and limitations.

## 2 FAULT, SUCCESS, AND ATTACK TREES

A fault tree is a graphical probabilistic risk assessment (PRA) technique whereby an undesirable event (called the *top event*) is postulated and the possible ways for this top event to occur are systematically deduced for combinations of initiating and intermediate events [3]. The events are generally binary (or Boolean), that is, events may or may not occur. System components are either in parallel or in series, so combinations of events that lead to failure are identified with logic gates. Figure 1 shows two fault tree diagrams in which the failure of the system depends on two Boolean events. Figure 1a portrays a system that fails when events A *or* B occur, and Figure 1b portrays a system that fails when events C *and* D occur. The Fail block is known as the *top event*, and events A, B, C, and D are basic events. In more complex trees, events in between the top event and the basic events are called *intermediate events*.

Bell Telephone Laboratories developed fault tree analysis in 1961 to support the US Air Force in development of the Minuteman missile system [4]. Others realized the benefits of fault tree analysis and began using the technique for analyzing failures of complex systems. In 1981, the Nuclear Regulatory Commission published the Fault Tree Handbook [5] which remains a valuable resource today. Many others have contributed to development of theory and tools to enable fault tree analysis; Ericson [6] provides a timeline of significant individuals and their contributions up to 1999. Fault trees are useful for assessing risks in almost any uncertain situation, and applications have included software design, space system design, nuclear safety, project management, and information assurance.

Derivatives of fault trees include success trees and attack trees. Fault trees have historically been used to analyze the failure of a system (e.g. the auxiliary water feed system in a nuclear power plant) where the basic events are failures of system components (e.g. tanks, pumps, etc.) and/or acts of nature. A success tree is the complement of a fault tree and models the combination of events that lead to success. Events in attack trees [7] are defined by hostile actions from an adversary against a system. Attack trees (also called *vulnerability trees* [8]) can be used to determine the probability of success, given an attack where the top event is a successful system attack. Additionally, an attack tree used to determine the probability of an attack is often referred to as a *threat tree* [9]. All of these techniques use the basic fault treelike structure and probabilistic relationships between components or events to determine the likelihood of the undesired, top event. Boolean logic and probability remain the foundation of all these models.

Sometimes attack trees can be a mixture of fault and event trees (event trees are described in the next section). The fault tree portion enumerates the cut sets—the smallest number of components that, if they all fail, will lead to system failure—in an efficient manner. Once you have the cut sets, the attacks are treated in a manner similar to the event tree, where sequence matters and the probabilities of events are conditional on the

**TABLE 1 Comparison of Logic Trees**

| Logic Tree | Use | Mathematical Foundation | Data Required | Advantages | Limitations |
|---|---|---|---|---|---|
| Fault tree | Calculate the probability of failure<br>Determine the cut sets | Boolean logic<br>Probability theory<br>Reliability theory | System knowledge<br>failure modes, and probabilities | Focus on components and failure modes | Specialized software |
| Success tree | Calculate the probability of success<br>Determine the cut sets | Boolean logic<br>Probability theory<br>Reliability theory | System knowledge<br>Success modes and probabilities | Focus on success modes | Specialized software |
| Attack tree | Calculate the probability of successful attack<br>Determine the cut sets | Boolean logic<br>Probability theory | System knowledge<br>Adversary knowledge<br>Attack steps and probabilities | Focus on adversary actions | Specialized software |
| Event tree | Calculate the probability of scenarios and consequences | Probability theory | Events Sequencing<br>Outcome spaces | Multiple outcomes<br>Conceptually simple to develop and solve | Binary outcomes<br>Do not appropriately model terrorist decisions. |
| Probability tree | Calculate the probability of any uncertain event in a joint probability distribution | Probability theory<br>Expected value<br>Dominance Bayes' theorem | Events sequencing<br>Outcome spaces<br>Probabilities<br>Consequences | Multiple outcomes<br>Conceptually simple to develop and solve | Large trees are difficult to understand, display, and solve<br>Do not appropriately model terrorist decisions. |
| Decision tree | Identify the best decision strategy under uncertainty | Expected value<br>Dominance Bayes' theorem Bellman optimality principle<br>Utility theory axioms | Events Sequencing<br>Outcome spaces<br>Probabilities<br>Alternatives<br>Consequences | Conceptually simple to develop and solve<br>Can model terrorist decisions | Large trees are difficult to understand, display, and solve |

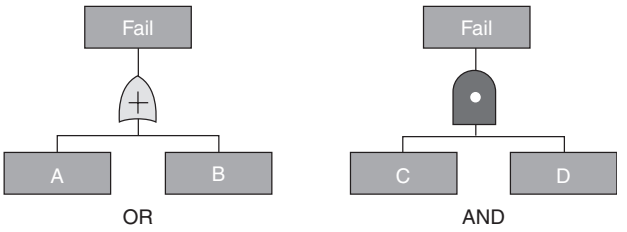



**FIGURE 1** Example fault trees.

previous steps [10]. But, there are many dead-end branches of the event tree that cannot happen given a failure at an early step.

Fault trees are constructed using deductive logic starting at the top event (the failure of all or part of the system) and diagramming the relationships and interactions of events that can constitute a system failure until the system is decomposed into a set of basic events [11]. Each fault tree specifically addresses one top-level system failure; defining this failure is the first step of fault tree construction. The tree is then expanded using "gate" and "event" symbols to logically show the possible events that would lead to the top-level failure. Event symbols represent specific occurrences within the system, such as a component failure; gate symbols describe how lower-level events can be integrated up to higher-level events.

While other logic gates are available, the two basic gate symbols used for fault tree construction are the AND gate and the OR gate. The AND gate demonstrates that the higher-level event (the gate's output) will occur only if all immediate lower-level events (the gate's inputs) occur. Logically, OR gates demonstrate that only one of the gate's inputs must occur for the gate's output to occur. Note that although a gate can have many inputs, gates have only one output.

Fault tree diagrams should be detailed enough to satisfy the scope of the analysis, yet they should be presented such that the relationships between the components are easily understood. Qualitative analysis of fault trees requires determining the minimal cut set(s). This involves a Boolean manipulation of events. The most common algorithm to determine the minimal cut sets for complex fault trees is the successive substitution method (see [5] for algorithm details). In Figure 1a, there are two minimal cut sets with one event each: {A} and {B}. In Figure 1b, there is a single minimal cut set that comprises both events: {C, D}. From this minimal cut set determination, one may qualitatively assess the most important components of a system (i.e. a qualitative ranking of components contributing to system failure) and possible common failure causes.

To conduct any quantitative analysis of the system's reliability, it is necessary to have data on the reliability (i.e. probability of failure) of the system's components, which can then be used to calculate the reliability of the overall system. A quantitative evaluation of a fault tree evaluates the likelihood that the system will fail due to any of the cut sets and all their respective events occurring. Based on a quantitative analysis, one may rank the contributors to system failure and examine the system's sensitivity to component failure data.

For example, in the system in Figure 1a, if A and B are independent events, the system will fail with probability:

$$\mathrm{P(System\ Fail)} = \mathrm{P(A)} + \mathrm{P(B)} - \mathrm{P(A)P(B)}$$

Simplistically, if P(A) is greater than P(B), one may conclude that prevention of event A is more important than prevention of event B in reducing the likelihood of system failure. If C and D are independent events, the system in Figure 1b will fail with probability:

$$P(\text{System Fail}) = P(C)P(D)$$

In the second example, an effective strategy could emphasize making one event extremely unlikely regardless of the likelihood of the other event.

Fault trees (and success and attack trees) have several advantages over purely qualitative techniques for risk assessment. These models are designed to handle complex logical relationships between system components. Where human logic and computational abilities fail to comprehend component interactions when multiple subsystems and components are introduced, fault trees provide concise information about the state of the system and its components and allow rapid calculation of the effects of component changes or changes in system design. As a technique with wide applicability to scenarios requiring decomposition and analysis of system components and sources of failure, fault trees can be valuable additions to any risk assessment task. Some fault tree software packages allow embedding of fault trees within decision analysis models.

In conclusion, fault trees, success trees, and attack trees impose logic and calculate probabilistic interactions between component states to support the analysis of failure, success, and attack scenarios. For complex systems, specialized software is required to support these modeling techniques.

## 2.1 Fault, Success, and Attack Tree Example

Consider an anthrax attack where the delivery mechanism is the US Postal Service. For the attack to be successful, the anthrax package must not be detected.

Suppose the postal service detects anthrax packages either by physical observation or by electronic sensors (see Figure 2). If anthrax packages are to bypass physical protections they must not show any outward threat (i.e. leaking powdery substance) or no one can detect the visible threat. For packages to bypass electronic detection, the package may

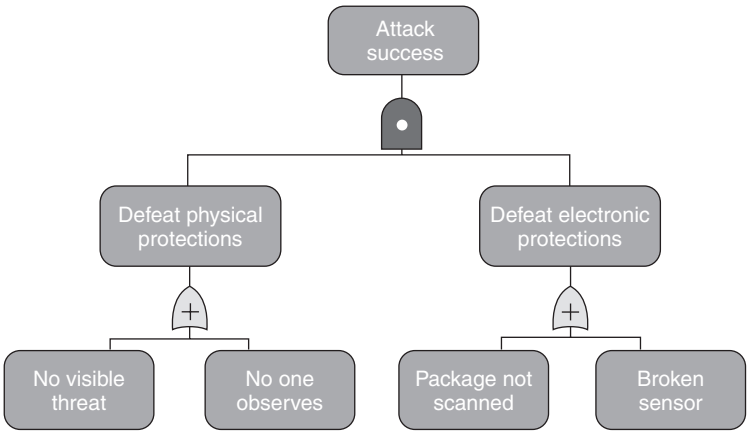



**FIGURE 2** Bioterrorism attack example.

either not be scanned by electronic sensors or the sensors may not be functioning properly. Given a set of event probabilities, we can easily calculate the probability of attack success.

## 3 EVENT TREES AND PROBABILITY TREES

An event tree is a logic tree model for illustrating the sequence of outcomes which may arise after the occurrence of an initiating event. An event tree diagrams the sequences of random events where the chain or path through the tree represents a particular failure scenario and each node represents a binary outcome of success or failure for each event in the scenario. A probability tree is a similar but more general tool than an event tree because in a probability tree, event nodes can have more than binary branches.

Event trees are generally constructed using deductive logic, starting with an initiating event, and then considering the occurrence or nonoccurrence of other possible events, to determine the outcome of each possible failure scenario [11]. The probabilities associated with each additional event (or node) are conditional on all previous outcomes in the tree.

Event trees are useful for structuring failure scenarios because building an event tree addresses all three risk assessment questions (What can happen? What is the likelihood? What are the consequences?). Separate trees can be built for each possible initiating event, where end-path outputs document the chain of events that starts with an event such as an attack and progresses through intermediate events (e.g. loss of a critical infrastructure asset) to determine outcomes and consequences. Event tree analysis was developed in conjunction with fault tree analysis by the nuclear industry [12, 13], and was used to study the operability of nuclear power plants (to include identifying accident sequences in the Three Mile Island-2 accident).

Event trees are commonly integrated with fault trees in a comprehensive risk analysis. In these cases, the left side of the event tree connects to a top event identified by a fault tree, and the right side of the tree with a damage state model (e.g. a plume dispersion model for a dirty bomb). Each node in the tree models the branching probabilities that can be obtained from a system analysis. In contrast to the fault tree, the event tree can easily capture the issue of timing (or evolution) of events. The initiating events used to model event trees are those commonly identified as top events from the fault tree analysis.

Event trees are mainly used in consequence analysis for preincident and postincident application. Because risk assessment frequently requires the systematic identification of all failure (or accident or attack) scenarios, event tree structures provide convenient tools for analyzing families of such scenarios. To quantitatively evaluate an event tree, an event's probability must be assessed conditionally on all prior event outcomes. The probability of any path is the joint probability distribution for the events on that path.

### 3.1 Event and Probability Tree Example

Three nodes are denoted in the example for a bioterrorism event in Figure 3. For such an event to succeed, the terrorist needs to be able to acquire the agent, deliver the agent, and successfully contaminate the surrounding population. In this simple event tree, the probability of a successful bioterrorism attack in a fixed period of time would be calculated as 0.045 (0.05 * 0.30 * 0.50). Consequence models could be used in conjunction with an event tree to model the potential health impacts if contamination is successful.

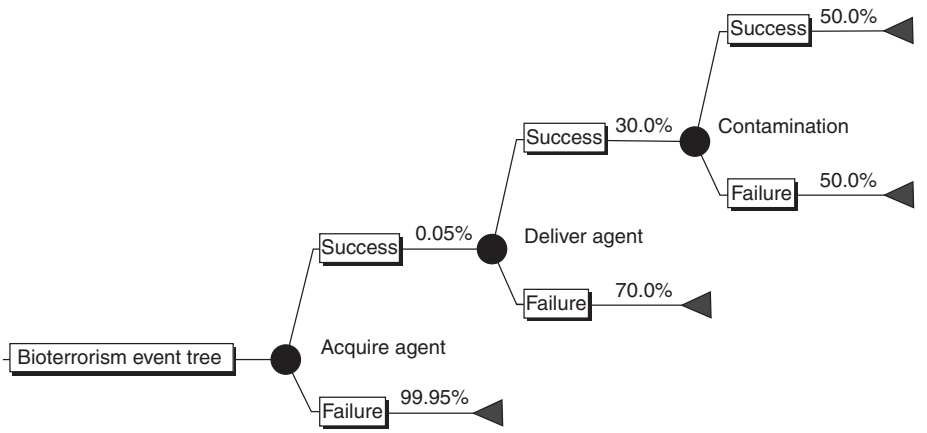



**FIGURE 3** Event tree for bioterrorism event.

## 4 DECISION TREES

Decision trees extend probability trees by including decision nodes among the event nodes [2], where a decision node's branches represent the choices at that node. The decisions and events are logically sequenced in time. To solve a decision tree, one must specify the relevant decision alternatives, the relevant branch probabilities, and the outcome values (sometimes called *consequences*) associated with each path. A decision tree is solved by starting at the right end and working backwards to the base. At each uncertainty node, the expected value of its branches is found, and at each decision node, the branch that maximizes/minimizes the expected value/expected cost is chosen. By taking this approach, the best decisions and their expected values are found. Decision trees work the same way for expected utility [2].

### 4.1 Decision Tree Example

Decision trees expand the modeling capabilities of simple event trees by including decisions such as which agent and/or which target an adversary could choose (See Figure 4). The remaining event nodes (acquire agent, deliver agent, and contamination) would be assessed conditional on the agent and target. In an alternative formulation, we could model the adversary actions as uncertain and add decision nodes interdiction, tests, warning, and treatment decisions. Decision trees would generally include consequences at the terminal nodes of the trees. This allows the risk analyst to calculate the probability distributions for each decision strategy and identify the nondominated decision strategies [2].

## 5 SEEING THE FOREST FOR THE TREES

In this section we discuss the advantages and limitations of each type of logic tree used in decision and risk analysis. Table 1 summarizes the key comparisons of each logic tree based on uses, mathematical foundations, data requirements, advantages, and limitations. We focus our discussion here on the advantages and limitations.

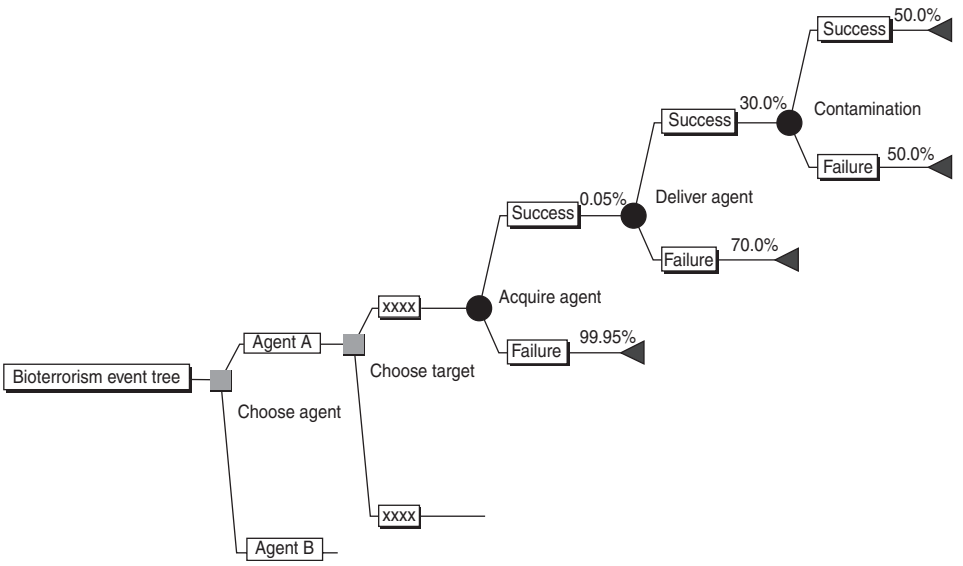



**FIGURE 4** Decision tree for terrorist bioterrorism decisions and events.

### 5.1 Advantages

For event and decision trees: (i) analysis focuses upon paths or scenarios that lead to failure; (ii) analysts can concentrate upon one specific scenario at a time; (iii) results provide a graph that depicts system weaknesses; and (iv) trees serve other risk analysis techniques, such as PRA. These advantages are also true for fault trees. However, unlike fault trees, probability trees can capture complex dependent temporal events that need not be binary. In addition, probability trees can include more than two outcomes and independence assumptions are not required.

### 5.2 Limitations

For event, decision, and fault trees: (i) possibility of overlooking a significant source of failure when building the fault tree; and (ii) difficulties of eliciting probability estimates, particularly where human reliability is concerned [14]. Eliciting adversary attack type and attack target probabilities is problematic. A recent National Research Council study (NRC 2008) recommends not using event trees for terrorist decisions. Another disadvantage of decision trees is that a few decision nodes can quickly make the tree large and complex. For these reasons, an influence diagram [2] is often a better representation of a failure scenario. The requirement for a specialized analysis tool is the primary disadvantage to using fault trees for risk assessment. Use of specialized fault tree software tools typically requires an experienced risk analyst to develop an appropriate model and represent the probabilistic relationships consistently. The necessity to include all relevant factors requires input from multiple stakeholders and many areas of expertise may be time-consuming. Haimes [14] identifies other limitations such as the implausibility of an assumption of independence between component failures.

## 6 RESEARCH CHALLENGES

Logic trees for decision and risk analysis offer several research challenges for homeland security applications: probability elicitation of expert data, appropriate models for intelligent adversary decisions, software to solve large problems and perform value of information for risk analysis, tools to allow collaboration between risk analysts, techniques to integrate logic tree analysis results for resource allocation, and ability to compare risk analysis between risk areas.

### 6.1 Probability Elicitation of Expert Data

Probability elicitation of expert data is a common challenge in decision and risk analysis. Tversky and Kahneman show that subject-matter experts are subject to several biases which can lead to poor probability estimations [15]. Fischhoff suggests elicitation support techniques that might be promising in helping experts avoid many of the biases [16]. But few have shown any value in minimizing the biases. Of more concern is a study by Weiss and Shanteau [17] that showed that intelligence analyst probability estimates were better than flipping a coin but their judgments could be highly suspect and should be used with caution. Buede et al. [18] reviewed the literature and recommended best practices for probability elicitation and aggregation of multiple expert assessments; however, more work is required to test the recommendations through controlled experimentation.

### 6.2 Models for Intelligent Adversary Decision Making

Intelligent adversaries determine their actions based on their capabilities, the defensive system capabilities, the risk they are willing to take, and the consequences they hope to achieve. Modeling terrorists involves the types of adversaries (e.g. nation state, international terror organization, or individuals), the capabilities of adversaries, the type of attack, the probability of attack, the type of target, the attack location(s), and the timing of attack. Given the challenges of eliciting expert data for the states of nature, the challenges of Modeling intelligent actors are much more problematic. Promising approaches to modeling intelligent adversaries include terrorist decision analysis models, attacker-defender-attacker optimization models, game theory [19], and red teams (NRC 2008).

### 6.3 Software to Solve Large Logic Trees

Homeland security problems involve complex systems with many interactions and many ways that intelligent adversaries may attempt to defeat the system defenses and achieve the consequences they desire. To defeat these potential attacks, homeland security analysts will need to understand the adversaries' capabilities, the potential targets, target vulnerabilities, consequences of these attacks, and potential mitigation strategies. The PRA software should integrate consequence models with decision trees and should be able to perform value of information calculations [2] on uncertain information.

### 6.4 Software to Solve Large PRA Combined with Decision Analysis

Homeland security decision makers need to make resource allocation decisions. They will need to evaluate several countermeasures to assess their potential to reduce the likelihood

of attack, reduce the vulnerabilities, and/or mitigate the consequences. We may need to develop new software to solve the large decision trees and determine the best portfolio of design changes and countermeasures for the resources available. An information assurance example of this capability is the Microsoft Excel and Access implementation of the mission-oriented risk and design analysis (MORDA) process used by the Department of Defense [10] that can be improved through professional software development.

### 6.5 Collaborative Risk Analysis

Many of our critical infrastructure are interdependent. Information technology connects and enables the efficient operation of many of our infrastructure. For example, Supervisory Control and Data Acquisition (SCADA) systems are used to manage many of our infrastructure; and information enabled transportation systems are critical for the efficient operation of many infrastructure. Independent risk analysis wastes resources (e.g. multiple organizations analyzing the same systems); may miss the risk associated with interdependent systems due to lack of system knowledge; may lead to suboptimal decisions (e.g. one organization selecting an inefficient countermeasure when collaboration could result in a more efficient use of resources); and may lead to risk transfers (e.g. a simple reprioritization of the adversaries target selection). We will need to develop a standard risk analysis lexicon and allow collaborative risk analyses. Collaborative risk analyses would share information and allow for the most efficient risk analysis (both risk assessments and risk management actions). Collaborative risk analyses will require the sharing of information between private and public organizations and between government agencies, including federal, state, and local governments.

### 6.6 Ability to Compare Risk Analyses between All-hazards

The Department of Homeland Security (DHS) has the responsibility of securing the homeland against all hazards. In order for the DHS to make an efficient allocation of risk assessment and risk management resources, the risk analysis results must be communicated in a manner that allows the DHS and oversight organizations to assess the relative risk for all hazards and the cost-effectiveness of mitigation actions. A critical first step would be to require all risk assessment results to be presented in comparable formats (e.g. the risk of bioterrorism and the risk of chemical spills would be comparable). The second critical step would be to require that all risk management actions be compared with the reduction in risk per dollar spent.

## REFERENCES

1. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*, Chapman and Hall/CRC, London.
2. Clemen, R. T. (1996). *Making Hard Decisions*, 2nd Ed., Duxbury Press. Belmont, CA.
3. Modarres, M. (1993). *What Every Engineer Should Know About Reliability and Risk Analysis*, Marcel Dekker, Inc., New York.
4. Watson, H. A. (1961). *Launch Control Safety Study*, Section VII, Volume 1, Bell Labs, Murray Hill, NJ.
5. U.S. Nuclear Regulatory Commission (1981). *Fault Tree Handbook. NUREG-81/0492.*

6. Ericson II, C. A. (1999). *Course No. 9Sv276 Fault tree analysis student workbook, D&SG Employee Training and Development*, The Boeing Company. Seattle, Washington.
7. Schneier, B. (1999). Attack trees: modeling security threats. *Dr. Dobbs J. Softw. Tools* **24**(12), 21–29.
8. Unkenholz, W. (1989). *Vulnerability Tree Analysis Method*, Unpublished Manuscript.
9. Amoroso, E. (1994). *Fundamentals of Computer Security Technology*, Prentice-Hall, Englewood Cliffs, NJ.
10. Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., Wallner, J. M., and Saydjari, O. S. (2005). Mission oriented risk and design analysis of critical information systems. *Mil. Operat. Res.* **2**(10), 19–38.
11. Paté-Cornell, M. E. (1984). Fault trees vs. event trees in reliability analysis. *Risk Anal.* **4**(3), 177–186.
12. U.S. Nuclear Regulatory Commission (1975). *Reactor safety study, WASH-1400 (NUREG-75/014)*, Washington, DC.
13. U.S. Nuclear Regulatory Commission (1983). *PRA procedures guide (NUREG/CR-2300)*, Washington, DC.
14. Haimes, Y. Y. (1999). *Risk Modeling, Assessment, and Management*, John Wiley and Sons, Inc., Hoboken, NJ.
15. Tversky, A., and Kahneman, D. (1974). Judgment under uncertainty: heuristics and biases. *Science*. **185** (1124–1131).
16. Fischhoff, B. (2002). Heuristics and biases. In *Application in Heuristics and Biases: The Psychology of Intuitive Judgment*, Gilovich, Griffin and Kahneman, Eds. Cambridge University Press. New York.
17. Weiss, D. J. and Shanteau, J. (2003). The vice of consensus and the virtue of consistency. In *Psychological explorations of competent decision making*, J. Shanteau, P. Johnson, and C. Smith, Eds. Cambridge University Press, New York.
18. Buede, D. M., Mahoney, S. M., Ulvila, J. W., and Smith T. C. (2006). *Review of Probability Elicitation and Examination of Approaches for Large Bayesian Networks. U.S. Department of Defense*, Unpublished Manuscript.
19. Hausken, K. (2002). Probabilistic risk analysis and game theory. *Risk Anal.* **22**(1). Available at http://www1.his.no/vit/oks/hausken.
20. Report on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis: A Call for Change, Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis, National Research Council of the National Academies, The National Academy Press, Washington, DC, (2008).

## FURTHER READING

Bedford, T. Cooke R. (2001). *Probabilistic Risk Analysis: Foundations and Methods*, Cambridge University Press, Cambridge, UK.

Kumamoto, H. and Henley, E. J. (1992). *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis*, IEEE Press. New York.

Parnell, G. S., Dillon-Merrill, R. L., Bresnick, T. A. (2005). *Integrating Risk Management with Homeland Security and Antiterrorism Resource Allocation Decision-making*, D. Kamien, Ed. The McGraw-Hill Handbook of Homeland Security, New York, pp. 431–461.

von Winterfeldt, D., and Rosoff, H. (2005). *Using Project Risk Analysis to Counter Terrorism*, Symposium on Terrorism Risk Analysis, Los Angeles, CA.

# BAYESIAN NETWORKS

DENNIS BUEDE, SUZANNE M. MAHONEY, AND JOSEPH A. TATMAN
*Innovative Decisions, Inc., Vienna, Virginia*

## 1 INTRODUCTION

Bayesian networks (BNs) may be used to address Department of Homeland Security (DHS) needs ranging from identifying and tracking suspect individuals to analyzing vulnerabilities and providing warning of attack. BNs factor complex problems into manageable networks of random variables. The graphical interface of BNs facilitates explanation while the local nature of the probabilistic relationships facilitates assessment. Computational algorithms provide rapid evaluation of available evidence to support decision-making in complex and evolving situations.

Section 2 provides a brief introduction to BNs while Section 3 provides some insight into the worldwide research community. The next section describes the application of BNs to meet DHS' critical needs. In the final section, research goals relevant to meet DHS's critical needs are summarized.

## 2 SCIENTIFIC OVERVIEW

This section presents the basics of BNs. This is followed by a section on inference (or computation). The issue of obtaining the probabilistic inputs for a model is described under knowledge acquisition.

### 2.1 Modeling with Bayesian Networks

A BNs is a factorization of a joint probability distribution. An acyclic directed graph specifies the network's structure. Nodes stand for random variables. Directed arcs indicate probabilistic dependence. Lack of an arc indicates probabilistic independence. A BNs stores parameters with each node in the form of a conditional probability table (CPT). A CPT contains distributions of a dependent/child variable given possible combinations of its conditioning/parent variables. Given its parents, each random variable is independent of its nondescendants [1].

Practitioners often use BNs to model uncertain situations. Frequently, these models follow the pattern shown in Figure 1. *Domain uncertainty* applies to hypotheses and their observables. Four types of random variables represent the domain of interest.

- *Context* that is broadly defined includes the random variables whose values are usually known when the problem arises, but not when the model is built. Context potentially influences all other variables in a network. In a medical application, context may include a patient's gender and age. In an information assurance application, context would include operating system and software.

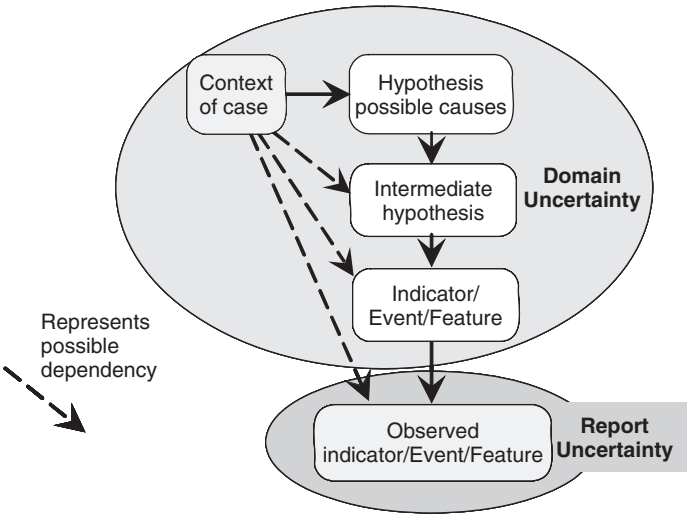



**FIGURE 1** Pattern for a Bayesian network.

- *Hypothesis/Possible Causes* variables are the variables of interest in a network whose purpose is diagnosis. Examples include diseases in a medical diagnostic network, possible information attack plans in an information assurance network, faults in an equipment repair application, and types of bombs in a bomb detection application.
- *Intermediate hypotheses* provide support to one or more of the hypotheses. Examples include plan steps of an information attack and detectable components of a dirty bomb.
- *Indicator/Events/Features* are those elements of a situation that are observable. Examples include symptoms of diseases, equipment readings (e.g. level of $\gamma$ rays), and airline passenger behavior. These are often the variables of interest in networks whose purpose is prediction.

Observations are subject to *report uncertainty*. In addition to depending upon the context of the domain and the indicator/event/feature being observed, observations also depend upon characteristics of the observer. For example, a sensor is limited by its inherent sensitivity (whether it can detect an event when the event is present) and specificity (how often it detects an event when the event is not present). Human reports are influenced by the ability of the observer to make the observation, whether the observer actually believes his/her observations and whether the observer is lying.

## 2.2 Applying Bayesian Networks

Inference in a BNs flows throughout the network. Consequently, a network may be used for multiple purposes. For example, in a medical application one uses test results and symptoms to diagnose the disease. In this case one makes inferences about the hypotheses, given the observations of the disease indicators. This is the typical diagnostic application. At the same time, one may make inferences about unobserved disease indicators or how

a probable disease is likely to progress over time. In this case, one is using the same network for prediction or what-if evaluation.

The BN's structure and parameters represent a knowledge base about a problem of interest. For example, the structure of a disease network shows that colds and allergies share some of the same symptoms. The parameters of the network indicate how much more likely a fever is with a cold than with an allergy.

In applying BNs to real world applications the evidence or observations may come from a variety of sources. Evidence may be stored in a database or generated by a simulation or entered in real-time by a human observer or received from a sensor. Because BNs provide a general framework for representing uncertainty, they are excellent models for multisensor fusion.

### 2.3 Example

Figure 2 shows a small BNs that collects information about passengers boarding a public conveyance. The network's purpose is to decide whether a passenger is "of interest" and should therefore be subject to further screening.

The node in the upper right hand corner supplies the context "passenger screening". The nodes above the line across Figure 2 reflect domain uncertainty. The "passenger" node is the hypothesis. There are no intermediate hypotheses in this network. The three other nodes above the line are observable features. Representing report uncertainty, the node "reported behavior" is an observation of the "suspicious behavior" node. The "observer quality" node conditions how well an observer's report matches the observed behavior.

Each node displays the random variable's possible values or states with their associated probability (displayed as percents in the nodes of Figure 2). As evidence about nodes in the network is accumulated the probabilities are updated by the inference algorithm.

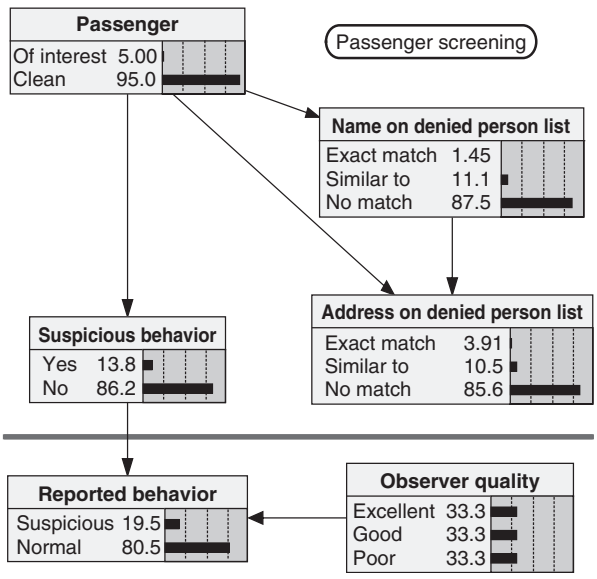



**FIGURE 2** Passenger screening network.

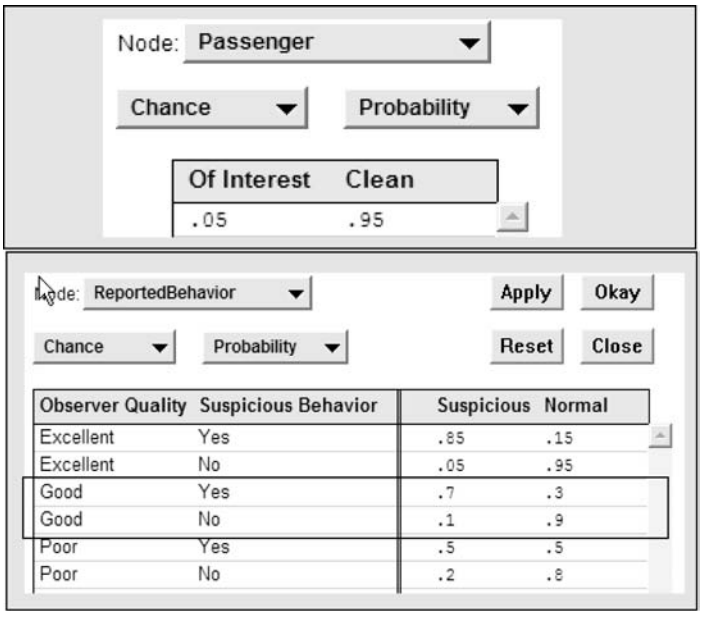



**FIGURE 3** Conditional probability tables for the passenger screening network.

Figure 3 shows two of the passenger screening network's CPTs. The top CPT, belonging to the "passenger" node, displays a single distribution indicating that about 5% of passengers are of interest. The bottom CPT is for the node "reported behavior"; it depends on two other nodes. The states of these other two nodes are displayed on the left side of the CPT. The CPT represents the probability of an expert of a specified quality making a particular observation given the true state of the observed behavior. The portion of the CPT outlined by the box displays the distributions associated with a good observer. For passengers exhibiting suspicious behavior, the good observer is correct 70% of the time while, for passengers behaving normally, the observer is correct 90% of the time.

Figure 4 shows two instances of the passenger screening network. Each shows some nodes set to specific values. Compare the displayed probability distributions of these networks with the ones in Figure 2. The instance on the left shows how the probabilities in the unobserved nodes change when we note that a passenger's name and address are similar to ones on the denied persons list. This evidence not only changes the probabilities of the hypothesis node "passenger" but also the probabilities of the nodes "suspicious behavior" and "reported behavior". This reflects our belief that persons who may be on the denied person list are more likely to exhibit suspicious behavior. At the same time, this knowledge about the passenger does not change our belief about the quality of the observer. Many people have names similar to those in the database, so we also observe the passenger's behavior before making a decision to subject the passenger to further screening. As shown in the network on the right side of Figure 4, the observation of suspicious behavior by a good quality observer raises the probability of the passenger being of interest to 69%. In this case, the quality of the observer makes a difference in the probabilities of the unobserved nodes. A poor observer would produce a probability of only 54% that the passenger is of interest.

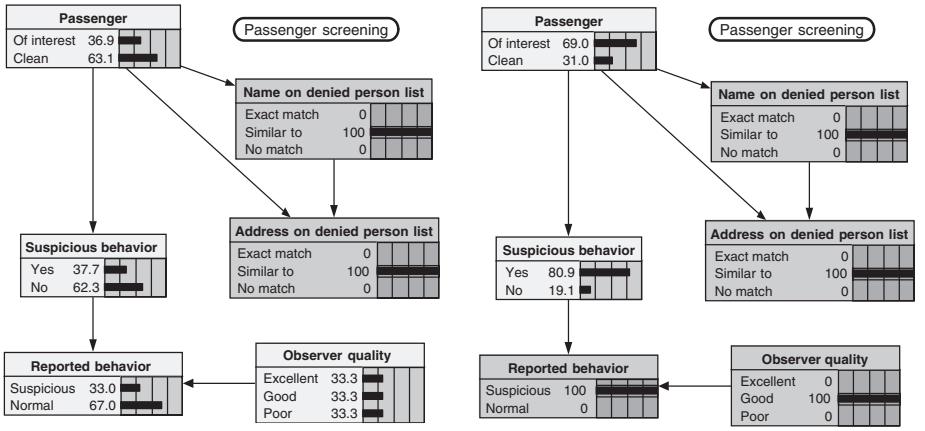



**FIGURE 4** Passenger screening network with observations.

## 2.4 Bayesian Network Structures

For many applications of BNs, networks similar to those in Figure 1 are reused for different entities (passengers). With each reuse the evidence of previous uses is cleared and new evidence is entered. This is an example of a template model. When in use, the network's structure and parameters remain fixed and unchanging. Only the evidence regarding the current circumstance differs from one use to the next. Other usage examples are dynamic Bayesian networks (DBNs) and situation-specific networks. DBNs [2] are specifically designed to model cases in which the situation changes over time in a predictable fashion. Situation-specific BNs [3] are constructed by pulling network fragments from a knowledge base in response to evidence and context about the situation being modeled. Unlike template networks, DBNs and situation-specific BNs extend the structure of a BNs to include additional variables. Like template networks, the parameters associated with the variables remain unchanged.

## 2.5 Inference

A BNs factors the joint probability distribution so that any query about joint/marginal probability distributions in a BNs can be computed by the product of all CPTs found in the BNs followed by the marginalization of the variables not in the query. For example the joint probability distribution of the network shown in Figure 2 is computed from the following product:

$$
\begin{aligned}
&P(\text{Passenger, Name on Denied Person List, Addresson Denied Person List, Suspicious Behavior Observer Quality, Reported Behavior}) \\
&= P(\text{Passanger}) \times P(\text{Name on Denied Person List} \mid \text{Passenger}) \\
&\quad \times P(\text{Name on Denied Person List} \mid \text{Name on Denied Person, Passenger}) \\
&\quad \times P(\text{Suspicious Behavior} \mid \text{Passenger}) \\
&\quad \times P(\text{Observer Quality}) \\
&\quad \times P(\text{Reported Behavior} \mid \text{Suspicious Behavior, Observer Quality}).
\end{aligned}
$$

Pearl's algorithm [1] applied a message passing approach to a BNs whose structure was a polytree. In a polytree there is exactly one path from one node to another. To solve BNs, whose graphs are not polytrees, researchers have taken two different approaches to convert such networks to polytrees. Graph theoretic approaches use the topology of the graph to cluster nodes into a junction tree [4], while algebraic approaches consider the nature of the query and evidence [5].

The worst-case complexity of any exact inference algorithm is known to be NP-hard [6]. Hence, researchers have also turned to approximate inference algorithms. Existing approximate BNs inference algorithms fall into three major categories.

- *Monte Carlo sampling* algorithms estimate a posterior probability distribution (the target distribution) by sampling from another computationally simpler probability distribution (the sampling distribution). Sampling algorithms include: logic sampling, Gibbs sampling, likelihood weighting, and adaptive importance sampling [7]. For DBNs, particle filtering [8] algorithms represent the past expression, a summary of all past observations, by a set of samples called *particles*.
- *Dependency reduction* algorithms weaken or ignore some of the dependencies among nodes. The iterative belief propagation algorithm, also known as *loopy belief propagation* [9], applies Pearl's belief propagation algorithm for singly connected BNs to loopy networks. For DBNs, Boyen and Koller [10] factorize the past expression into a set of smaller tables by ignoring the dependencies among some interface variables.
- *Variational* methods fit an approximating distribution to the true posterior [11].

Many approximate algorithms exhibit an anytime property, which offers the user the control of the trade-off between the cost and accuracy. The complexity of the approximate inference algorithms to obtain the desired accuracy is also known to be NP-hard [12].

### 2.6 Knowledge Acquisition

Knowledge acquisition includes the following activities: identify the structure of the BNs; assess its parameters; and evaluate the resulting network. Sources of knowledge include both subject matter experts and available data. One advantage of a BNs is that both sources can be combined by treating expert knowledge as an equivalent number of data cases.

### 2.7 Eliciting Knowledge from Experts

When obtaining knowledge from experts, the facilitator is presented with a number of challenges. Experts arrive with different amounts and types of expertise. Furthermore, the elicitation method may be unfamiliar to the experts, making communication between the elicitor and the experts difficult. In addition, humans have biases that may skew the elicitation process. Among these are overconfidence, extrapolating population statistics from small samples, and adjusting probabilities too little given an initial value. Reliability studies have found that experts dealing with scientific areas are the most reliable while those working with human activities are the least reliable.

Methods for eliciting probabilities and distributions have been researched for more than 40 years. Initially, the emphasis was on eliciting probabilities for single events.

With the introduction of BNs, populating CPTs became a concern. Generally, a facilitator elicits probabilities from experts. However, the requirement to fill numerous CPTs in large BNs and the capability to develop graphical user interfaces have led to the use of computer-supported graphical tools.

Eliciting the structure of BNs has received little research attention. Causal structures have been recommended as a way of minimizing network complexity. Others recommend an iterative object-oriented approach. Various researchers have noted patterns that appear regularly in BNs.

### 2.8 Learning from Data

The problem of learning a BNs from observations can be decomposed into the tasks of searching over possible structures, estimating the CPTs given the structure, and scoring the structure given the data [13].

1. Search efficiently over the large number of possible structures to find a subset of good structures.

   There are an exponentially large number of possible structures for a given set of variables. The K2 algorithm [14] applied a simple heuristic hill-climbing search. It compared the posterior probability of the structures that differed by a single arc added to the network. More recent approaches use genetic algorithms and Markov Chain Monte Carlo (MCMC) to search over possible structures.
2. Estimate the local probability tables for a given structure.

   Cooper and Herskovits [14] developed the first algorithm for joint estimation of structure and parameters for the discrete variable case. The discovery of more general estimation methods for mixtures of graphical models is an active area of research.
3. Estimate the relative posterior probabilities of any subset of structures.

   Most algorithms assume a uniform probability across all structures. The structure score is an estimate of how well it explains the data. The posterior probability of the structure is calculated from

$$P(D) = \sum_{S_c} P(D/S_c).P(S_c)$$

   where $S_c$ is the structure being considered and $D$ is the data. The term $P(D|S_c)$ is calculated directly from a proposed network.

In cases of incomplete or missing data, one commonly applied approach is the expectation maximization (EM) algorithm [15]. EM applies when data are “missing at random”. The EM algorithm is guaranteed to converge to a local optimum. An alternative option is to simulate missing observations along with structures in an MCMC algorithm.

## 3 RESEARCH AND FUNDING DATA

Research into BNs began in the middle of the 1980s. There have been at least 20 books written on this topic since 1988. There are active research programs on the topic at the

most prestigious universities (e.g. MIT, Stanford University, Harvard University, University of Cambridge, and Oxford University) as well as many other universities around the world. There are several major conferences that address BNs: Uncertainty in Artificial Intelligence (http://www.auai.org/), Florida Artificial Intelligence Research Society (http://www.flairs.com/), and Artificial Intelligence and Statistics (http://www.stat.umn.edu/~aistat/index.html). Finally the major IT companies around the world are investing heavily in the use of BNs for their product development: Microsoft, Yahoo, IBM, Boeing, Google, and Intel.

Current research topics reported across several conferences and journals include the following.

- Advanced algorithms for difficult networks, for example compiling graphical models.
- Advanced modeling techniques, for example dealing with non-Gaussian continuous variables.
- Advanced software implementations, for example sensitivity analysis and user friendliness for naïve users.
- Advanced learning techniques.
- Improved elicitation of expert's probabilities.
- Development of ontologies for probabilistic reasoning.
- Causal reasoning on the basis of probabilistic modeling.

More applied research deals with applications of BNs to

- user modeling;
- cognitive agents and practical robots for network management, unmanned robots, computer games, educational games, and sensor management;
- sensor fusion;
- forensic science;
- reliability models;
- spam filters;
- biologic systems;
- cyber attacks and user behavior;
- decision support to military commanders;
- gene expression;
- combining BNs and social networks to address predicting organizational activities and responses to changes.

Funding sources for research into the theory and application of BNs includes corporations, government agencies and foundations. Current corporate funding comes from

- Microsoft
- Yahoo
- IBM
- Boeing

- Google
- Intel
- Siemens
- Toyota
- SAIC.

Funding from government agencies in the United States comes from:

- ONR
- NSF
- Air Force
- JPL/NASA
- DARPA
- NASA
- Federal Aviation Administration
- National Library of Medicine
- National Institute of Health.

Funding from governments around the world comes from:

- Academy of Finland
- Finnish Funding Agency for Technology and Innovation
- Netherlands Organization for Scientific Research
- German Research Foundation
- Norwegian Academy of Science and Letters
- Israel Science Foundation
- US–Israel Binational Science Foundation
- National Sciences and Engineering Research Council of Canada
- Canada Foundation for Innovation
- Ministry of Education, Culture, Sports, Science, and Technology of Japan
- Swedish Research Council
- Swedish Foundation for Strategic Research
- Information Societies Technologies (IST) Programme of the European Commission
- Dutch Ministry of Economic Affairs.

Foundations supporting BNs research are:

- Leverhulme Trust, UK
- Rothschild Foundation
- Sumitomo Foundation
- Kayamori Foundation of Information Science Advancement
- Japan Society for the Promotion of Science
- James S. McDonnell Foundation Causal Learning Collaborative

- Sloan Foundation
- Gatsby Charitable Foundation
- Minerva Foundation
- Ridgefield Foundation

## 4 CRITICAL NEEDS ANALYSIS

Two major classes of BNs are relevant for DHS. Diagnostic networks are useful for a broad array of problems involving a set of hypotheses and a collection of evidence that distinguishes among the hypotheses. They provide a probability distribution over the set of hypotheses given any combination of evidence. An example is the passenger screening network shown in Figure 2. The "passenger" node provides the hypotheses. Its probability distribution is updated as findings are entered into the evidence nodes such as "name on denied person list". Predictive networks have one or more output nodes with probabilistic relationships to a set of input nodes as in Figure 5. The CPT of the output node accounts for dependencies among the states of the input nodes. In Figure 5, the output node, "structural failure", is predicted by the combination of possible values of the other nodes in the network.

The next paragraphs discuss four critical needs of DHS. These needs are relevant to two major functions of DHS, counterterrorism and border control.

### 4.1 Indications and Warnings

The DHS strategic plan states that "The prevention of terrorist attacks is the first priority in securing our homeland." Key to preventing an attack is obtaining a warning that such

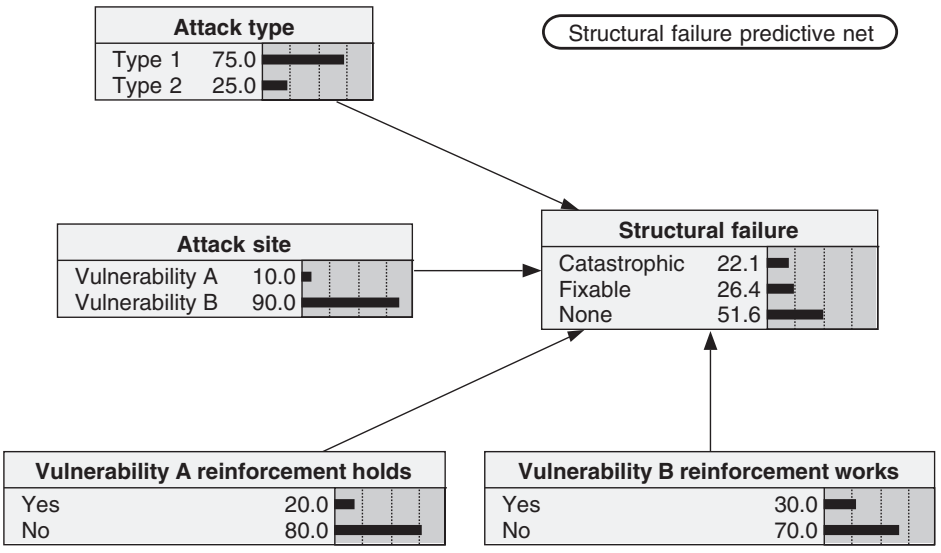



**FIGURE 5** Predictive bayesian network.

an attack is planned. To do so, one must combine many disparate indicators in a way that lends support to whether or not such an attack is planned.

The diagnostic class of BNs offers an effective, systematic framework for integrating diverse sets of data. The hypotheses are whether or not an attack is being planned and the stage of development of the plan. The indicators include events such as the purchase of specific types of materials, communication between persons who may have terrorist leanings and known terrorists, experimentation by suspected terrorists with specific items that could be used for weapons, and anomalous behavior of suspected terrorists.

In actual applications, BNs have been applied to understanding adversary intent in international crises, detecting deception by an adversary, and in decision support tools that predict enemy attacks for battlefield commanders. These examples demonstrate that indications and warning is a high impact, high probability of success application of BNs.

### 4.2 Assessment of Information Quality

The DHS strategic plan recognizes the need for integrating information received from diverse sources ranging from humans to electronic sensors and coming from all levels of government. BNs effectively address two problems here. The first problem is the need to combine information from diverse types of sources (as in the "indications and warning" discussion). The second problem is the reliability of human reporting.

The diagnostic class of BNs is relevant for both problems. Such a BNs has a hypothesis node that represents the event being reported. One evidence node (of possibly many) is the human report. In this case the link between hypothesis and evidence (or report) is decomposed into nodes representing the competence and credibility of the source. It further breaks down credibility into sensitivity, objectivity, and veracity, see Figure 6. The BNs facilitates calculation for this complex problem. BNs provide a methodology for integrating information not only from multiple human sources but also from traditional

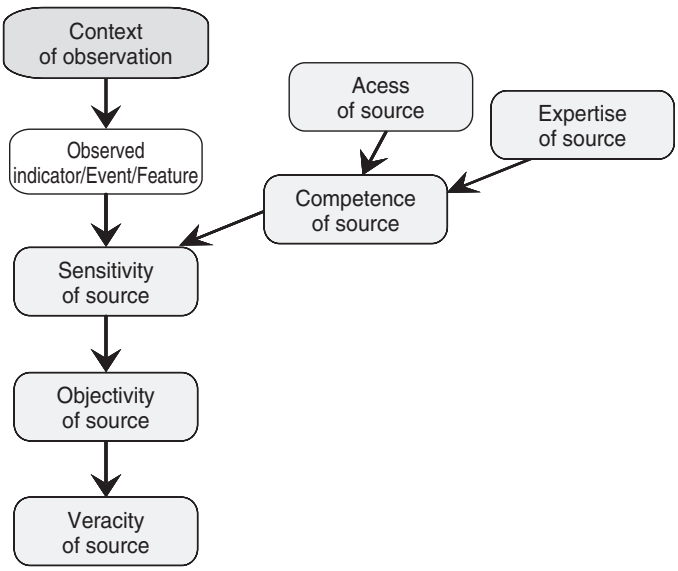



**FIGURE 6** Source credibility model.

sensors. Their application to the assessment of information quality is rigorous and proven in real world applications [16].

### 4.3 Analyze Risks and Vulnerabilities

A top priority in implementing the DHS strategic plan is a framework for continuously assessing what can go wrong, the likelihood of occurrence, and the potential consequences. Also, a strategic objective asserts that risk-based analytic tools will be used to help prioritize projects to protect critical infrastructure.

Such risk assessment and analysis is a natural application for the predictive class of BNs. The variable of interest in a risk application could be the level of damage to a critical building as in Figure 5. This level of damage depends on many random events or variables, such as the nature of the attack, the location of the attack, or the degree of training of security personnel.

BNs have been successfully applied to the risk analysis of major engineering development projects. The impact of many uncertain variables on the timing and cost of successful project completion had to be considered. In another application, assessments performed by a large number of experts on the safety level of a critical software-intensive system were integrated [17].

The level of complexity and the factors modeled in these applications indicate that they can be extended to meet DHS's vulnerability and risk assessment needs.

### 4.4 Identify and Track Suspect Persons

Critical to counterterrorism is the ability to identify and track individuals. Identifying the suspect in a scene is a natural application for a diagnostic BNs. The network is used to assimilate many bits of evidence about the suspect to make an identification. On the other hand, a predictive BNs can be applied to track a person. The variable of interest may be the person's location during a specific time period. Such a location would be a probabilistic function of the person's location during a previous time period and other uncertain factors such as the receipt of a cell phone call.

One application automatically tracks a varying number of people exposed to an advertisement, and determines whether they looked at the ad. A hybrid dynamic BNs simultaneously infers the number of people in the scene and their body and head locations [18]. Another application is a tracking algorithm that can identify and track distinct individuals in a scene and recover when it loses track [19].

These applications, while limited, provide a starting point in attacking this difficult problem.

### 4.5 Summary

A broad collection of DHS critical needs may be addressed using BNs. BNs are a natural, effective solution for problems involving uncertainty and the integration of evidence from diverse sources. They provide a powerful probability calculator for problems requiring the calculation of risk. Finally, BNs balance mathematical rigor with a capability to analyze messy real world problems involving uncertainty, while providing an intuitive modeling front-end for most decision makers.

## 5 RESEARCH DIRECTIONS

Homeland security is exemplified by intelligent adversaries and evolving science and technology. These characteristics mean that what is true or likely today may not be true or likely tomorrow or next week and certainly not true or likely next year. Such a domain is difficult for any human reasoning, whether qualitative or quantitative. Those approaches that use modular building blocks that can be swapped in and out relatively easily are the most likely to provide rapid and useful support. BNs certainly fall into this category. But achieving the benefits of this type of an approach is not easy or readily available.

A sample of research directions for dealing with domains that have dynamic expertise are:

- extend the theory behind model fragments;
- develop adaptive learning algorithms that make use of limited data;
- develop graphical user interfaces to facilitate the capture of expertise from humans.

In addition to homeland security having a dynamic base, there is a tremendous amount of complexity. This complexity includes technology interactions such as incompatibilities among communication devices, as well as finding the right sequence of activities during a catastrophe that will save the most lives. Most of this complexity is present because of the need to harness hundreds or thousands of humans together to work as a team when they have never performed as a team before in dealing with a situation never before envisaged. Automated reasoning tools (including BNs) can be used both to increase the productivity of individuals as well as to manage the team effort more effectively.

A sample of research directions for dealing with large, complex domains are:

- develop more adaptable connections between BNs and other modeling tools, for example simulation packages and spread sheets;
- embed BNs in radios, personal digital assistants (PDAs), and so on.

## REFERENCES

1. Pearl, J. (1988). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann, San Mateo, CA.
2. Murphy, K. (2004). Dynamic Bayesian networks. Proposed chapter in *Probabilistic Graphical Models*, M. Jordan, Ed. http://www.cs.ubc.ca/~murphyk/Papers/dbnchapter.pdf.
3. Wellman, M. P., Breese, J. S., and Goldman, R. P. (1992). From knowledge bases to decision models. *Knowl. Eng. Rev.* **7**(1), 35–53.
4. Lauritzen, S., and Spiegelhalter, D. (1988). Local computations with probabilities on graphical structures and their application to expert systems. *J. R. Stat. Soc.* **B 50**, 157–224.
5. Dechter, R. (1996). Bucket Elimination: A unifying framework for probabilistic inference. *Proceedings of UAI-96*. Portland Oregon, August. http://www.ics.uci.edu/~dechter/publications/.
6. Cooper, G. F. (1990). The computational complexity of probabilistic inference using Bayesian belief networks. *Int. J. Artif. Intell.* **42**, 393–405.
7. Shachter, R. D., and Peot, M. A. (1989). Simulation approaches to general probabilistic inference on belief networks. *Proceedings of the Fifth Workshop on Uncertainty in Artificial Intelligence*. Santa Cruz, CA, pp. 311–318.

8. Doucet, A., deFreitas, N., Murphy, K., and Russell, S. (2000). Rao-Blackwellised particle filtering for dynamic BNs, *UAI-00*. www.foi.se/fusion/fusion24.ps.
9. Murphy, K., Weiss, Y., and Jordan, M. (1999). Loopy-belief propagation for approximate inference: an empirical study. *Proceedings of UAI-99*. http://citeseer.ist.psu.edu/murphy99loopy.html.
10. Boyen, X., and Koller, D. (1998). Tractable inference for complex stochastic processes. *Proceedings of the Conference on Uncertainty in AI*. http://ai.stanford.edu/~koller/papers/nips98.html.
11. Jaakkola, T. S., and Jordan, M. I. (1996). Recursive algorithms for approximating probabilities in graphical models. In *Advances in Neural Information Processing Systems*, 9. http://people.csail.mit.edu/people/tommi/inf.html.
12. Dagum, P., and Luby, M. (1993). Approximating probabilistic inference in Bayesian belief networks is NP-hard. *National Conference on Artificial Intelligence*. Washington, DC.
13. Heckerman, D. (1999). A tutorial on learning with Bayesian networks. In *Learning in Graphical Models*, M. Jordan, Ed. MIT Press, Cambridge, MA.
14. Cooper, G. F., and Herskovits, E. (1992). A Bayesian method for the induction of probabilistic networks from data. *Mach. Learn.* **9**, 309–347.
15. Lauritzen, S. L. (1995). The EM algorithm for graphical association models with missing data. *Comput. Stat. Data Anal.* **19**, 191–201.
16. (a) Schum, D. (1989). Knowledge, probability, and credibility. *J. Behav. Decis. Mak.* **2**, 39–62; (b) Schum, D. (1992). Hearsay from a layperson. *Cardozo Law Rev.* **14**(1), 1–77.
17. Bouissoum, M., and Nguyen, T. (2002). Decision making based on expert assessments: use of belief networks to take into account uncertainty, bias, and weak signals. *Proceedings of the Lambda Mu 13/ESREL Conference*. perso-math.univ-mlv.fr/users/bouissou.marc/ExpertsAndBN_ESREL02.pdf.
18. Smith, K., Ba, S., and Gatica-Perez, D. (2006). Tracking the MultiPerson wandering visual focus of attention. *International Conference on Multimodal Interfaces*. www.idiap.ch/~smith/SMITH_ICMI06.pdf.
19. Ramanan, D., and Forsyth, D. A. (2003). Finding and tracking people from the bottom up. *Proceedings Computer Vision and Pattern Recognition (CVPR)*. www.cs.berkeley.edu/~ramanan/papers/trackingpeople.pdf.

## FURTHER READING

Howson, C., and Urbach, P. (2005). *Scientific Reasoning: The Bayesian Approach*, Open Court Publishing Company, Chicago, IL.

Jensen, F. V. (2002). *Bayesian Networks and Decision Graphs*, Springer, NY.

Jordan, M., Ed. (1999). *Learning in Graphical Models*, MIT Press, Cambridge, MA.

Korb, K. B., and Nicholson, A. E. (2003). *Bayesian Artificial Intelligence*, Chapman & Hall/CRC Press, Boca Raton, FL.

Neopolitan, R. E. (2004). *Leaning Bayesian Networks*, Pearson Prentice Hall, Upper Saddle River, NJ.

Pearl, J. (1988). *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann, San Mateo, CA.

Pearl, J. (2000). *Causality: Models, Reasoning, and Inference*, Cambridge University Press, New York.

Zdziarski, J. A. (2005). *Ending Spam: Bayesian Content Filtering and the Art of Statistical Language Classification*, No Starch Press, San Francisco, CA.

# USING RISK ANALYSIS TO INFORM INTELLIGENCE ANALYSIS

HENRY H. WILLIS
*RAND Corporation, Pittsburgh, Pennsylvania*

## 1 INTRODUCTION

The goal of intelligence is to produce guidance on the basis of available information within a time frame that allows for purposeful action. In efforts to combat terrorism, actionable guidance could come in many forms.

Sometimes guidance is needed to shape strategy. For example,

- the federal government must decide whether to maintain stockpiles to enhance emergency preparedness, or
- state and local governments must choose for which scenarios to develop response plans and train.

Sometimes guidance is needed to inform operational decisions. For example,

- if the federal government decides to use stockpiles, it must decide what to put in them and how to preposition them; or
- airports must decide how to deploy technologies and modify operations to enhance security.

Sometimes the required guidance is on a tactical level. For example,

- law enforcement must know when to deploy additional surveillance around a building or for an event;
- law enforcement is interested in who may be planning an attack; or
- critical infrastructure owners and operators need to know when greater security is required.

All of these examples require different information, but have one thing in common. They all require that the information be appropriate for the intended use.

The concept of the intelligence cycle provides a structure to the process of producing this guidance. The intelligence cycle (Figure 1) begins with the direction of intelligence collection (step 1). This results in collection of new information (step 2) that must be processed (step 3), analyzed (step 4), and disseminated and used (step 5). Use of the intelligence products creates new information through either active (i.e. new directed intelligence collection) or passive (i.e. observance of resulting events) means. The intelligence cycle is completed by feeding this new information back into this process [1].

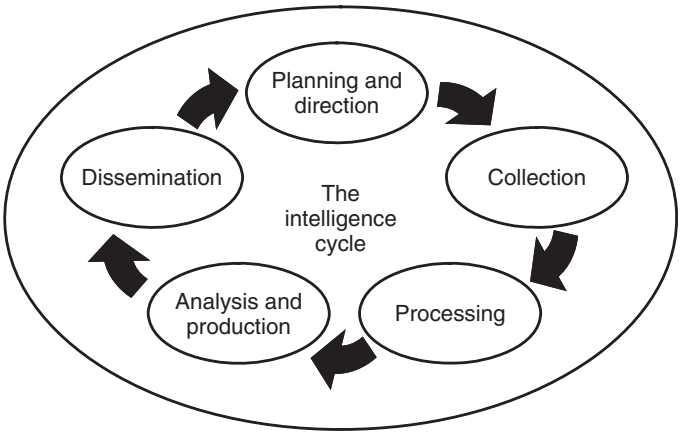



**FIGURE 1** The intelligence cycle (adapted from Krizan 1999) [1].

Time is critical to the success of this process because adversaries also carry out their own intelligence processes to identify promising opportunities for attack and target vulnerabilities. Intelligence is more valuable if the intelligence cycle operates faster than the opponent's. More rapid intelligence enables faster recognition of new threats and adaptation to shifts in opponents' strategies. Thus, methods to improve the accuracy and speed of the process provide a strategic advantage in efforts to combat terrorism.

This article discusses how risk analysis can help intelligence analysts assess threats of terrorism. The discussion leads to two conclusions. First, risk analysis can be used to sharpen intelligence products. Second, risk analysis can be used to prioritize resources for intelligence collection. However, it is important that practitioners applying risk analysis recognize its limitations to ensure that results are appropriate for the purpose and that its use does not blind the analyst to potential surprises.

The remainder of the article is organized as follows. The next section describes intelligence analysis as an input–output process and maps risk analysis to this process. Following this description is an introduction of challenges to the successful application of risk analysis to intelligence analysis. The article closes with a summary of how risk analysis can best serve the intelligence analysis community.

## 2 INTELLIGENCE ANALYSIS AS AN INPUT–OUTPUT PROCESS

The analysis function of the intelligence cycle in Figure 1 can be considered an input–output process in which raw intelligence is the input and intelligence products are the outputs. Within this framing, Willis et al. [2] described how risk analysis can be connected to the intelligence cycle (Figure 2).

The process outlined in Figure 2 represents an interaction between the intelligence community and the intelligence customer. In the case of terrorism risk, it is the managers who are responsible for implementing homeland security policies and programs. In the same way that the intelligence cycle must be an iterative process, the intelligence community and the homeland security community must interact closely and at many stages throughout the process of collection, processing, and analysis.

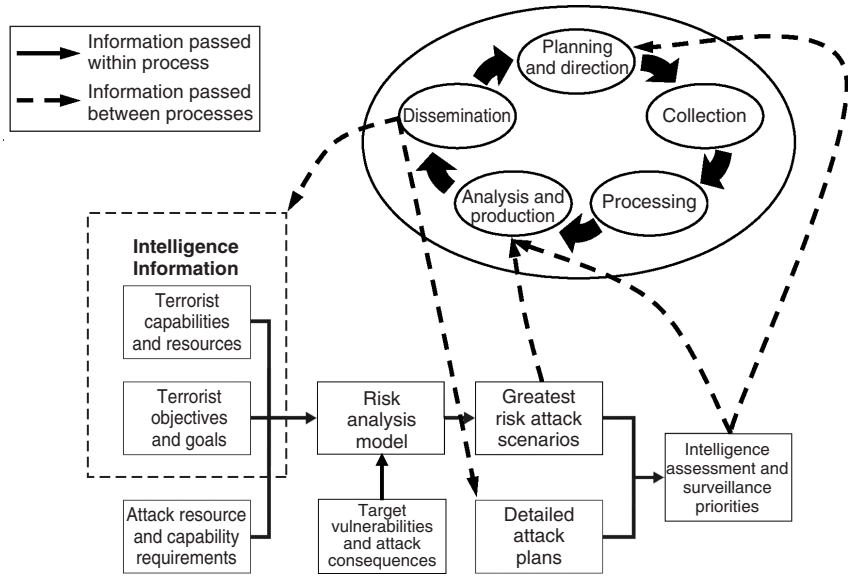



**FIGURE 2** Connections between risk analysis and the intelligence cycle (adapted from Willis et al., 2006).

Collection activities produce intelligence that can be used to assess the magnitude and nature of terrorism threats. Here, relevant information is that which describes terrorist capabilities to carry out attacks of different complexity, fiscal and personnel resources to support such attacks, goals in pursuing terrorist activities, and objectives associated with any particular attack plan. This information alone has been used to assess the range of terrorist threats that exist and how they are adapting to evolving security postures. Analyzing all of these factors is important as threat does not exist unless a group or an individual has both the intent and capability to conduct an attack [3, 4].

However, terrorism risk is not determined by threat assessment alone. Risk from terrorism only exists when there is a credible threat of attack that could cause harm to a target that is vulnerable [5]. Risk analysis provides a framework for considering threat, vulnerability, and consequences of potential terrorist attacks and developing strategies to manage these risks most effectively with limited resources.

As depicted in Figure 2, risk analysis combines intelligence about the objectives and capabilities of terrorist groups with assessments of the required capabilities and resources to complete an attack successfully, assessments of the vulnerabilities of targets to different attack modes, and assessments of consequences of different types of attacks on different targets. The product of this analysis is identification of terrorism scenarios that present the greatest risk.

This result itself can be used by the intelligence cycle. Thus, at its most basic form, risk analysis can be integrated into the intelligence cycle as part of the analysis and production step. However, assessments of the relative risks of different attack scenarios may only be adequate as intelligence products to support for strategic and operational analysis.

Often more specificity than relative risks of different attacks is required about where an attack will occur, when the attack will occur, or who will try to attempt the attack. In

particular, law enforcement agencies attempting to prevent future terrorist attacks need to have guidance of where to conduct further surveillance and who to target with such efforts. This information requires an understanding of the detailed steps and time lines associated with the planning and orchestrating of an attack. Some aspects of this are specific to the target and attack mode being considered. Other aspects are specific to how the group that is planning the attack operates.

Detailed information about attack planning can be developed through surveillance of terrorist groups, investigations into foiled or successful plans for attacks, and red-teaming studies facilitated by tools of risk analysis. Rosoff and von Winterfeldt [6] have demonstrated how probabilistic risk analysis can be used in this way within the context of scenarios for detonating a radiological device at the ports of Los Angeles and Long Beach. In this study, probabilistic risk analysis was used to decompose the attack scenario into its component steps and explore how defensive countermeasures directed at each step could reduce the risks of attack.

By combining the results of risk analysis with detailed assessments of the planning stages of terrorist attacks, the intelligence process can provide directed intelligence products and refine future planning and direction of intelligence collection.

## 3 ANALYST'S CHALLENGES TO APPLYING RISK ANALYSIS PRODUCTIVELY

The productive application of risk analysis to support intelligence analysis must address four methodological challenges: (i) developing methods that can be supported with obtainable information; (ii) matching resolution of results with the problem; (iii) applying the best practices of risk analysis; and (iv) avoiding the potential for blinding analysts to the possibility of surprise.

### 3.1 Basing Analysis on Obtainable Information

While discussions of terrorism risk have received more attention recently, the methods of risk analysis are supported by decades of development and application, which include the study of risks of terrorism to critical infrastructure [7, 8]. This creates a strong methodological foundation on which to build and a pool of expertise on which to draw.

However, it also creates the potential that well-intentioned risk analysts could develop tools for which required input data are not obtainable in an effort to bring their capabilities to bear on the issue *de jure*. This problem of pushing tools in a manner for which they cannot be used can be avoided by asking and answering four questions at early stages of a risk analysis (Figure 3).

First, simply consider what data are needed. Asking this question initiates the process of considering what information is required and what information is available.

Second, determine whether the risk assessment requires additional data collection. In some cases, if the data are not already available, financial or time considerations will preclude going further. In other words, if the data are not obtainable, the analytic approach is dead on arrival. In other cases, learning that new data are needed initiates a process of refining future planning and direction of intelligence collection or developing innovative approaches to obtaining proxies for required data elements.

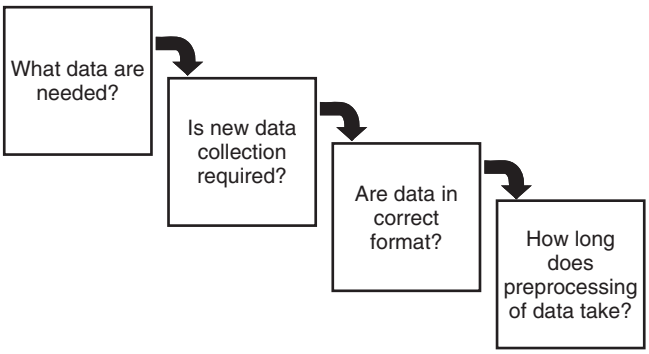



**FIGURE 3** Considerations regarding availability of information to support risk analysis.

Third, analysts must consider whether data are in the correct format and resolution for the analysis. Typically, the data that have been already collected will not have been assembled with risk analysis in mind. The data could be in an incorrect format, could be incomplete because of missing data elements, or could also be internally incoherent because of conflicting reports or assessments of particular data elements. In any of these cases, the data may require cleaning and processing before they can be used in risk analysis. This is important because of the fourth question: How long does any required preprocessing take to complete?

It may be the case that new data are required and that new or existing data must be preprocessed before the data can be used in a risk analysis. However, the time required to do this affects how and whether the information can be used to support intelligence analysis. Tactical decision making is generally very time critical and allows little time for analysis. Strategic and operational decision making is generally less urgent. Ideally, all required information is immediately available and its collection and processing does not lengthen the time of the intelligence cycle. To the extent more time is required, the information may become less useful for supporting tactical operations where the value of intelligence information is measured in its ability to inform decisions that are made in a matter of hours if not a few days.

These four questions are all basic and seemingly second nature to analysts familiar with informing real decisions. However, if not carefully considered when developing or proposing applications of risk analysis, the results can be a process of little or no value.

### 3.2 Matching Resolution of Analysis to the Problem

There is no single risk assessment tool that fits the demands of all problems. Each problem has unique aspects that determine requirements for the spatial and temporal resolution of results [9].

Risk assessments intended to support design or performance assessment for security need to be tuned to a specific threat or target, but not necessarily to a specific time. For example, consider an assessment used to buttress physical security at a nuclear power plant. Designs need to be focused on specific types of attacks on specific parts of the plant, but it is much less important whether the attacks would occur this year or next.

Risk assessments for strategic planning need to be specific about what types of attacks could occur, but do not require specificity of when or where the attacks will occur

because strategic assessments need only reflect the range of threats of terrorism. For example, think of an analysis to support the division of resources among control of nuclear proliferation and border security. Here the decision making does not require distinctions between specific places or which attack will happen first. It is important instead that the planning consider the correct range of attacks.

Finally, risk assessments to support tactical decisions require both spatial and temporal specificity. They will be used to help commanders decide what actions to take and when to take them. For example, consider an analysis that would help local law enforcement determine where and how many officers to deploy in security around a national political convention and when and where to supplement security in response to specific threats. Assessments of risks based on capabilities terrorists had last year are irrelevant if the way the group operates has changed dramatically.

Figure 4 presents the results of a comparative risk assessment that one user may see as having little value but which another could see as insightful. This figure presents an estimate of the distribution of the relative risk of terrorism across Manhattan in terms of casualty costs associated with workers' compensation claims following a terrorist attack. In this figure, darker shaded areas reflect regions of higher risk. A first order conclusion drawn from this figure is that terrorism risk is greatest in midtown Manhattan and the financial district of lower Manhattan.

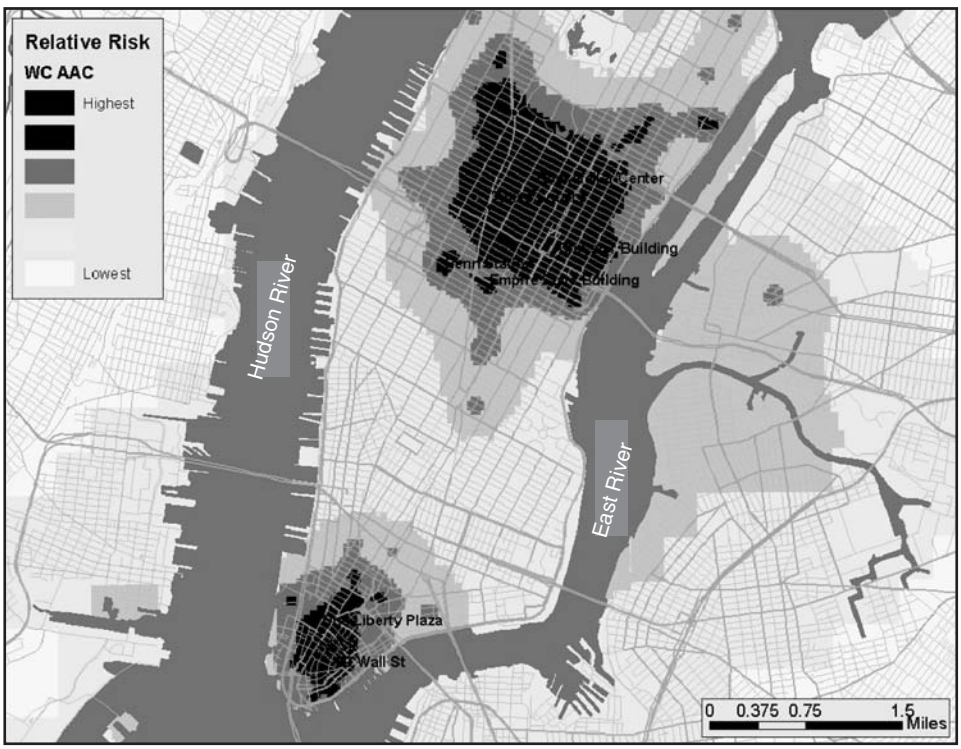



**FIGURE 4** Graphical depiction of assessment of relative terrorism risk in Manhattan from the risk management solutions terrorism risk model expressed as workers' compensation (WC) average annual consequences (AAC). Source: Willis et al. (2006).

To the New York Police Department, such information is likely to have little value. The local community enters the challenge of protecting New York with a strong understanding of where the greatest vulnerabilities exist, and which events or locations represent particular value targets. For them, risk analysis must have a much sharper resolution to be useful. In the effort to prevent future terrorist events, local law enforcement requires help in determining which intersections to patrol, what questions to ask detainees to crack terrorist networks, and when to step up security because threats seem more imminent.

For state or federal officials, the analysis may have more value. These groups may not have the same entrenched knowledge of local vulnerabilities and targets. They may also be solving different problems. For example, federal officials are responsible for allocating resources to combat terrorism across the United States in proportion to terrorism risk [5]. Also, when faced with new threat information, federal officials may need to ascertain quickly for which communities the threat information is relevant [2]. In each of these cases, there is value in having the capability to access quickly or conduct studies of relative risks of terrorism across multiple cities using a common approach with consistent assumptions and data. In such cases, results like those presented in Figure 4 could be useful if accompanied by similar analyses for other communities across the nation.

### 3.3 Applying the Best Practices of Risk Analysis

The best practices of risk analysis recognize that risk is a social construct and that risk analysis requires an analytic and deliberative process [10]. For terrorism risk, these characteristics can be refined to provide further definition of a good assessment.

***3.3.1 Analytic.*** An analytic terrorism risk assessment must address all three factors that determine terrorism risk: (i) threat, (ii) vulnerability, and (iii) consequence [2]. When feasible, this should be done quantitatively, using qualitative methods to fill in data gaps were necessary and appropriate. To the extent qualitative methods are used, risk analysis will be more useful for sorting high risks from low ones than for optimizing or fine tuning risk management strategies.

Risk assessments must be repeatable so all parties can replicate, analyze, and understand them. Risk assessment will require standard definitions within an analysis or methodology to ensure that results are consistent among analysts. It may be impossible to develop consistent definitions across all risk analyses. However, that is not necessary so long as consistency is applied within an analysis and when results are compared from one analysis to another. It is most important that the analysis is transparent such that definitions are clearly documented and appropriate for the problem on hand.

Because of uncertainties associated with terrorism risk, standard expected value decision-making tools that focus on the average or best estimate of risks may not be appropriate [8]. In particular, the most significant uncertainty surrounds assessment of terrorism threat. There is little consensus about when terrorists will attack next, how severe such an attack will be, and how quickly terrorist threats are evolving as terrorist groups attempt to obtain weapons of mass destruction and governments adopt tighter security. In light of this tremendous uncertainty, approaches that consider a very broad range of plausible threats may be necessary as well as adoption of decision support tools that help

identify strategies that perform well across a wide spectrum of these plausible scenarios (see [11] as an example of such an approach).

***3.3.2 Deliberative.*** A deliberative process is necessary because the notion of a cold, actuarial risk assessment is unrealistic. Although one might think risk analysis could be performed only on the basis of data about threat, vulnerability, and consequences, it is not possible to assess risks without considering individual values and judgments about risks and risk exposures. As a result, risk analyses must include deliberative processes that make it possible to take these judgments into account. A transparent analytic process, as outlined above, is necessary to support the deliberative process. This is the only way to address credibly trade-offs between risks to people from risks to property and risks from a conventional bomb, nuclear attack, biological attack, or even hurricane or other natural disaster. Applications of risk analysis to terrorism have to date focused more on the analytic components of risk than on the deliberative dimensions that require a difficult discussion of priorities and a judgment of which risks shall be tolerated.

### 3.4 Avoiding Blinding Analysts to Surprise

The strength of applying risk analysis to intelligence analysis is that it provides a set of tools for translating available information about terrorist motivations, terrorist capabilities, infrastructure vulnerabilities, and attack consequences into a set of common metrics that can be used to develop strategies to protect communities from attack effectively. However, this is also the root of one weakness of the approach.

The results of a risk analysis are bounded by the information and assumptions that go into it. Only those attacks that are envisioned will be assessed and only those targets that are considered relevant will be considered. As a result, the potential exists that risk analysis could lead the intelligence community to place too much attention on events that are presumed to be likely, thus only reinforcing prior beliefs about terrorist threats and risks and not revealing new insights or trends.

To counter this potential bias, it is necessary to state explicitly the principal assumptions built into terrorism risk assessments and homeland security plans, fully explore uncertainties around terrorism risk [5], adopt methods that allow analysts to consider the extent to which information they are assessing could explain alternatives that they are not considering [12], and consider institutional structures designed to prevent myopic policies with respect to the possibility of surprise [13].

## 4 SUMMARY

This article describes how methods of risk analysis can be integrated into the intelligence cycle used to produce terrorism warnings and threat assessments. This connection reveals two ways by which risk analysis can be of potential value to the intelligence community.

Risk analysis can be a tool that can help intelligence practitioners sharpen their conclusions by providing analytic support for identification of scenarios of greatest concern. Risk analysis can also be used to direct future collection efforts on information that appears to be most relevant to refining existing estimates of terrorism risks.

However, risk analyses must be conducted to meet challenges of information availability, matching resolution of results to the problem, reflecting risk as the social construct that it is, and not ignoring the possibility of surprise.

## ACKNOWLEDGMENTS

This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Contract N00014-05-0630 (Office of Naval Research). Any opinions, findings, conclusions, or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security. I would also like to thank my colleagues Brian Jackson, Terrence Kelly, Don Kleinmuntz, Tom LaTourrette, Jack Riley, Errol Southers, Greg Treverton, Detlof von Winterfeldt, and Mike Wermuth at RAND and USC for their informal comments on my work in this research area.

## REFERENCES

1. Krizan, L. (1999). *Intelligence Essentials for Everyone*, Occasional Paper Number Six. Joint Military Intelligence College, Washington, DC. Available online at http://www.dia.mil/college/pubs/pdf/8342.pdf (accessed February 5, 2007).
2. Willis, H. H., LaTourrette, T., Kelly, T. K., Hickey, S. C., and Neill, S. (2007). *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection*. TR-386-DHS. RAND Corporation, Santa Monica, CA.
3. Cragin, K., and Daly, S. (2004). *The Dynamic Terrorist Threat: An Assessment of Group Motivations and Capabilities in a Changing World*, MR-1782-AF. RAND Corporation, Santa Monica, CA.
4. Chalk, P., Hoffman, B., Reville, R., and Kasupski, A.-B. (2005). *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act*, MG-393. RAND Corporation, Santa Monica, CA.
5. Willis, H. H., Morral, A. R., Kelly, T. K., and Medby, J. J. (2005). *Estimating Terrorism Risk*, MG-388-RC. RAND Corporation, Santa Monica, CA.
6. Rosoff, H., and von Winterfeldt, D. (2007). A risk and economic analysis of dirty bomb attacks on the ports of Los Angeles and Long Beach. *Risk Anal.* **27**(3), 533–546.
7. Garrick, J. B. (2002). Perspectives on the use of risk assessment to address terrorism. *Risk Anal.* **22**(3), 421–423.
8. Haimes, Y. Y. (2004). *Risk Modeling, Assessment, and Management*, 2nd ed. John Wiley & Sons, Hoboken, NJ.
9. Willis, H. H. (2005). *Analyzing Terrorism Risk*. Testimony presented before the House Homeland Security Committee, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, on November 17, 2005.
10. International Risk Governance Council (2005). *White Paper on Risk Governance: Towards an Integrative Approach*. International Risk Governance Council, Geneva. Available online at http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance_reprinted_version_pdf (accessed February 5, 2007).
11. Lempert, R., Popper, S. W., and Bankes, S. C. (2003). *Shaping the Next One Hundred Years: New Methods for Quantitative, Long-Term Policy Analysis*, MG-1626-RPC. RAND Corporation, Santa Monica, CA.
12. McGill, W., and Ayyub, B. (2006). Quantitative methods for terrorism warnings analysis. Presentation at the *Annual Meeting of the Society for Risk Analysis*, December 6, 2006, Baltimore, MD.
13. Posner, R. A. (2005). *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11*. Rowman & Littlefield Publishers, Lanham, MD.

# VULNERABILITY ASSESSMENT

DONALD E. NEALE
*Department of Homeland Security, Washington, D.C.*
ELIZABETH M. JACKSON
*George Mason University School of Law, Arlington, Virginia*
GLENN COGHLAN, CPP
*Founder and CEO, Coghlan Associates, Inc., Springfield, Virginia*

## 1 DEFINING TERMINOLOGY

The term *vulnerability assessment* is commonly misunderstood. Surveys and inspections are regularly labeled as vulnerability assessments, possibly due to the fact that surveys, inspections, and vulnerability assessments all have a security focus and use a checklist to maintain their scope. Although these terminologies are often used interchangeably, the following descriptions delineate their differences.

*Survey.* In general terms, a survey identifies current security posture and helps ascertain what countermeasures/protective measures exist or need to exist. The survey process is used to gather information about a site and its countermeasures/protective measures. The information is then analyzed in order to make recommendations for the security design of a site, whether an individual building, an entire complex with multiple buildings or facilities, or an event location.

*Inspection.* An inspection is conducted to verify compliance with pre-established security standards and procedures as described in policy and regulation in an effort to help maintain security posture. Inspection teams use checklists to compare a site's security posture to that outlined by an authoritative or regulatory body, the results of which are detailed in after-action reports provided to the responsible party.

*Vulnerability assessment.* A vulnerability assessment is an aspect or component of risk analysis. Essentially, it is the systematic examination of a security posture to identify vulnerabilities or gaps in security or supporting infrastructures that may allow an adversary to exploit a site's weaknesses. A vulnerability assessment also helps to determine the appropriate countermeasures/protective measures necessary to reduce risk.

A vulnerability assessment represents a holistic look at security. Its goal is to identify any overlooked details in a site's security posture; details may be disregarded due to underdeveloped procedures or due to lack of understanding of the capabilities of existing technologies or of an adversary to exploit vulnerabilities within security posture to compromise the site and surrounding population. Ensuring that a qualified team conducts a vulnerability assessment can present a broader perspective and greater knowledge of key

security issues to a site's owner/operator. Assessment teams complete assessment reports that document a site's vulnerabilities and recommend specific countermeasures/protective measures to address those vulnerabilities.

A good analogy of a vulnerability assessment is the instance of a home buyer who examines the house he intends to purchase, but overlooks a popped nail on the roof partly holding down a shingle. During high winds and rain, the shingle may be knocked loose, leading to water damage inside the house. If the water damage is excessive, the house could be lost. Similarly, if a vulnerability is overlooked in an assessment, that vulnerability could be exploited and lead to catastrophic damage to the site and surrounding population, as well as significant cascading effects. A common maxim encapsulates this situation, "for want of a nail . . . the kingdom was lost . . . "—attributed to a Benjamin Franklin poem in 1757s *Poor Richard's Almanac*.

One example of exploited vulnerabilities is illustrated by the terrorist attacks of September 11, 2001. Terrorists are trained to find what has been overlooked, whether by surveillance or open source research; such training was apparent in these attacks. Terrorists identified a vulnerability at airport security checkpoints and exploited that vulnerability by defeating X-ray technology and its operators, thereby enabling them to successfully hijack airliners in an attack resulting in the deaths of thousands of Americans. Additional countermeasures/protective measures and training programs relative to airport screening were subsequently implemented, and a heightened tolerance for increased security screening was instilled in the American people.

## 2 VULNERABILITY ASSESSMENT METHODOLOGIES

Many hybrids of vulnerability assessments have been developed over the years. The majority of vulnerability assessment methodologies concentrate on one of three primary focal points: population protection, site and systems security effectiveness of high-value/high-risk assets, and mission/service survivability. While most assessment methodologies integrate these concentrations, outlined below, each will typically have a defined scope.

*Population protection.* Population protection is sought through the combination of security initiatives protecting the population both inside and around a site from attack. Using an integrated approach, population protection coordinates countermeasures/protective measures to mitigate the effects of an incident, whether it is the product of a natural or man-made disaster or terrorism. This process is illustrated in Figure 1.

*Site and systems security effectiveness (high-value/high-risk assets).* Site and systems security effectiveness implies a comprehensive vulnerability assessment of a layered security system within security postures. Utilizing "design basis threat", it dictates the evaluation of security system effectiveness to deter, detect, defend against, and respond to adversarial capabilities. Following evaluation, specific system vulnerabilities may be identified. Modeling and estimation of success rates are used to gauge the appropriate countermeasures/protective measures for implementation. This process is illustrated in Figure 2.

*Mission/service survivability.* Mission/service survivability centers on the protection, robustness, and assurance of mission or service continuation, as well as the protection of workforce essential to mission/service execution. It considers a full-threat,

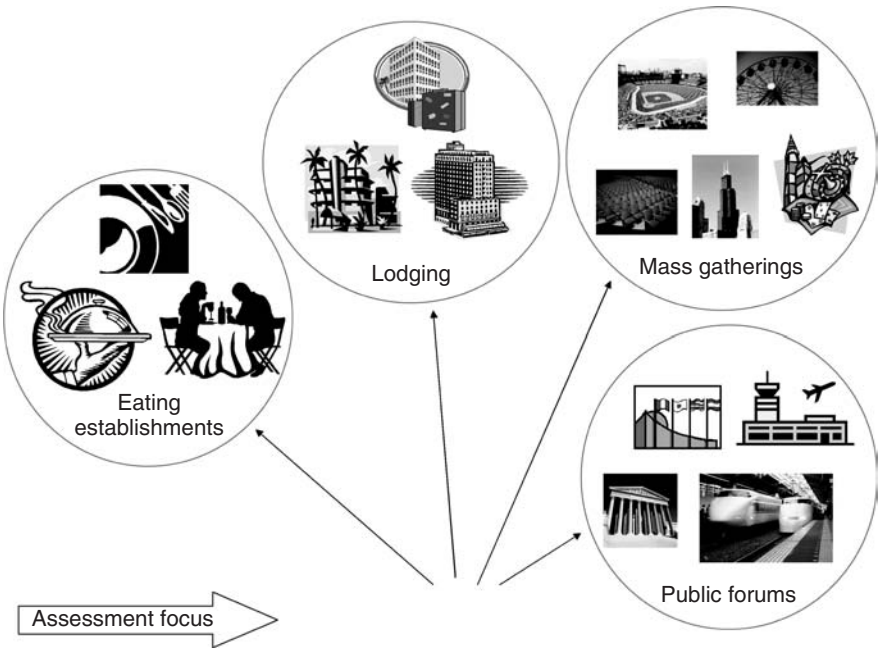



**FIGURE 1** Population protection.

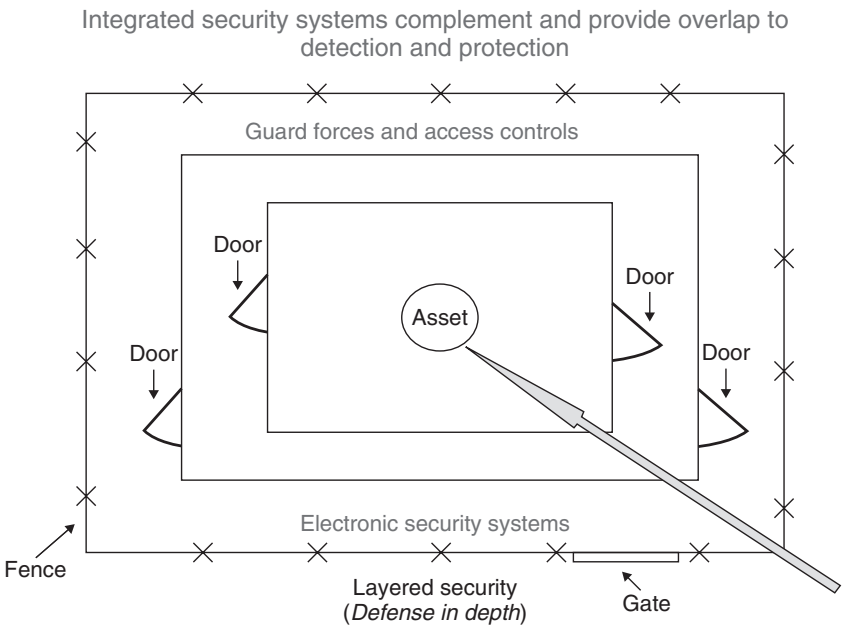



**FIGURE 2** Site and systems security effectiveness.

all-hazards spectrum, looking at site criticality (internal) in conjunction with assessing the criticality of outside supporting infrastructures (external). In doing so, it:

- normally starts from the center of the site and moves to the fence line and beyond, to at least the first node of critical failure of any supporting infrastructure;
- produces suggestions to reduce strategic infrastructure vulnerabilities;
- identifies any cascading effects stemming from a systems failure;
- identifies interoperability, interdependencies, redundancies, and diversity of infrastructure, to include the resiliency of specific critical infrastructure;
- incorporates site experts/systems engineers and security specialists; and
- considers the operating parameters, realistic threats, and acceptable loss and funding of the site being assessed.

This process is illustrated in Figure 3.

There is no single methodology that adequately encapsulates all three concentrations in totality. However, no one methodology is better than another; the results of a vulnerability assessment are predominantly affected by the composition of the assessment team and the expertise of other individuals within the vulnerability assessment process. Given this, many methodologies attempt to employ the same skill sets. It must also be noted that vulnerability assessment methodologies regardless of their focus or scope, more often than not, use a similar common sense, systematic approach.

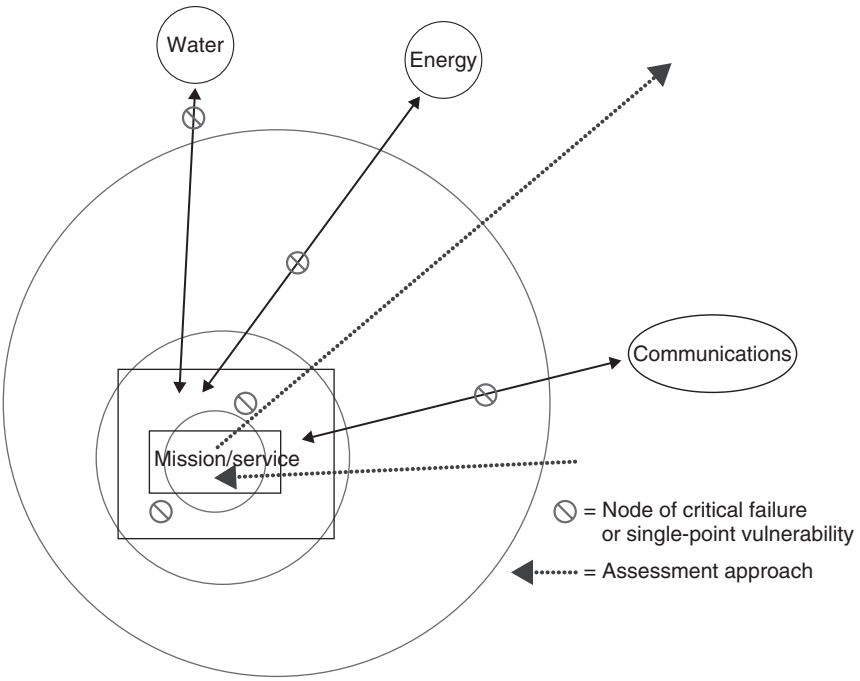



**FIGURE 3** Mission/service survivability.

## 3 VULNERABILITY ASSESSMENT TEAM COMPOSITION

The focus of the assessment and a site's uniqueness will dictate specific vulnerability assessment team composition. The following list of selected protection elements and disciplines, each of which can encompass a vast array of specific concentrations or areas of expertise, may be considered in the makeup of an assessment team:

- Technical integration (Assessment Team Lead)
- Physical security
- Information operations
  - Cyber security
  - Information security
  - Operations security
- Personnel security
- Surveillance operations
- Site expert/systems engineer
- Communications
- Supervisory control and data acquisition (SCADA) systems
- Utilities
  - Energy
  - Water
- Structural engineering (building hardening)
- Emergency management and response
- Fire protection
- Restoration/continuity of operations
- Weapons of mass destruction
- Electromagnetic and radio frequency protection

The assessment team will follow a systematic vulnerability assessment process similar to that outlined below. The Assessment Team Lead will oversee and integrate the various aspects of the assessment, while each assessment team member will conduct a comprehensive assessment of his/her respective protection element or discipline. *Typically, these subject-matter experts will break down the assessed area into systems, subsystems, and components (or categories, topics, and subtopics) to obtain a clearer, more detailed picture of the vulnerabilities and gaps in overall security posture*.

## 4 VULNERABILITY ASSESSMENT PROCESS

The assessment process stresses a common sense approach to protecting and securing systems, components, and personnel necessary for the continued operation of a site's mission (or services) and is executed by the assessment team in three phases: pre-assessment, on-site assessment, and post-assessment. Established regulations, policies, and standards should neither be used as guiding principles nor reviewed for compliance as, in some instances, such guidance has been found to cause mission vulnerabilities. This being said,

assessment team members must have a basic understanding of the regulatory requirements that a site's owner/operator uses when establishing site security guidelines.

The following explanation of the execution of an all hazards vulnerability assessment focusing on mission/service survivability can help the reader understand and recognize the basic framework of vulnerability assessments, as well as elements that can be tailored for a specific need. *The assessment described does not detail specific protection elements and disciplines considered during the assessment; rather, it depicts an overall systematic approach used by all methodologies*.

### 4.1 Phase I: Pre-assessment

Phase I generally consists of two primary sets of activities: customer (responsible party, owner/operator or otherwise) orientation and coordination and assessment planning. This phase normally begins weeks prior to Phase II (the actual on-site assessment) because of the complexities and unique requirements of each assessment. During this phase, assessment team members conduct the essential groundwork to underwrite assessment success.

Working with the assessment team according to standard operating procedures, the Assessment Team Lead will select a team task organized for the site's mission, and liaise with the appropriate parties to pass clearances, make lodging and travel arrangements, and settle other administrative matters. During Phase I, the Assessment Team Lead will coordinate with secondary assessment sites (external) as appropriate, relative to the support of the primary site (internal) and its mission. Unless restrictions are put in place by the customer, assessment team members should initiate contact with their customer counterparts as soon as the Assessment Team Lead obtains points of contact (POCs) for specific protection elements and disciplines.

During any assessment phase, assessment team members should notify the Assessment Team Lead of any significant problems or issues that arise, and provide recommended actions to remedy such problems or issues. The Assessment Team Lead shall provide guidance to the assessment team on submission deadlines and procedures.

***4.1.1 Customer Orientation and Coordination Activities.*** Key customer orientation and coordination activities will be performed by the Assessment Team Lead or by assessment team members in close coordination with the Lead. These activities should include, but are not limited to, the following tasks:

1. Identify the site(s) to be assessed. For each site, identify:
   - its assigned mission or services it provides;
   - an initial list of other key sites or infrastructures (e.g. host site or other tenants) that provide vital support to the site to be assessed; and
   - the customer's goals and objectives for the assessment.
2. Obtain the site briefing and organizational chart.
3. Coordinate the scope of the assessment:
   - identify any constraints or limitations relative to the site (e.g. site boundaries, security classification, or special access restrictions);
   - ensure the customer understands that recommended countermeasures/protective measures will not solve all problems, meaning that there is no 100% guarantee for site protection; and

- ensure the customer understands that periodic assessment reviews and a risk management program should supplement any vulnerability assessments.

4. Identify the customer's perception of the primary threats to the site's ability to execute its assigned mission.
5. Coordinate the assessment's timeline with the site POC.
6. Conduct a site pre-visit.
   - Provide the customer, key personnel, and representatives of key supporting infrastructures with an assessment presentation that, at a minimum:
     - addresses customer goals, objectives, intended scope, envisioned timeline with major milestones or events, and any known constraints or limitations;
     - identifies or confirms specifics for milestones, such as the date, time, location, and attendees for the in-brief and out-brief;
     - provides an overview of the planned assessment methodology;
     - describes the assessment team's functional composition and POCs for specific protection elements and disciplines, and provides team contact information;
     - details requirements for the assessed site to coordinate with other host, tenant, or local supporting sites or infrastructures;
     - describes assessment team Phase I and II information and documentation requirements for each protection element and discipline;
     - emphasizes that information and documentation is required for the assessment team to effectively conduct its assessment, and that the team's timely access to required documentation is critical to assessment thoroughness and efficiency; and
     - describes assessment team on-site administrative and logistics support requirements, such as office space, parking, security containers, telephone access, information on personnel POCs and POC contact information (e.g. telephone numbers and e-mail addresses), and any other support issues.

***4.1.2 Assessment Planning Activities.*** Primary assessment planning activities that take place during Phase I include, but are not limited to, the following tasks:

1. Conduct an initial review and analysis of the site's mission and supporting documents, as well as other information obtained during Phase I, to identify vulnerabilities and to focus Phase II efforts. Site documents and information for review include:
   - briefing and organizational chart;
   - critical mission and mission support functions;
   - relative priorities or importance over time;
   - interrelationships and interdependencies;
   - logical, physical, and functional network and system diagrams, blueprints, or user manuals;
   - concept of operations (CONOPs);
   - previous vulnerability, threat, or risk assessment results and/or reports;

- previous exercise after-action reports;
- training program curricula, standard operating procedures, and relevant policies or directives to include applicable laws and regulations;
- continuity of operations, contingency, disaster recovery, and backup plans or procedures; and
- details on sites or infrastructures that support critical mission and mission support functions (e.g. SCADA, telephone/fiber-optic line connectivity, and utilities).

2. Particularly for large, complex sites, develop an assessment timeline with major milestones or events for assessment Phase II activities to maximize the efficiency of on-site activities and minimize the impact on the site and its personnel.
3. Conduct open source research for information to characterize the site being assessed, critical mission and mission support functions, and supporting infrastructures.
4. Obtain preliminary, relevant information on:
   - the key site personnel perceptions of the primary threats to the site's critical mission and mission support functions;
   - the type of threat: insider (access, knowledge, and privileges), hacker (novice or professional), organized crime or terrorist, foreign or industrial intelligence, weapon of mass destruction, and etc.; and
   - anticipated threat tactics: social engineering or collusion, stealth, brute force, physical attack or damage, open source research, third-party usage, and etc.
5. Identify the site's POC for each assessment protection element or discipline.
6. Contact site POCs and set up tentative interview schedules (dates, times, and locations). Doing this prior to Phase II is a courtesy to the site personnel in that they can schedule the interviews around other commitments, minimize impact on their jobs, and ensure that key personnel are appropriately involved.
7. Conduct intra-assessment team coordination to integrate efforts, thus minimizing impact on on-site personnel.

### 4.2 Phase II: On-Site Assessment

This phase consists of all on-site activities, such as site personnel interviews, site tours, data collection and analyses, and observations to develop and verify ground truth about the site's mission survivability. Specific assessment Phase II activities include, but are not limited to, the following tasks:

- Document mission and mission support survivability activities and security posture through observation of systems, assets, or personnel in action; interviews; analyses of documentation; and assessment tool and/or modeling usage, as authorized.
- Identify, obtain, review, and analyze additional, relevant customer information and documentation.
- Work with intelligence agencies and local law enforcement to discuss potential and known threats directed toward the site.
- Observe demonstrations and/or exercises related to security and survivability.

***4.2.1 Assessment In-brief.*** The assessment team will normally meet its key personnel counterparts, those with knowledge in the specific protection elements and disciplines considered, at the assessment in-brief. Similar to the pre-visit conducted by the Assessment Team Lead, the assessment in-brief should, at a minimum, provide the customer and key personnel with:

- identification or confirmation of specifics for major milestones or events, such as the date, time, location, and attendees for the assessment out-brief;
- an overview of the assessment methodology;
- a description of the assessment team's functional area composition and protection element and discipline POCs;
- requirements for the site to coordinate with other host, tenant, or local support sites and infrastructures;
- an overview of information and documentation requirements; and
- requirements for site authorization documentation, such as that needed for photography, special badges, or access.

***4.2.2 Site Tours.*** After the in-brief, assessment team members typically receive a group tour of the site. This initial tour should be regarded as a site overview. It is appropriate for team members to ask general questions; however, detailed questions regarding specific protection elements and disciplines are best noted and asked later. Assessment team members should schedule detailed follow-up tours of site and supporting infrastructures of direct interest as necessary.

***4.2.3 Interviews.*** Ideally, site POCs are obtained during the site pre-visit, and initial interviews are scheduled before Phase II begins. If not, scheduling interviews with key personnel should be a priority for the assessment team once it arrives on site.

The objective of the interviews is to learn the reality of how operations occur, capturing information on both official and unofficial procedures and processes used. Where applicable, data gained via this means should be compared with official policies, directives, or standard operating procedures.

Key considerations to conducting successful interviews are as follows:

- Ask questions to learn, not to interrogate.
- Be prepared, focused, and organized (with core questions written or thought out in advance).
- Maintain control of the interview.
- Use two assessment team members, when possible: one to focus on questioning and the other to focus on note taking.

Questions to consider asking during interviews include the following:

- What are the cascading effects resulting from loss or damage to the site's critical mission and mission support functions?
- What redundancies exist if the site's critical mission and mission support functions are lost or damaged?
- What are your worst fears?
- What are your perceived vulnerabilities and penetration points?

- What are your recommendations for the customer to improve the security posture of the site?
- What do you consider critical, relative to your specific discipline(s), and why?

***4.2.4 Data Collection and Analysis.*** The assessment team should seek to obtain, review, and analyze all available documentation and information on the site's critical mission and mission support functions, processes, and procedures. Ideally, this data collection and analysis will begin during Phase I.

The assessment team should characterize critical mission and mission support functions and supporting infrastructures to identify vulnerabilities. This includes evaluating and assessing security posture and vulnerabilities, with emphasis on identifying single-point vulnerabilities, for the impact on the site's mission, specifically if systems are lost or degraded.

The assessment team should assess the impact of the loss or degradation of each critical mission and mission support function, its critical components, and its critical dependencies. Specific issues to consider include the following:

- What actions, components, factors, or assumptions are required for critical mission accomplishment or success?
- What are the high-value nodes, components, or systems?
- What actions, components, or factors could result in loss of life or personnel injuries?
- What actions, components, or factors could result in damage to property or equipment?
- What actions, components, or factors could present a potential liability to the site?
- What actions, components, or factors could result in mission failure, disruption, delay, or denial?
- What amount of time is required to recover from an incident?
- What redundancies or backup capabilities exist to ensure mission survivability?
- What contingency and continuity of operations plans exist? How often are they reviewed, exercised, or tested?

***4.2.5 Assessment Out-brief.*** At the conclusion of the assessment team site visit, the team should present an out-brief to the customer and key personnel. The out-brief should be focused on and address all single-point and major vulnerabilities, to include any interdependencies between them. The assessment out-brief should not attempt to address all minor vulnerabilities or issues that will be contained in the assessment final written report. It should reflect validated, coordinated, and deconflicted information regarding specific protection elements and disciplines. Other areas for consideration include the following:

- What are the cascading effects resulting from loss or damage to the site's critical mission and mission support functions?
- What redundancies exist if the site's critical mission and mission support functions are lost or damaged?
- What are the current protection strategies and plans?
- What are the gaps in current protection strategies and plans?
- Do any single-point or major vulnerabilities exist? If so, what are they? Do interdependencies between them exist? If so, what are they?

- What can be done to mitigate existing vulnerabilities through improved policies, resources (personnel, equipment, training, and funding), procedures, or processes in either the near or long term?

### 4.3 Phase III: Post-assessment Activities

This phase includes final report writing, delivering the report to the customer, and conducting follow-up actions as needed to complete the assessment process. This phase is highly intensive, time consuming, and requires extensive collaboration among assessment team members.

## 5 KEY CONSIDERATIONS FOR VULNERABILITY ASSESSMENTS

The aforementioned descriptions of vulnerability assessment methodology focal points, systematic approach, and assessment execution touch upon the fundamental components of vulnerability assessments. Nonetheless, additional considerations must be taken into account when conducting a vulnerability assessment. These considerations may drive funding for countermeasures/protective measures, as well as overall security posture. They include, but are not limited to, the following:

- Political and social tolerance for loss.
  - For example, the common, prudent person on the street would favor spending the money necessary to protect nuclear weapons from theft. Due to the zero tolerance for loss of these weapons systems, more money will be spent on security and the implementation of stringent countermeasures/protective measures.
- Costs versus benefits of added countermeasures/protective measures.
  - Recommended countermeasures/protective measures must be commensurate with risk. For instance, is the value of a site less than the cost of a countermeasure/protective measure with limited benefits?
- Agreement of safety issues and security.
  - Recommended countermeasures/protective measures must work in conjunction with life safety issues. For instance, do the recommended countermeasures/protective measures comply with fire safety regulations?

## 6 CONCLUSION

Vulnerability assessments represent systematic approaches to identifying weaknesses in security postures, procedures, or infrastructure configuration. With no one methodology better than another, vulnerability assessments are distinguished by their focus—population protection, security system effectiveness, or mission survivability. Importantly, the results of a vulnerability assessment are affected, either positively or negatively, by the expertise of those conducting the assessment. Institutions are attempting to develop a single vulnerability assessment methodology that ensures consistent results. However, this feat is virtually impossible due to the subjectivity involved in assessment execution and report development. Rather than trying to develop such a methodology, efforts should be focused on standardizing expertise criterion and required background experience for assessment team members in every protection element and discipline. Experienced

vulnerability assessment professionals can coalesce assessment concentrations and apply tailored assessment approaches based on specific needs to enhance the assessment and the assessment team's findings. Vulnerability assessment methodologies are consistently based on the same framework, using the same approach; the human element is where strengths or weaknesses lie.

## END NOTE

The views expressed herein are those of the authors and may not represent the views of their respective organizations.

## FURTHER READING

Broder, J. F. (2000). *Risk Analysis and the Security Survey*, 2nd ed., Butterworth-Heinemann, Boston.

Center for Chemical Process Safety. (2003). *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*, American Institute of Chemical Engineers, New York.

Cumming, N. (1992). *Security: A Guide to Security System Design and Equipment Selection and Installation*, 2nd ed., Butterworth-Heinemann, Boston.

Garcia, M. L. (2001). *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann, Boston.

Ramo, S., St. Clair, R. K. (1998). *The Systems Approach: Fresh Solutions to Complex Civil Problems Through Combining Science and Practical Common Sense*, KNI, Incorporated, Anaheim.

# RISK COMMUNICATION

MONIQUE MITCHELL TURNER

*Center for Risk Communication Research, Department of Communication, University of Maryland, College Park, Maryland*

SHAWN S. TURNER

*United States Marine Corps, Arlington, Virginia*

## 1 INTRODUCTION

In 1987, University of Oregon Psychology Professor, Paul Slovic, wrote "in recent decades, the profound development of chemical and nuclear technologies has been accompanied by the potential to cause catastrophic and long-lasting damage to the earth and

the life forms that inhabit it. The mechanisms underlying these complex technologies are unfamiliar and incomprehensible to most citizens" (p. 280). Slovic's words are still poignant. The recent rash of natural and man-made disasters and the ever present threat of terrorist attack abroad and at home demonstrate the ever increasing need for organizations charged with communicating risk to be more proactive in their planning, more strategic in their approach, and more educated about risk communication. Social scientists and communication professionals have long studied how shifts in the ease of availability of information coupled with the credibility of the source and the emotional state of the receiver impact individual behaviors and perceptions of events. Unfortunately, findings from this research are often slow to reach frontline practitioners. For organizations involved in communicating risks to publics, these shifts are particularly significant because they are part and parcel to a dynamic communication environment in which our understanding of what constitutes truly effective communication is rapidly evolving. When risks present themselves, communication professionals face formidable challenges in collecting and assessing vital information, designing effective communication strategies, and assessing public's response. In this article, we will present some of the challenges that risk communicators face, best practices for risk communicators, and promising directions for the future of risk communication scholarship.

## 2 CHALLENGES TO EFFECTIVELY COMMUNICATING RISK

Risk communication is a challenging enterprise. Many of those challenges are in no small part due to the lack of clear understanding regarding the nature of risk, particularly as it relates to scientific innovations and public safety. Elucidating the difficulties associated with risk communication starts with understanding the word "risk". To us, risk is the probability of negative consequences of a hazard occurring and the magnitude of those consequences. So, risk deals with the severity of any given threat (i.e. hazard and risk). But, it is also tied to susceptibility to that threat [1]. Moreover, it is important that we note we are talking about *perceived* risk. Certainly, there are risk assessors who can calculate our risk based on a series of factors—but, humans rarely perceive an objective amount of risk. In fact, there are often huge discrepancies between "real" risk and "perceived risk" [2]. Hence, the notion of uncertainty, pros and cons, as well as doubt and ambiguity are inherent in the term risk. Therefore, when communicators talk about risk, they have to recognize the difficulty of the decisions people must make. We must be mindful of the fact that an outcome cannot be guaranteed. There is no such thing as zero risk and there are numerous psychological and emotional factors affecting the way key audiences perceive risk. We highlight some of the specific challenges in communicating risk.

### 2.1 Uncertainty

The notion that science and technology is constantly evolving, coupled with the dynamic nature of public security threats, creates and compounds risk related uncertainty. Lay audiences are often unclear about the risks associated with new innovations and overwhelmed by the amount and complexity of public safety information. Misinterpretations and seemingly contradictory assessments of scientific findings can lead to both over- and underreactions, and create feelings of anger and resentment toward the communicating organization. Moreover, the act of communicating uncertain information, that is,

communicating information on topics about which the full implications are unknown, represents unique challenges for practitioners. A real-world example of this phenomenon can be seen in public's perception of the risk associated with the avian bird flu. According to the Centers for Disease Control, the risk from avian influenza is generally low to most people, because the viruses do not usually infect humans. But, a study released at the World Economic forum entitled [3] claimed that avian bird flu was a more significant threat than terrorism and that, given the right circumstances, could kill between 40 and 50 million people worldwide. Such contradictory information highlights the complexity of the risk, and will also lead to a great deal of frustration and doubt on the part of the public. The goal is to reduce uncertainty by communicating in a confident, credible, and assertive manner while ensuring that key audiences respond appropriately to new and evolving information.

### 2.2 Experts and Consumers Define Risk Differently

Slovic [2, 4] reviewed the biases that laypeople employ in order to make risk assessments. He examined the complex and subtle meanings that people have when they say that something is "risky". To do so, he examined past psychometric data of particular risks with the goal of developing a taxonomic scheme from which we can understand the distinctions among risks. A factor analysis indicated that most risks break down into two continuous factors: dread risk and unknown risk. High dread risk is defined by a perceived lack of control, dread, catastrophic potential, fatal consequences, high risk to future generations, not easily reduced, involuntary, increasing in riskiness, and the inequitable distribution of risks and benefits. Nuclear weapons, nerve gas incidents, nuclear weapons fallout, and radioactive waste among others scored high on dread risk. Unknown risk, at its high end, is defined by hazards that are unobservable, unknown to those exposed, unknown to scientists, new, and delayed in their manifestation of harm. Chemical technologies score high on unknown risk as did cadmium usage and radioactive waste.

These data have been used to predict the kinds of risk that will lead to public outcry. Risks that are perceived to be high on dread risk are perceived to be bigger threats. Risks that are high in both dread and unknown factors will be the most likely to garner attention by the public. One way that experts have attempted to deal with public's rising concerns with particular risks is to educate and inform people about the true nature of the risk. For example, although experts ranked nuclear power twentieth out of 30 potential risks, college students and the league of women voters (examples of lay groups) rated it first; revealing the discrepancy in knowledge about the risk among experts and publics. Yet, simply communicating facts and figures about risks will not decrease public's concerns.

### 2.3 Use of Heuristics in Decision Making

People often use heuristics, simple decision-making tactics, when making decisions that revolve around risk. Often, use of these heuristics can lead to uninformed decisions. Risk decisions are often affected by the availability heuristic. Risks that are more memorable or readily accessible are believed to be riskier. Unfortunately, if the media catch hold of an especially interesting or controversial risk, the story is likely to gain attention of the nation. Media attention can lead to increased memorability on the part of receivers—exacerbating the availability heuristic. Problematically, the availability heuristic leads people to overestimate the frequency of rare events [5, 6].

How a risk is framed will also affect the decisions that people make [6, 7]. Describing the costs of accepting a risk (i.e. a negative frame) will lead to different decisions than will describing the benefits of rejecting a risk (i.e. a positive frame). Research indicates that when an event is communicated in terms of its risks, a negative frame will lead to more attitude change in the direction of the message, but when that same event is communicated in terms of prevention, a positive frame will be more effective.

Extant data also illustrates the omission bias, which reveals that people believe that no action is less harmful than action [8, 9]. For example, parents who are concerned about the risks of vaccination are more likely to withhold vaccinating their children because they believe that their action will be more harmful than no action.

## 3 BEST PRACTICES IN RISK COMMUNICATION

Given the potential negative repercussions of unskilled risk communication, it is important that practitioners be well trained and capable of developing strategies that are informed by relevant communication research. Often, communicators believe that more risk communication equates to better risk communication. However, it is quality and not quantity that lays the foundation for effective risk communication. A significant body of research has led to the development of several risk communication best practices. These practices are reviewed here and some advice on implementing these practices in your organization communication plans are also provided.

### 3.1 Risk and Crisis Communication is an Ongoing Process

Given the uncertainties that are inextricably tied to risk, it is imperative that communicators do their job in communicating the evolving nature of science to community members. Communicators should be clear that they are using the most up-to-date science in their assessments, and as they get more information they will update the public. This way, when updates do arise people will not mistake this as "the so-called experts have no idea what they are talking about". When possible, communicate with the public about why uncertainties exist, that you are collaborating with teams of scientists who are still working, and/or the difficulties in establishing a certain outcome. It is important to be clear about when updates will be communicated and how they will be communicated. People are more accepting of the evolving nature of risk when communicators tell them to expect it.

### 3.2 Listen to Public's Concerns and Understand Your Audience

The discrepancy between true, objective risk and perceived risk is clear. But, until communicators take the time to understand the community members experiencing the risk, we will not know if their perceived risk is exaggerated, too low, or accurate.

When perceived risk is exaggerated the goal is to calm the audience down. Communicating empathetically is an important skill in this regard and is discussed later. The way that people act when their risk is inflated depends upon the emotion they are experiencing [10]. Turner's [11] Anger Activism Model suggests that when people are angry about an issue and they feel they can do something to ameliorate (what they think is) the problem, they are likely to begin engaging in activist behaviors. This can be troublesome

for some organizations if consumers begin protesting, picketing, or engaging in a sit-in. In such cases, the communicators must discuss the risk in ways that address audiences' concerns.

When our perceived risk is too low, people are unlikely to engage in precaution behaviors (e.g. emergency preparedness). In such situations, it is imperative to communicate about the severity of the problem and audience's susceptibility to encounter the risk. Fear appeal theory [1, 12] reveals that when people perceive high severity and high susceptibility, they will perceive an imminent threat in their environment. If the audience feel efficacious in their ability to handle the issue (efficacy is discussed in a subsequent section), then they will engage in preventative behaviors.

Hence, in high stress situations, people must perceive high trust and credibility and they must feel efficacious. But, we also understand that the anxiety created by stress can lead to deficiencies in information processing [13]. To help audiences understand the issue, risk communicators have to create targeted messages. Using clear, nontechnical language is advisable when you are communicating about the nature, severity, or magnitude of risk [15]. The US Department of Health and Human Services provides the following tips:

- Use consistent names, denominators, and other terms throughout the risk (or crisis) situation. For example, do not switch from person per million to person per billion. This may throw people off, and they might not notice that you changed your unit of analysis.
- Use graphics and pictures to help the audience understand the risk.
- Avoid jargon and acronyms.
- Answer not only the question "how much?" but also "will it hurt me?" to ensure that people get relevant information.
- Use familiar frames (or metaphors) to explain how much, how small, or how many. Try to create a mental picture for the audience.

### 3.3 Demonstrate Honesty, Candor, and Openness

Covello's [14] research indicates that during low stress situations, public's perception of trust in communicator is based on their perceived level of expertise. So, in low stress situations people will look to someone's competencies, job title, education, and so on. However, in high stress situations, people base their trust on perceptions of listening, caring, and empathy.

Communicating trust and credibility is the first and foremost important skill of the risk communicator. Decades of research in source credibility help lay the groundwork for what makes a communicator appear credible [16]. Credibility is made up of multiple components, in particular, trust, dynamism, and expertise. Dynamism is not covered in this article, but researchers have studied what people think of when they use the word "*expert*". This research indicates that experts are those who have or communicate the following:

*Training.* Experts have an advanced knowledge and/or degrees in the area being spoken about.

*Skill.* Experts have specialized skills.

*Informed.* Experts stay up to date on advanced research and are well informed on the current information about his/her topic.

*Authoritative.* Experts speak with authority. Experts act assured in their knowledge.

*Ability.* Experts have the ability to take action.

*Intelligence.* Experts have generalized intelligence.

Studies show that in low-trust, high-concern situations, credibility is assessed using these four measures: empathy and/or caring (50%, assessed in the first 30 s), competence and expertise (15–20%), honesty and openness (15–20%), and commitment and dedication (15–20%). Nonverbal cues have also been documented to impact trust and credibility [14].

Often, risk communication teams will have their scientists as the public spokesperson during times of risk and crisis because the public believe that a scientist knows what is going on. In fact, successful risk communication does require expertise in conveying understandable and usable information to all interested parties. Risk managers and technical experts may not have the time or skill to do all of the complex risk communication jobs such as responding to the media, the public, industry, and so on. People with real expertise should be involved as early as possible. This expertise was likely developed by training and experience.

Trustworthiness is the second dimension of credibility. It is truly not enough to be an expert—who cares if you are an expert if people do not believe in your proclivity to tell the truth? Also, when an issue is personal, frightening, or serious, we look for trustworthy speakers. The risk communication literature identifies the following three factors that determine whether or not the public will perceive a communicator as trustworthy:

- empathy and caring,
- honesty and openness,
- dedication and commitment.

When communicators make certain to relate their message to audience's perspectives, emphasizing relevant information to any practical steps that they can take, the message will be more effective. Use clear and plain language. Make sure that you clearly state the existence of uncertainty, and avoid trivializing the concern. Covello et al. [18, 19] also offer the following guidelines:

- be balanced;
- focus on a specific issue;
- pay attention to what the audience already knows;
- be respectful in tone and recognize that people have legitimate feelings and thoughts;
- be honest about the limits of scientific knowledge;
- consider and address the broader social dynamics in which risks are embedded;
- be subjected to careful evaluation;

The single most important determinant of gain or loss of trust is whether the communicator is subsequently proven to be correct or incorrect, and that the communicator is demonstrated to be unbiased. Trust is contextual; that is, whether you are seen as

trustworthy may depend on the audience. Take into consideration whether the audience is made up of scientists, members of the military, or government employees, for example.

Speakers should always act calmly. Do not hesitate when speaking or appear nervous. Do not give the impression that you are holding back information, or that you do not like what you are saying. If you are a nervous speaker, you should practice speaking. Be willing to admit that you do not know everything. If someone asks you a question that you do not know the answer to, say so. Or, you may say "*I do not know, but I will find out the answer to that*". When you are honest about not knowing something, people will assume that you are honest about other things as well. And, it appears that you are not simply trying to look good.

- Trust is linked with perceptions of accuracy and expertise—these qualities work in concert.
- Admit to uncertainty. Facilitate public understanding that risk science is a process.
- Be forthcoming with information and involve the public from the outset.
- Avoid secret meetings.

### 3.4 Communicate with Compassion, Concern, and Empathy

Select a messenger who can really connect with the audience and help them understand that the risk affects their lives personally. This is known as *creating outcome involvement* [19]. Outcome involvement refers to how much the audiences feel that the issue at hand will directly affect their lives. Provided that message, receivers are cognitively able to process information; the more involved they feel, the more they will pay attention to the arguments presented. An audience who feels involved is a thinking audience. The communicator should ask the community what their concerns are. When speaking to the community, use opening remarks to solicit their concern and issues. Address those issues with sincerity. Here are some other practical pieces of advice:

- Stay late after your talk. Show the audience that you are there to answer their questions. This communicates your commitment to their concerns. This principle holds for showing up early too.
- If you make a promise, keep it.
- Provide contact information—give your audience your phone number and/or e-mail address.
- Listen to what various groups have to tell you.

### 3.5 Provide Messages that Foster Efficacy

One of the most common mistakes that risk communicators make is limiting their communication to the susceptibility and severity of the risk. For example, we often communicate that the audience is at high risk, but take no other steps. When people perceive high risk, they are likely to become fearful and anxious. Although this is a natural and effective human response to threat, when people are afraid the "fight or flight" mode is activated.

Bandura [20–22] argued that perceptions of self-efficacy influence thought patterns, actions, and emotional arousal. Self-efficacy refers to the perception that one has the

personal capability to do the things necessary to avert the threat. Bandura also noted, "perceived self-efficacy helps to account for such diverse phenomena as changes in coping behavior produced by different modes of influence" (p. 122). But, self-efficacy is only one part of this picture; audiences must also perceive that the recommendations you are giving to them will work to avert the threat. This latter issue is known as *creating response efficacy*. When individuals have both response and self-efficacy, they will be able to cognitively process information about the risk and engage in "danger control". Danger control refers to behaviors that work at preventing the threat versus simply avoiding the threat.

### 3.6 Conduct Precrisis Planning

Deciding when to communicate is also an important part of strategic risk communication. Scherer [23] describes two types of strategies:

1. Reactive
2. Proactive.

Reactive strategies essentially describe communication that is in reaction to an event or occurrence. This type of strategy does not call attention to a particular risk, but waits until there is already considerable public and media attention about a risk issue.

Advantage

- allows the public to vent about the issue.

Disadvantages

- science may be less relevant when issues become highly emotionally charged;
- places communicator in defensive position;
- people may not believe information that is delayed;
- people may unknowingly be exposed to risk.

Proactive strategies represent a more ongoing risk communication effort. Rather than waiting until an event happens or is subsequently discovered by the public, this type of strategy calls attention to a risk issue, both potential and existing; suggests the agenda for discussion; and provides mechanisms for information exchange.

Advantages

- may alert people to something of which they are not aware;
- allows for a much more meaningful discussion of risk;
- generates more balanced discussion about risk.

Disadvantage

- may alert people to something of which they are not aware.

## 4 CRITICAL NEEDS ANALYSIS AND RESEARCH DIRECTIONS

There is much still to be discovered about risk communication.

### 4.1 Communicating Uncertainty

It was made clear in this article that the biggest difficulty with communicating risk is the uncertainty involved. Data does indicate what does not work well: using ambiguous terms such as "probably", "remote", or "almost certainly" [24]. But, it is less clear *how to* communicate uncertain data. In particular, the importance of considering your audience and messenger cannot be overstated. Fessenden-Raden et al. [25, p. 100] wrote,

> No matter how accurate it is, risk information may be misperceived or rejected if those who give information are unaware of the complex, interactive nature of risk communication and the various factors affecting the reception of the risk message.

Researchers must begin to focus on better ways to communicate uncertainty without frustrating the audience. We suggested earlier using graphic or visual evidence, but even here knowledge is limited. What kinds of visuals are most effective? Is effectiveness moderating by personality factors such as learning styles?

### 4.2 Emotion and Risk

Emotion plays an important role in risk perception. Emotions prompt responses, which facilitate individuals' ability to deal quickly with problems in the environment [10, 26]. And, negative emotions (e.g. anger, fear, and guilt) cause distinct cognitive patterns. Fischhoff et al. [27] found that relative to fear, anger activated optimistic perceptions of terrorism. Lerner et al. [28] found that compared to neutral feelings, anger activated more punitive attributions and more heuristic processing. Turner et al. [13] found that when people perceive that a threat is high (high severity and high susceptibility), their anxiety related feelings increased. This increase in anxiety motivated people to engage in information seeking about the risk, but decreased their ability to correctly process the information. Despite this understanding, much is still unknown. For example, most of the attention has been paid on anger and fear. Yet, guilt is a relevant emotion surrounding risk. Pregnant women, for example, may experience a great deal of anticipated guilt if they are led to believe that a future risk decision could harm their unborn child. Parents generally may feel guilty if they believe their decisions affected their children.

Also, our risk communication can induce emotional responses. There is a great deal of research on fear appeals [1, 12], but little is known about other kinds of emotion appeals such as guilt, anger, disgust, or even hope appeals. Turner [11] has focused attention on anger messages and has found that when the anger appeal is proattitudinal and communicates efficacy, persuasiveness linearly increases. But, we know relatively little about how emotional appeals can be used to motivate emergency preparedness and risk prevention. In situations such as preparing for a terrorist attack, which is emotion laden to begin with, what emotions might be used to motivate people?

## 5 CONCLUSION

Communicating risk is filled with opportunities. When risk is correctly communicated, we have the ability to help people make informed and effective decisions. Effective communication helps ensure that people understand the positive and negative aspects of risk, and that they can process that information without negative emotions overloading their

cognitive capacity. We continue to live in an increasingly dangerous world where national security has become an important focus of our attention. Scientists continue to develop new technologies to thwart such threats, but these technologies lessen some risks and create new risks. Consumers must understand, weigh pros and cons, and make effective decisions about how they deal with such things. To do so, they must be communicated with appropriately and sensitively.

## REFERENCES


1. Witte, K. (1992). Putting the fear back in to fear appeals: the extended parallel process model. *Commun. Monogr*. **59**, 329–349.
2. Slovic, P. (1987). Perception of risk. *Science* **236**, 280–285.
3. Global Risks (2006). (n.d.) *A world economic forum report*. Retrieved October 18, 2008, from http://www.weforum.org/pdf/CSI/Global_Risk_Report.pdf.
4. Slovic, P. (1992). Perceptions of risk: reflections on the psychometric paradigm. In *Risk Communication*, J. C. Davies, V. Covello, and F. Allen, Eds. The Conservation Foundation, Washington, DC.
5. Carroll, J. S. (1978). The effect of imagining an event on expectations for the event: an interpretation in terms of the availability heuristic. *J. Exp. Soc. Psychol*. **14**, 88–96.
6. Tversky, A., and Kahneman, D. (1974). Judgment under uncertainty: heuristics and biases. *Science* **185**, 1124–1131.
7. Tversky, A., and Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science* **211**, 453–458.
8. Ritov, I., and Baron, J. (1990). Reluctance to vaccinate: omission bias and ambiguity. *J. Behav. Decis. Mak.* **3**, 263–277.
9. Spranca, M. D., Minsk, E., and Baron, J. (1991). Omission and commission in judgment and choice. *J. Exp. Soc. Psychol.* **27**, 76–105.
10. Lerner, J. S., and Tiedens, L. Z. (2006). Portrait of the angry decision maker: how appraisal tendencies shape anger's influence on cognition. *J. Behav. Decis. Mak.* **19**, 115–137.
11. Turner, M. M. (2007). Using emotion to prevent risky behavior: the anger activism model. *Public Relat. Rev.* **33**, 114–119.
12. Witte, K. (1994). Fear control and danger control: a test of the extended parallel process model. *Commun. Monogr.* **61**, 113–134.
13. Turner, M. M., Rimal, R. N., Morrison, D., and Kim, H. (2006). The role of anxiety in seeking and retaining risk information: testing the risk perception attitude framework in two studies. *Hum. Commun. Res.* **32**, 130–156.
14. Covello, V. T. (1992). Risk communication: an emerging area of health communication research. In *Communication Yearbook 15*, S. Deetz, Ed. Sage Publications, Newbury Park and London, pp. 359–373.
15. U.S. Department of Health and Human Services (2002). *Communicating in a Crisis: Risk Communication Guidelines for Public Officials*.
16. McCroskey, J. C. (1966). Scales for the measurement of ethos. *Speech Monogr.* **33**, 65–72.
17. Covello V. T., Sandman P., and Slovic, P. (1988). *Risk Communication, Risk Statistics and Risk Comparisons: A Manual for Plant Managers*. Chemical Manufacturers Association, Washington, DC.
18. Covello, V. T. and Allen, F. (1988). *Seven Cardinal Rules of Risk Communication*. US Environmental Protection Agency, Office of Policy Analysis, Washington, DC.

19. Johnson, B. T., and Eagly, A. H. (1989). Effects of involvement on persuasion: a meta-analysis. *Psychol. Bull.* **106**, 290–314.
20. Bandura, A. (1969). *Principles of Behavior Modification*. Holt, Rinehart & Winston, New York.
21. Bandura, A. (1971). *Social Learning Theory*. General Learning Press, New York.
22. Bandura, A. (1986). *Social Foundations of Thought and Action*. Prentice-Hall, Engelwood Cliffs, NJ.
23. Scherer, D.C. (1991). Strategies for communicating risks to the public. *Food Technol.* **45**, 110–116.
24. Cooke, R. M. (1991). *Experts in Uncertainty: Opinion and Subjective Probability in Science*. Oxford University Press, New York.
25. Fessenden-Raden, J., Fitchen, J. M., and Heath, J. S. (1987). Providing risk information in communities: factors influencing what is heard and accepted. *Sci. Technol. Human Values* **12**(3 & 4), 94–101.
26. Frijda, N. H. (1986). *The Emotions*. Cambridge University Press, Cambridge.
27. Fischhoff, B., Gonzales, R. M., Lerner, J. S., and Small, D. A. (2005). Evolving judgments of terror risks: foresight, hindsight and emotion. *J. Exp. Psychol.* **11**, 124–139.
28. Lerner, J. S., Goldberg, J. H., and Tetlock, P. E. (1998). Sober second thought: the effects of accountability, anger and authoritarianism attributions of responsibility. *Pers. Soc. Psychol. Bull.* **24**, 563–574.

## FURTHER READING

Fearn-Banks, K. (2002). *Crisis Communications: A Casebook Approach*, 2nd ed. Lawrence Erlbaum, Mahwah, NJ.

Fisher, A., Pavlova, M., and Covello, V. (Eds.) (1991). *Evaluation and Effective Risk Communications: Workshop Proceedings*. Interagency Task Force on Environmental Cancer and Heart and Lung Disease. EPA/600/9-90/054.

Grunig, J., and Hunt, T. (1984) *Managing Public Relations*. Holt, Rinehart and Winston.

Kasperson, R. E., Golding, D., and Tuler, S. (1992). Social distrust as a factor in siting hazardous facilities and communicating risks. *J. Soc. Issues* **48**(4), 161–187.

Meyer, P. (1988). Defining and measuring credibility of newspapers: developing an index. *Journal. Q.* **65**, 567–574, 588.

National Research Council (1989). *Improving Risk Communication*. National Academy Press, Washington, DC.

Plough, A., and Krimsky, S. (1987). The emergence of risk communication studies: social and political context. *Sci. Technol. Human Values* **12**(3 & 4), 4–10.

Powell, D., and Leiss, W. (1997) *Mad Cows And Mother's Milk: The Perils Of Poor Risk Communication*. McGill University Press, Montreal and Kingston.

Presidential/Congressional Commission on Risk Assessment and Risk Management (1997). *Framework for Environmental Health Risk Management*. Final Report, Volume 1. Available at http://www.riskworld.com/Nreports/1997/risk-rpt/html/epajana.htm.

Renn, O., and Levine, D. (1991). Credibility and trust in risk communication. In *Communicating Risks to the Public: International Perspectives*, R. E. Kasperson, and P. J. M. Stallen, Eds. Vol. 4. Kluwer Academic Publishers, Dordrecht, pp. 175–218.

Sandman, P. M. (1993). Definitions of risk: managing the outrage, not just the hazard. Paper presented at *Regulating Risk: The Science and Politics of Risk*. Washington, DC.

# PROBABILISTIC RISK ASSESSMENT (PRA)

GEORGE E. APOSTOLAKIS

*Engineering Systems Division and Department of Nuclear Science and Engineering, Massachusetts Institute of Technology Cambridge, Massachusetts*

## 1 INTRODUCTION

Probabilistic risk assessment (PRA) is a scenario-based analytical methodology that has been developed to manage the risks of complex technological systems such as nuclear power plants (NPPs) [1], chemical agent disposal facilities [2], and space systems (e.g. the International Space Station (ISS) [3]). It is also called *probabilistic safety assessment (PSA)* and *quantitative risk assessment (QRA)*. In general terms, PRA answers the following three questions [4]: What can go wrong? What are the consequences? How likely is it? The principal PRA results are the probabilities of various consequences of accidents, the identification of the most likely scenarios (event sequences) that may lead to these consequences, as well as the most important (from a risk perspective) structures, subsystems, and components. This information is very valuable to operators, designers, and regulators because the responsible parties can focus resources on what is really important to the safe operation of the system.

For a given system, PRA answers the above three questions by proceeding as follows:

1. A set of undesirable *end states* is defined.
2. For each end state, a set of disturbances to normal operation is defined, which, if uncontained or unmitigated, can lead to this end state. These are called *initiating events (IEs)*.
3. Sequences of events that start with an IE and end at an end state are identified. Thus, *accident scenarios* are generated.
4. The probabilities of these scenarios are evaluated using all available evidence, primarily past experience, and expert judgment.
5. The scenarios are ranked according to their contributions to the frequencies of the end states.
6. Systems, structures, and components are also ranked according to their contributions to the frequencies of the end states.

## 2 SCENARIO IDENTIFICATION

The identification of scenarios that may defeat the built-in defenses of the system and lead to undesirable system states requires intimate knowledge about the system and its operation. These scenarios are the potential failure modes of the system. The development

of the scenario list is usually facilitated by the use of computer codes such as SAPHIRE, RISKMAN, and RiskSpectrum [5].

### 2.1 End States

The end states are any undesirable states that are of interest to the risk manager (decision maker). For example, the two end states that are used routinely in NPP risk assessments are *reactor core damage* and *large, early release of radioactivity to the atmosphere* ("early" means that the release occurs before any evacuation of the surrounding population can be effected). For the ISS, the two end states that have been analyzed are *loss of crew and vehicle* and *evacuation of the ISS*.

### 2.2 Initiating Events

A PRA requires a good understanding of the system and its normal operation. There is usually a set of functions that must be performed for normal operation. For example, in an NPP, the reactor core produces large amounts of heat that must be removed by the cooling systems. Disturbances to the heat production or removal may start a sequence of failures that may ultimately lead to the end states. These disturbances are the IEs. Examples are the loss of off-site electric power and various sizes of loss-of-coolant accidents. For the ISS, the station functions (e.g. propulsion) and the functions needed for the crew's health (e.g. removal of $CO_2$ from the station's atmosphere) are the basis for defining the IEs.

### 2.3 Accident Scenarios

The question now is how an IE could lead to an end state, that is, what additional events (failures) must occur for the end state to materialize. The logic diagram that is used for this purpose is the event tree (*see* Logic Trees: Event, Fault, Success, Attack, Probability, and Decision Trees), which is a decision tree without decision nodes.

The technological systems to which PRAs are applied are well defended. This means that sufficient redundancy and diversity are built into their design to prevent IEs from happening and to mitigate their consequences. Let us suppose that two protective systems, PS1 and PS2, have been designed to mitigate the consequences of a particular IE. Either system can mitigate the consequences. Figure 1 shows how the accident sequences associated with this IE are determined. The top line is the sequence $IE \cap PS1 \cap PS2$, that is, the IE has occurred and both protective systems work. The result is OK, that is, no damage. The sequence leading to *damage level 1* is $IE \cap \overline{PS1} \cap PS2$, that is, the IE has occurred, PS1 has failed, and PS2 has worked. Similarly, *damage level 2* results from the sequence $IE \cap \overline{PS1} \cap \overline{PS2}$, in which both the protective systems have failed.

An event tree may be developed at a high level in which general protective functions are listed, for example, *electric power available*, or at lower levels in which individual systems or subsystems are listed, for example, *off-site power available* and *diesel generator A available*. In the latter case, the number of sequences increases significantly. It is customary to start with high-level event trees and to proceed to develop more detailed trees as the accident sequences are becoming better understood. It is evident that the term *accident sequence* is not well defined since it may be a high-level sequence involving functions or a very detailed sequence involving components. It is common practice to call those sequences involving system failures as accident sequences.

The development of event trees requires detailed knowledge about system function, operation, and intersystem dependencies. Various tools have been developed to facilitate the collection and understanding of the relevant information. For example, event sequence diagrams can be developed to show the sequence of actions required by procedures as various events occur, and dependency matrices to display the dependencies among systems [6, 7].

The next step is the investigation of the failure modes of the systems/functions that appear in the event tree, that is, the protective systems in Figure 1. The question that the analysts ask is "how can PS1 fail?" This question is to be contrasted with the question that is asked when the event tree is developed: "how can this IE lead to an end state?"

The failure modes of individual systems can be identified using fault-tree analysis (*see* Logic Trees: Event, Fault, Success, Attack, Probability, and Decision Trees). The analysis includes hardware failures and human errors during routine operations such as test and maintenance [8]. Human actions during the evolution of an accident sequence are usually placed in the event tree. The unique failure modes of a system resulting from fault-tree analysis are usually called *minimal cut sets*. A minimal cut set is a set of failures whose occurrence guarantees the failure of the system. The word "minimal" means that, if a failure is removed from this set, the system will not fail.

There are still models being developed for human actions that occur post-IE, that is, during the accident [9–12]. The focus is the identification of the contexts within which the human actions occur and the evaluation of the probabilities of errors given a specific context. The context is defined both by the accident sequence that is occurring and various cognitive and organizational crew performance shaping factors. The evaluation of the probabilities is done by utilizing expert judgments supported by extensive discussions of the contexts, the results of simulator exercises, and other supporting information.

In developing the accident sequences and system failure modes, it is important to capture the possible dependencies among systems and components. System functional dependencies are usually included in the event trees. For example, if "availability of ac power" is one of the event tree headings, then all subsequent systems or components that depend on electric power will be assumed failed if electric power has failed. Other major dependencies result when fires, earthquakes, tornadoes, and other similar events occur. These "external" events can cause an IE and, at the same time, affect the performance

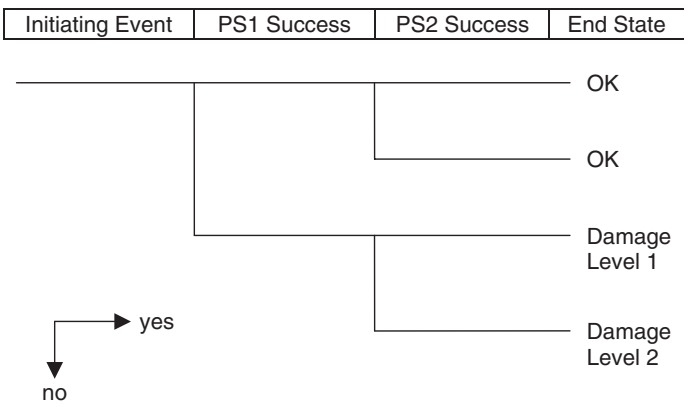



**FIGURE 1** Example of an event tree.

of safety systems. These events and the resulting dependencies are usually investigated separately [13, 14].

The various events that appear in event and fault trees are binary (true–false). We associate an indicator variable $X_j$ with event $j$ so that the event is true (failure) when $X_j = 1$ and false when $X_j = 0$. Then the result of the whole analysis is represented by a logic function that expresses the logical relationship between the end state $k$ and the failures that may lead to it, that is,

$$X_{\mathrm{ES}k} = \varphi(X_1, \cdots, X_n) \equiv \varphi(\underline{X}) \tag{1}$$

where $X_{\mathrm{ES}k}$ is the indicator variable for end state $k$ and $(X_1, \ldots, X_n)$ is the set of (primary or basic) failures that have been input to the logic diagrams. Eq. (1) contains all the information that the logic diagrams have produced. It is called the *structure function of the system*.

Let $\mathrm{AS}_i$ be an accident sequence (or a minimal cut set in the case of fault trees). Eq. (1) is equivalent to

$$X_{\mathrm{ES}k} = \sum_{i=1}^{N} \mathrm{AS}_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \mathrm{AS}_i \mathrm{AS}_j + \cdots + (-1)^{N+1} \prod_{i=1}^{N} \mathrm{AS}_i \tag{2}$$

where $N$ is the total number of accident sequences and

$$\mathrm{AS}_i = \prod_{X_m \in \mathrm{AS}_i} X_m \tag{3}$$

that is, the indicator variable of accident sequence $\mathrm{AS}_i$ is the intersection of all the indicator variables of the failure events that belong to this accident sequence.

The binary modeling of systems and components (success–failure) that is employed in event trees and fault trees is not appropriate when phenomenological (physical, chemical, and biological) processes must be considered in the evaluation of the end states. For example, the analysis of fires requires models for the fire plume and the radiative and convective heat transfer processes that may damage systems and components [14]. These analyses result in accident scenarios that consist of the sequences of the phenomenological processes which, in combination with binary component failures, may lead to the end states.

Risk assessments for nuclear waste geologic repositories [15, 16] are completely dominated by phenomenological processes and the concept of binary accident scenarios is of little use. The end state is usually the amount of radioactivity released to the accessible environment at a particular time (e.g. 10,000 years in the future). The so-called base-case scenario models the evolution of the repository during very long times using a suite of computer programs that model the interdependent physical and chemical processes that are expected to occur. Similarly, when an IE is considered, such as human intrusion via exploratory drilling for natural resources, the evaluation of the end state is again done using the computer programs. The formulation of Eqs. (1–3) does not apply to these "performance assessments" (as risk assessments for repositories are called). Accident scenarios as defined in Eq. (3) cannot be identified (a proposal for an alternative scenario definition appropriate for performance assessments is presented in [17]). We will see later that a similar situation arises when infrastructures are investigated in the sense that

computer programs appropriate to the specific infrastructure must be used to determine its response to external disturbances.

## 3 PROBABILITIES

The probability distribution of an end state requires the probability distributions of the primary failure events that are input to the event and fault trees. In mathematical terms, the probability distributions of the indicator variables $X_i$ are propagated through Eq. (2), the logic of the system, to produce the probability distribution of the indicator variable for the end state $X_{\mathrm{ES}k}$. This leads us to the following equations:

$$R_k \equiv \Pr\left(X_{\mathrm{ES}k}\right) = \sum_{i=1}^{N} \Pr\left(\mathrm{AS}_i\right) - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} \Pr\left(\mathrm{AS}_i \mathrm{AS}_j\right) + \cdots + (-1)^{N+1} \prod_{i=1}^{N} \Pr\left(\mathrm{AS}_i\right) \tag{4}$$

where

$$\Pr\left(\mathrm{AS}_i\right) = \Pr\left(\prod_{X_m \in \mathrm{AS}_i} X_m\right) \tag{5}$$

The probabilities of the accident sequences $\Pr\left(AS_i\right)$ are produced from the probabilities of the primary failures that are input to the event and fault trees. In Eq. (5), the probability of the accident sequence is not, in general, the product of the primary failure probabilities; the dependencies among the primary failures must be taken into account [6, 7].

The primary failure probabilities are generally low ($<0.1$), and so the resulting probabilities of the end states are very low ($<10^{-2}$). In other words, we are in the realm of rare events. This is a consequence of the fact that, as stated earlier, these technological systems are well defended, that is, sufficient redundancy and diversity are built into their design to reduce their failure probabilities to acceptable levels.

As the failure probabilities become small, the uncertainties become large because the statistical evidence from system operation becomes weak (this is, of course, also true for "new" designs for which there may be no operational experience). This means that the analysts must rely on expert judgment in evaluating probabilities. Such judgments are subject to biases [18], thereby increasing the uncertainties. This state of affairs creates the need to examine interpretation of the concept of probability.

### 3.1 Interpretation of the Concept of Probability

The theory of probability, as expounded in textbooks, is an axiomatic mathematical theory that needs no interpretation. In engineering practice, however, it is useful to have an interpretation in mind. In risk assessment, in particular, the rarity of the events of interest makes it a necessity [19, 20].

The usual interpretation of probability is as the limit of relative frequencies. This interpretation is very restrictive for PRA. It allows the use of statistical evidence only in

probability evaluations, whereas, as stated above, the use of expert judgment is inevitable when rare events are analyzed. The uncertainties in the probability estimates are expressed in terms of confidence intervals, which are impossible to propagate in any meaningful way through the structure function of the system (Eq. 1) to produce a statement on the uncertainties of the probabilities of the end states. There are no PRAs that have been conducted with this interpretation in mind.

Probability is interpreted as a measure of degree of belief [21]. We accept that it is meaningful to say that one judges an event to be more (equally, less) likely than another event. Probability is simply a numerical expression of this judgment. When we say that event A has probability 0.6, we mean that A is more likely than any other event whose probability is less than 0.6 and it is less likely than all events whose probability is greater than 0.6. This primitive notion of likelihood, along with several other axioms, allows the development of a rigorous mathematical theory of subjective probability. Both the frequentist and subjectivist interpretations are consistent with the mathematical theory of probability.

It is useful to discuss how this concept is applied to PRA. The analysis begins by constructing a "model of the world", that is, a mathematical model of the system that may include the development of its structure function using event and fault trees as well as models for physical processes such as hear transfer. The "world" is defined as *the object about which the person is concerned* [22]. Occasionally, we refer to the model of the world as simply the model or the mathematical model. Constructing and solving such models is what most physical scientists and engineers do.

There are two types of models of the world, deterministic and probabilistic. The former include event and fault trees for the system logic and mechanistic models for physical processes such as convective heat transfer. Although it would be highly desirable to have the complete PRA done using deterministic models, we soon realize that many important phenomena cannot be modeled deterministically. For example, the failure time of a component while running (assuming a successful start) exhibits variability that we cannot eliminate; it is impossible for us to predict when the failure will occur. We, then, construct a model of the world that reflects this uncertainty. This model is usually the exponential distribution whose probability density function (pdf) is

$$f(t/\lambda, M) = \lambda e^{-\lambda t} \tag{6}$$

This expression shows explicitly that this probability is conditional on our knowing the numerical value of the parameter $\lambda$ (the failure rate) and accepting the assumption $M$ that the exponential model is appropriate, that is, its fundamental assumption that the failure rate is constant is valid. This observation is valid for deterministic models as well. For example, event trees are developed making assumptions regarding the success criteria of the protective systems. As another example, the development of deterministic models for fires requires assumptions regarding the fire plume. The numerical values of parameters of such models like the burning rate of the fuel must be known for the models to be used.

The uncertainty described by the model of the world is sometimes referred to as *randomness* or *stochastic uncertainty*. Recently, the term *aleatory models* was adopted because the preceding terms are used in many contexts in probabilistic analyses.

As stated above, each model of the world is conditional on the validity of its assumptions, $M_i$, and on the numerical values of its parameters. In general, the model has a

number of parameters, which can be represented in vector form as $\theta$. Since there is usually uncertainty associated with $M_i$ and $\theta$, we introduce the *epistemic* probability model that reflects in quantitative terms our state of knowledge (degree of belief) regarding the validity of $M_i$ (and hence the results of the model of the world) and the numerical values of $\theta$. It is important to bear in mind that the model of the world deals with observable quantities, such as failure times, and the epistemic model with parameters and assumptions that are not observable.

In its landmark Regulatory Guide 1.174 that established the framework for risk-informed regulatory decision making [23], the US Nuclear Regulatory Commission staff considers three categories of uncertainties: parameter, model, and completeness. Although we could consider the last two as part of model uncertainties, it may be useful in some cases to consider completeness separately. The Regulatory Guide states: "Completeness is not in itself an uncertainty, but a reflection of scope limitations. The result is, however, an uncertainty about where the true risk lies. The problem with completeness uncertainty is that, because it reflects an unanalyzed contribution, it is difficult (if not impossible) to estimate its magnitude. . . . There are issues, however, for which methods of analysis have not been developed, and they have to be accepted as potential limitations of the technology. Thus, for example, the impact on actual plant risk from unanalyzed issues such as the influences of organizational performance cannot now be explicitly assessed." Completeness is expected to be a major issue in terrorism studies.

Parameter uncertainties are usually represented by pdf's $\pi(\theta/M_j)$ that are produced using statistical evidence and expert judgments, as it is seen later. Model uncertainties are handled in a variety of ways, for example, using qualitative arguments, sensitivity studies, and expert judgments. Completeness uncertainties are handled in the context of decision making. For example, qualitative arguments may be made that completeness is not a significant issue for the decision to be made. Alternatively, additional safety-related requirements may be imposed that are not based on the PRA results (in other words, the decision-making process is risk *informed* rather than risk *based*).

### 3.2 The Epistemic Distributions and Expert Judgment

There are two kinds of evidence that are utilized to develop the epistemic pdf for the parameters: event-specific statistical evidence, $E_S$, and generic information, $E_G$, from other sources. To make the discussion concrete, we will deal with one parameter, the failure rate $\lambda$ of the exponential model (Eq. 6). Let $\pi(\lambda/E_G, M)$ be the pdf developed from generic information. The epistemic pdf for the failure rate is produced by combining $E_G$ with $E_S$ using Bayes' theorem:

$$\pi'(\lambda/E_{\mathrm{S}}, E_{\mathrm{G}}, M) = \frac{\pi(\lambda/E_{\mathrm{G}}, M)L(E_{\mathrm{S}/\lambda}, M)}{\displaystyle\int_0^\infty \pi(\lambda/E_{\mathrm{G}}, M)L(E_{\mathrm{S}}/\lambda, M)d\lambda} \tag{7}$$

The term $L(E_S/\lambda, M)$ is the likelihood of the evidence $E_S$ assuming that $\lambda$ is known and is calculated using the model of the world. In the case of component failures, the evidence $E_S$ may consist of the failure times of $n$ components, $t_1, \ldots, t_n$. Then, the

likelihood function is

$$L(E_S/\lambda, M) = \lambda^n \exp\left[-\lambda\left(\sum_1^n t_j\right)\right] \tag{8}$$

Expert judgment is prevalent in this formulation. Determining the evidence $E_S$ itself is usually not straightforward. Deciding what constitutes a "failure" and whether the operating conditions of the failed component were "identical" to those of the component of interest requires the exercise of judgment on the part of the analysts. In many cases, however, the impact of this judgment is overwhelmed by the judgment required to develop the generic pdf $\pi(\lambda/E_G, M)$.

Generic information may take many forms. For example, some generic sources may report "point" values of the failure rate while others may report a pdf. The degree of applicability of the information provided may also be an issue. For example, information on dependent failures in NPPs may be utilized to develop pdfs for such failures in space systems in which both the operating environment and the personnel culture are different. Widely acceptable methods for handling such situations are not available.

In cases of large model uncertainties and when the issue is of such importance that appropriate resources are available, the elicitation and processing of expert judgments have been formalized [13, 24, 25]. The purpose of the elicitation process is to reduce the biases as much as possible and to train the experts on how to express their judgments in terms of probabilities. The processing of the elicited judgments may be done in a number of ways all having advantages and disadvantages.

## 4 PRA RESULTS AND RISK MANAGEMENT

The epistemic distributions of the probabilities of the primary inputs to the PRA model are propagated through the model usually via Monte Carlo simulation to produce an epistemic distribution for the probability of each accident sequence, Eq. (5), and ultimately for each end state, Eq. (4). Monte Carlo simulation is also used when physical and chemical processes are modeled as in performance assessments. Because of the long running times of the computer programs involved, Latin hypercube sampling is employed to reduce the number of Monte Carlo trials [26].

Figure 2 shows the result for the end state *latent cancer fatalities* for an NPP [27]. The risk curves show the frequency of a given number of fatalities or greater. As an example, the frequency of 100 or more cancer fatalities has epistemic uncertainty that ranges from about $4 \times 10^{-7}$ per reactor year (fifth percentile) to about $3 \times 10^{-5}$ per reactor year (95th percentile). This uncertainty is the result of all the epistemic uncertainties associated with the primary inputs to the PRA (IE frequencies, component failure rates, human error rates, phenomenological uncertainties associated with severe accidents, and others) propagating through the PRA model. The mean and median frequency can also be found in the figure. An examination of the accident sequences that contribute the most to cancer fatalities shows that the dominant sequences are initiated by station blackout (all ac power lost) and sequences that bypass the containment. The complete accident sequences initiated by these events are detailed in the PRA report.

For the end state *core damage*, the results for the same plant are fifth percentile, $1.2 \times 10^{-5}$; median, $3.7 \times 10^{-5}$; mean, $5.7 \times 10^{-5}$; and 95th percentile, $1.8 \times 10^{-4}$

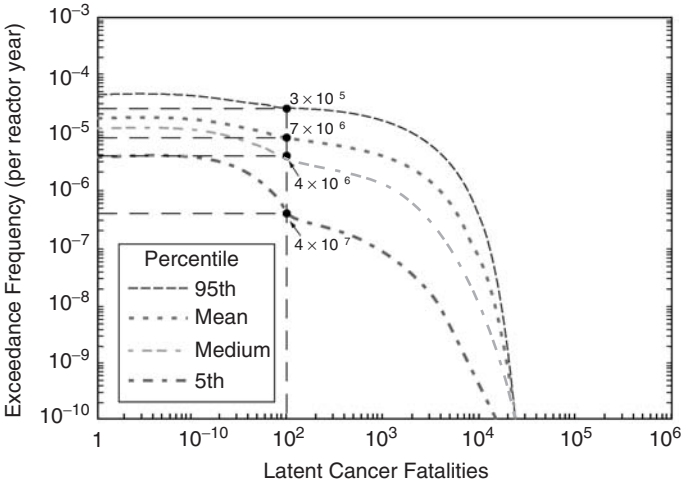



**FIGURE 2** Example of risk curves.

per reactor year. The dominant accident sequences for this end state are loss-of-coolant accidents and station blackout.

These results serve two purposes: they allow a determination as to whether the frequencies of the end states are "acceptable" by the society (or its representatives, that is, the relevant regulatory agencies) and, if it is found that the risk is "unacceptable" or if risk reduction is cost effective, measures can be taken to reduce the frequency of the dominant sequences. The risks that society "accepts" or "tolerates" (see, for example, [28]) are usually the basis for deciding what risks are "acceptable". The Nuclear Regulatory Commission has adopted quantitative heath objectives that define an acceptable level of risk from NPP operations that is 0.1% of all other risks to which an average individual of the public is exposed [29]. The United Kingdom Health and Safety Executive considers three regions of risk [30]. Risks to an individual of the general public greater than $10^{-4}$ per year (probability of death) are generally unacceptable and risks smaller than $10^{-6}$ per year are considered to be broadly acceptable. The region between these two limits is the tolerability region and represents risks "from activities that people are prepared to tolerate in order to secure benefits". The risks in this region are kept as low as reasonably practicable.

When the uncertainties in the frequencies of the end states are so large that they inhibit meaningful risk management, it may be possible to define subsidiary objectives for which the uncertainties are smaller. This is the case with NPPs. Because the uncertainties associated with the evaluation of individual risks are very large, the Nuclear Regulatory Commission staff is using a goal of $10^{-4}$ for the frequency (per year) of reactor core damage and $10^{-5}$ for the frequency (per year) of a large release of radioactivity from the containment building before evacuation of the surrounding population can be effected. These values are compared with the epistemic means of the frequencies of the corresponding end states.

Additional information useful to risk management is provided by assessing the relative importance of the thousands of events that are included in the PRA. This is done using importance measures [31]. One such measure is the risk reduction worth (RRW) of an

event. It is defined as follows:

$$\mathrm{RRW}_i^k = \frac{R_k}{R_k^{-i}} \tag{9}$$

where $\mathrm{RRW}_i^k$ is the risk reduction worth of event $i$ with respect to end state $k$ and $R_k^{-i}$ is the risk metric $R_k$ (Eq. 4) with the $i$th event assumed to always be a success (zero probability of failure).

This importance measure is particularly useful for identifying improvements in the reliability of elements, which can most reduce the risk. Using this importance measure, [31] finds that, with respect to the end state *core damage*, reducing the frequency of very small loss-of-coolant accidents could lead to a core damage frequency reduction of up to 38% in a particular case. Similarly, the improvement of the operator ability to control sprays during a small loss-of-coolant accident could reduce the core damage frequency by up to 37%.

Other importance measures used in practice are the Fussell–Vesely (FV) and the risk achievement worth (RAW) measures. The FV measure is defined as follows:

$$\mathrm{FV}_i^k = \frac{R_k - R_k^{-i}}{R_k} = 1 - \frac{R^{-i}}{R_k} = 1 - \frac{1}{\mathrm{RRW}_i^k} \tag{10}$$

As Eq. (10) shows, this measure can be derived from $\mathrm{RRW}_i^k$; therefore, it does not provide any additional information.

RAW is defined as follows:

$$\mathrm{RAW}_i^k = \frac{R_k^{+i}}{R_k} \tag{11}$$

where $R_k^{+i}$ is the risk metric $R_k$ (Eq. 4) with the $i$th event assumed to be always a failure (probability of failure equal to unity). RAW is a measure of the "worth" of a basic event in "achieving" the present level of risk and indicates the importance of maintaining the current level of reliability for this basic event.

Importance measures have found a variety of applications in risk management. They have been used to establish the maintenance strategy for systems and components at facilities so that specific reliability targets can be met. This allows maintenance to be performance based rather than prescriptive. Importance measures have also been used to identify systems and components on which special quality assurance requirements are imposed that go beyond the normal industrial standards. An application of this concept to infrastructures is seen later in this article.

The PRA results (probabilities of end states, dominant accident sequences, and important events) are extremely useful to risk management. It is important to point out, however, that decisions made by responsible authorities are never risk based. There are too many judgments and uncertainties (especially those due to models and completeness) for decisions to be risk based [23, 32]. The risk results are submitted to a deliberative process in which the known and unknown uncertainties are discussed and the assumptions behind the analyses are scrutinized. The decisions are usually based on a combination of risk insights, qualitative engineering analyses, and traditional safety measures that are precautionary in nature [33]. Such an "integrated decision-making process" [23] relies

on the experience and judgment of the risk managers and usually leads to decisions that are more conservative than the risk numbers would suggest. This approach is similar to the analytic-deliberative process for decision making proposed by the National Research Council [34]. The prioritization of accident sequences and events that PRA produces is the starting point for the deliberation among the risk managers (or, more generally, the stakeholders [35]). Risk management for terrorism is also expected to be risk informed rather than risk based.

## 5 TERRORISM

### 5.1 Challenges

After September 11, 2001, protection against terrorism has become a US and international focus and is likely to remain one in the foreseeable future. Large amounts of resources are expended to prevent terrorist acts and to mitigate their consequences if they occur. Given the many forms, terrorist acts can assume and the openness of democratic societies, it is evident that attempting to protect against all such acts is impossible. As an example, [36] offers numerous recommendations for vulnerability reduction in several diverse infrastructures. Implementing all of them would impose a considerable financial burden on the United States and would ignore the relative importance of these vulnerabilities.

It is evident that a prioritization of the national needs for protection against terrorism is needed. Since PRA has been proven to be an effective analytical tool for prioritizing accident sequences in complex technological systems, it is natural to explore the possibility of using it in combating terrorism. We must acknowledge, however, that the application of PRA to terrorism poses challenges that must be overcome.

Before we proceed to discuss challenges specific to terrorism, we state some major PRA limitations that exist even for applications to technological systems [32, 37, 38]. As mentioned earlier (Section 1.3), models are still being developed for human actions that occur post-IE, that is, during the accident [9–12]. At this time, there is no universally accepted model for such human actions, especially for errors of commission (the crew does something that worsens the situation). A related topic is that of the influence of organizational and managerial factors. Although they are recognized as having an important impact on personnel performance [39], they are not included in PRAs explicitly. It is stated in [32] that it is doubtful that the inclusion of organizational factors in PRA will be achieved any time soon. Finally, probabilistic models for digital software systems that are embedded in the system are in their infancy [40]. These challenges will, of course, be present when PRA methodology is applied to terrorism. Additional challenges due to some unique features of assessments that involve malevolent acts are discussed below.

The end states in technological system PRAs are very few (two or three) and are focused on health and safety impacts. Because they are very few, the results can be used easily by risk managers in combination with other requirements in their “integrated decision-making process” (deliberation) that ultimately leads to action. For specific assets and for specific purposes, the number of end states can be kept small even in the case of terrorism. As an example, the US Nuclear Regulatory Commission focuses on public health and safety and states [41]: “For the facilities analyzed, the results confirm that the likelihood of both damaging the reactor core and releasing radioactivity that could affect public health and safety is low. Even in the unlikely event of a radiological release, due

to a terrorist use of a large aircraft against an NPP, the studies indicate that there would be time to implement the required on-site mitigating actions."

For terrorism, the set of end states must be expanded considerably. As we stated earlier, the end states are determined by the risk manager (decision maker) because they are judged to be important to the decision. Decisions involving terrorism are usually based on more than just health and safety impacts. As stated in [42], "the end states must reflect initial, cascading, and collateral consequences (or levels of damage)". This approach leads to a large number of candidate end states. These include end states related to health and safety such as fatalities and injuries; economic losses such as the value of the assets attacked and replacement/repair costs; environmental impacts on flora and fauna; national security such as impacts on government functions; and many others. An additional complication is that some of the impacts may be immediate and others delayed. It is evident that not all of these end states are equally important or relevant to all situations. The end states to be evaluated depend on the assets under attack, the nature of the threat, and the interests of the risk managers (the decision makers).

The construction of scenarios leading to the end states is also a challenge. An important feature of technological systems to which PRAs have been applied is their spatial compactness. By focusing on NPPs and limiting the number of end states, the US Nuclear Regulatory Commission has been able to evaluate scenarios initiated by aircraft attacks using traditional PRA methods, as stated above. A major concern in terrorist studies is the vulnerability of infrastructures. These are interconnected across systems and spread out geographically [43]. Further, societal infrastructures have overlapping ownership and responsibility in private organizations and local, state, and national government. Therefore, technical complexity may be compounded by sociopolitical complexity. The views of stakeholders must be taken into account.

A traditional PRA requires the probabilities of IEs. The evaluation of the probability of a terrorist attack is a major challenge. Even if one resorts to expert opinion elicitation methods as discussed above in the context of model uncertainties, the uncertainties will be very large. Questions such as who the experts are and whether they have access to all available information contribute to these uncertainties. A major complicating factor is the fact that terrorist groups, unlike accidents, are intelligent and adaptable adversaries.

The challenges we have discussed have created a fertile area of research. Several investigators have proposed ideas and approaches to the management of terrorism risks that build on the principles of risk assessment and management. Thus the authors of [42] provide a detailed review of PRA methods and discuss how they would apply to terrorism. Traditional event trees are used to analyze a sample regional grid and the relevant probabilities are assumed to be produced by expert judgment. One of the authors' conclusions is: "It is with respect to catastrophic attacks that the principles and practices of quantitative risk assessment have their greatest value. The structuring of catastrophic attack scenarios could be one of the most important short-term benefits of quantitative risk assessment."

The observation that terrorist groups are intelligent adversaries has prompted researchers to explore the applicability of game theory. The authors of [44] develop an "overarching model" whose objective is to organize the mass of available information and to bring together various types of threat scenarios, various groups of attackers, and the amount of damage they could inflict. Decision analysis is employed to prioritize the threats and game theory helps in analyzing the dynamics of the events and the moves and countermoves of the United States and the perpetrators. A conclusion

is: “In designing and implementing strategies of response to potential terrorist attacks, it is essential to think beyond the reoccurrence of the last event. . . . The model presented here involves, in particular, probabilistic dependencies, and it uses a forward-looking approach to generate a set of possibilities and scenarios.” The authors argue that “ . . . in its practical application, the analysis must include the dynamics of the events and the moves and countermoves of both sides (the United States and the perpetrators)”.

Game theory, optimization methods, and reliability analysis are applied in [45] to simple series and parallel systems of components to develop insights into the nature of optimal defensive investments for managing terrorist attacks. The authors reach the following interesting conclusion: “Our results suggest that some high-value targets with a low probability of being successfully attacked may not merit investment, while other (less valuable but more vulnerable) targets may merit defending”.

Finally, game theory has been applied to the security analysis of computer networks [46]. The authors determine the Nash equilibria in a two-player (the attacker and the administrator) stochastic game and argue “a Nash equilibrium gives the administrator an idea of the attacker’s strategy and a plan for what to do in each state in the event of an attack”.

## 5.2 A Proposed Framework for Infrastructures

A framework that combines decision analysis [47] and PRA methods has been proposed and implemented in several infrastructure studies [48–50]. Decision analysis allows us to focus on the interests of the risk managers and stakeholders and to include the end states of concern to them. The objective is to rank the infrastructure elements according to their value to the decision maker. A further objective is to identify specific issues that arise when risk assessment methods are applied to infrastructures. The general framework is shown in Figure 3 and explained below.

The methodology begins by identifying assets and components of the infrastructure whose failure may lead to undesirable consequences. These failures may be random, in which case a traditional PRA is performed for the infrastructure, or due to a malevolent act, in which case terrorism or vandalism is analyzed. The element failures are the IEs in this case. The physical consequences of these failures are determined by analyzing the response of the infrastructure and human intervention. A central concept is that each of the infrastructure elements is characterized by a “capacity”. This concept can represent a carrying capacity, production, or consumption of goods. Any infrastructure has some characteristic that can be considered as its capacity. The units of this capacity might be the amount of water produced by treatment plants and transported by pipelines in a water-supply system [49] or the electric power generated by generators and transmitted by transmission lines in a power-supply system [50].

There is a physical limit on the amount of goods that can be generated/processed/transported/consumed by each element. The assumed failure of an element leads to a rearrangement of the amounts transported and consumed possibly leading to cascading failures. This analysis requires appropriate computer programs such as the Sandia AC load flow simulation model [51] for a bulk power infrastructure that was used in [50]. The consideration of the capacity of the infrastructure elements makes this analysis different from traditional PRAs, in which the performance of each element is modeled as a success or failure, thus leading to Boolean expressions such as those of Eqs. (1–3). This analysis resembles that conducted in performance

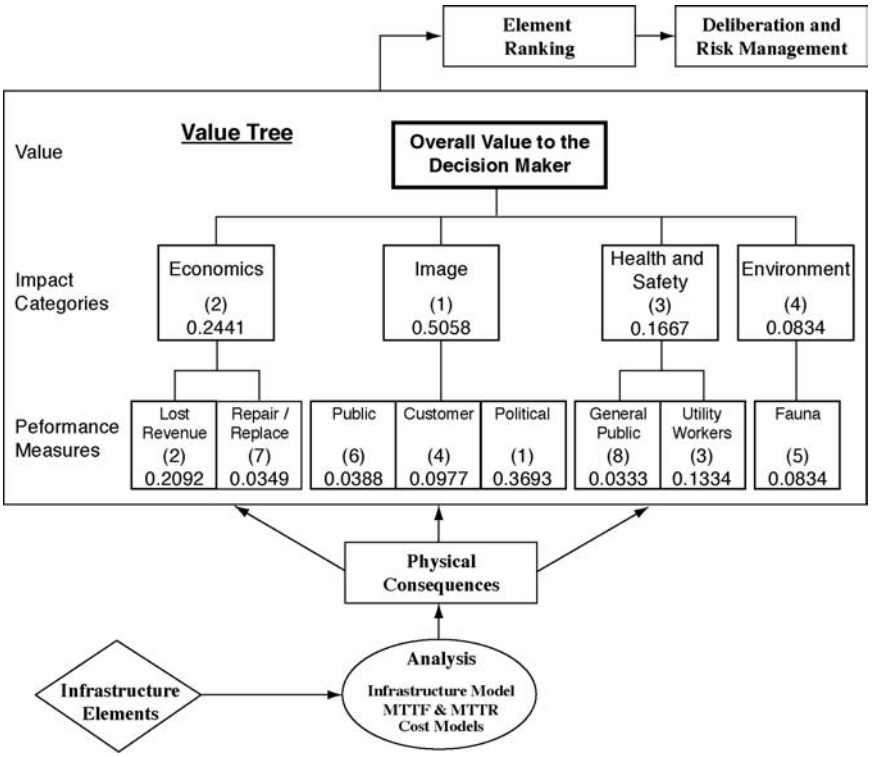



**FIGURE 3** A general framework for the evaluation of infrastructure elements.

assessments in which simulation models are used for the relevant physical and chemical processes.

The physical consequences of the failure of an infrastructure element include the numbers and types of customers affected (industrial users and individual households) and the duration of the denial of service, for example, power outages and no water supplies. The evaluation of these consequences requires inputs, such as the mean time to failure (MTTF) and mean time to repair (MTTR) of individual elements, cost estimates, and other inputs as appropriate for the problem at hand.

The physical consequences are input to a value tree that incorporates the decision maker's views on possible impacts. The value tree is then used to determine the impact the consequences have on the decision maker. The amount of impact a component represents to the decision maker is its value. Each component value is combined with its susceptibility to failure or attack. The combination of value and susceptibility is used to rank the components according to their risk significance.

In order to be able to assess the value of the physical consequences, the value system of the decision maker needs to be modeled explicitly. The value tree, also called *objectives hierarchy* [47], is based on multiattribute utility theory (MAUT) and provides a hierarchical view of the impact each physical consequence may have on the stakeholders. The value tree generally consists of three levels in which the top level is the overall impact, or value, of a failure scenario (Fig. 3). The second level breaks this overall impact into broad categories that we call impact categories. In the third level, these categories

are expressed as specific attributes, called *performance measures (PMs)*, that specifically describe the various ways physical consequences result in impacts to the decision maker.

In order to be able to rank the element failures, we need a single index that combines all the impacts (PMs) into a single number. This index includes the relative weights the decision maker assigns to the PMs and a number representing the degree of impact of each physical consequence on each PM (the "disutility" of that level).

The relative weights of the PMs can be determined using one of several methods that exist in the literature [47]. We have found the analytic hierarchy process (AHP) [52] particularly useful. The AHP is a hierarchical method of pairwise comparisons in which preferences among objectives are converted into numerical weights. Since the decision maker has already structured the value tree in a hierarchical arrangement, the application of AHP is fairly straightforward. In performing AHP, the decision maker first makes pairwise comparisons of the impact categories with respect to the overall goal. After making these comparisons and establishing the weights of the categories, the decision maker compares the next level of objectives (the PMs) to the objective above it. It is important to remember that the comparisons of objectives are not made in an absolute sense; they are made, instead, with respect to the decision context at hand. This means that the decision maker does not compare, for example, *health and safety* to *image* in general; rather, he/she compares them with respect to the *overall value to the agency* in the context of the problem that is being investigated. Therefore, the decision maker must be mindful of the ranges of the corresponding PMs. An advantage of the AHP is that it offers an estimation of the consistency of the judgments of the decision maker. We point out that the AHP is used here as a means for producing relative weights from stakeholder input and not as a decision-making method. The latter use has been criticized in the literature, for example, in [53, 54].

Figure 3 shows the relative weights for a particular decision maker. The relative rankings of the various elements of the value tree are shown in parentheses. Thus the decision maker ranks the impact category *image* as the most important and *environment* as the least important. This is a good example of our earlier comment that the evaluation is made in the context of the specific decision that the decision maker must make. In the present case, the decision maker was aware of the fact that failures of infrastructure elements would have very minor physical consequences. However, the political consequences of even the smallest failure would be major.

In several applications, we have found that the impact categories shown in Figure 3 capture the stakeholder concerns. Of course, the relative weights vary according to the application.

The PMs are described by constructed scales, that is, discrete levels of potential impacts on each PM. As an example, Table 1 shows the constructed scale and associated disutilities for the PM *image with the general public*. The disutilities are developed in close collaboration with the decision maker using pairwise comparisons of the levels of the constructed scale. Figure 3 shows the relative weights and rankings of the PMs in our example. Again, the most important PM for the decision maker in this problem is *political*.

The average performance index (PI) of a failure scenario is determined using the following equation:

**TABLE 1 Constructed Scale for the Performance Measure "Image with the General Public"**

| Level | Constructed Scale | Disutility |
|---|---|---|
| 4 | International interest from the media | 1.0 |
| 3 | Repeated articles in the national media, mention in the international media | 0.4092 |
| 2 | Repeated articles in the local media, appearance in the national media | 0.1363 |
| 1 | Single appearance in the local media | 0.0374 |
| 0 | No negative image with the general public | 0.0 |

$$\overline{\mathrm{PI}}_j = \sum_{i=1}^{k_{\mathrm{PM}}} w_i \overline{d}_{ij} \tag{12}$$

where $\overline{PI}_j$ is the expected performance index of the scenario initiated by the failure of element $j$, $w_i$ is the weight of the performance measure $i$, $\overline{d_{ij}}$ is the expected disutility of performance measure $i$ and failure scenario $j$, and $k_{PM}$ is the total number of PMs.

An intermediate step not shown in Eq. (12) is the evaluation of the physical consequences of scenario $j$, which are converted to the levels $d_{ij}$ of the constructed scales of the corresponding PM.

The additive independence assumption made in establishing Eq. (12) means that the preferences among the PMs can be assessed independently of one another. The analysts should work with the decision maker to confirm that the PMs are reasonably independent. The independence assumption is very strict and is rarely satisfied fully in practice. Nevertheless, it is widely used in applications. As stated in [47]: "Even if used only as an approximation, the additive utility function takes us a long way toward understanding our preferences and resolving difficult situations." Reference 47 also states: "In extremely complicated situations with many attributes, the additive model may be a useful rough-cut approximation". An additional safeguard is that the results of the formal analysis are subjected to deliberation, in which the decision maker evaluates the results of the analysis for reasonableness.

The physical consequences correspond to the end states of a traditional PRA. Unlike the framework described above, the values of the decision maker are not stated explicitly but, rather, are taken into account in the deliberation that is part of the integrated decision-making process. This is possible because the end states are part of a single impact category (that is, they are all related to health and safety) and their number is kept small. A proposal to apply the framework presented here to NASA systems is presented in [55].

### 5.3 Risk Ranking

The average performance index $\overline{PI}$ is the metric that should be used to rank the infrastructure elements. The inequality $\overline{PI}_j > \overline{PI}_m$ means that the decision maker assesses that element $j$ is of higher disutility, that is, its failure leads to less desirable consequences, than element $m$. From a risk management perspective, element $j$ should attract more attention than element $m$.

As shown in Eq. (12), the theory demands that the average PI should be calculated. This means that all the uncertainties should be accounted for in the analysis. These include the uncertainties in the failure rates of the elements. When random failures are considered, these uncertainties can be evaluated using past experience and expert judgment, as is done in traditional PRAs. In the case of terrorism or vandalism, however, the probabilities of successful attacks are difficult to evaluate in a meaningful way. Reference 42 argues that expert opinions can be used in this evaluation. This approach would require access to intelligence information that is generally unavailable and also raises the question of whether experts on this issue actually exist.

An alternative to the evaluation of the probabilities of a successful attack is to calculate a conditional PI assuming that the threat exists. Similarly, the disutilities of the various consequences are assessed conservatively so that probabilities are not needed. The conditional PI is then

$$\mathrm{PI}_j = \sum_{i=1}^{k_{\mathrm{PM}}} w_i d_{ij} \tag{13}$$

where $\mathrm{PI}_j$ is the performance index of the scenario initiated by the failure of element $j$ and $d_{ij}$ is the conservative value of the disutility of performance measure $i$ and failure scenario $j$.

Even though the probability of attack has been excluded from Eq. (13), the structuring of the scenarios that lead to physical consequences depends on the nature and magnitude of the assumed threat. In the applications of the methodology presented in [48–50], the threat is assumed to be "minor". This means that major attacks that fail several infrastructure elements at the same time are not considered. Minor threats (vandalism) emanate from individuals or small groups of individuals and not from organized terrorist organizations.

Although Eq. (13) excludes the probability of a successful attack, we can add more information to the ranking process by including the susceptibility to attack of the infrastructure elements. As Table 2 shows, we consider six levels of susceptibility to malevolent acts ranging from completely secure (the lowest level) to completely open (the highest level). These susceptibility levels are combined subjectively with the numerical results for the PI to place a scenario into one of five color categories as shown in Table 3. Table 4 shows how the categories were developed by combining susceptibility and PI in one particular case. The decision maker should develop a similar table for the problem in hand. This subjective evaluation, which may lead to results inconsistent with those

**TABLE 2 Susceptibility Levels of Infrastructure Elements**

| Level | Description |
|---|---|
| 5—Extreme | Completely open, no controls, no barriers |
| 4—High | Unlocked, non-complex barriers (door or access panel) |
| 3—Moderate | Complex barrier, security patrols, video surveillance |
| 2—Low | Secure area, locked, complex closure |
| 1—Very low | Guarded, secure area, locked, alarmed, complex closure |
| 0—Zero | Completely secure, inaccessible |

**TABLE 3 Vulnerability Categories**

| Vulnerability Category | Description |
|---|---|
| Red | This category represents a severe vulnerability in the infrastructure. It is reserved for the most critical locations that are highly susceptible to attack. Red vulnerabilities are those requiring the most immediate attention. |
| Orange | This category represents the second priority for counter terrorism efforts. These locations are generally moderate to extreme valuable and moderately to extreme susceptible. |
| Yellow | This category represents the third priority for counter terrorism efforts. These locations are normally less vulnerable because they are either less susceptible or less valuable than the terrorist desire. |
| Blue | This category represents the fourth priority for counter terrorism efforts. |
| Green | This is the final category for action. It gathers all locations not included in the more severe cases, typically those that are low (and below) on the susceptibility scale and low (and below) on the value scale. It is recognized that constrained fiscal resources is likely to limit efforts in this category, but it should not be ignored. |

**TABLE 4 Determination of the Vulnerability Category from the Performance Index and Susceptibility Level**

| | Susceptibility levels | | | | | |
|---|---|---|---|---|---|---|
| Value Levels | Zero | Very Low | Low | Moderate | High | Extreme |
| 0.0000–0.0049 | G | G | G | G | G | G |
| 0.0050–0.0299 | G | B | B | B | B | B |
| 0.0300–0.0499 | G | B | B | Y | Y | Y |
| 0.0500–0.0999 | G | B | Y | Y | O | O |
| 0.1000–0.2499 | G | Y | Y | O | O | R |
| >0.2500 | B | Y | O | R | R | R |

of a rigorous quantitative analysis [56], is the price the decision maker pays for not quantifying the probabilities of successful attacks.

The results of the analysis presented above should be subjected to deliberation among the stakeholders to assess their reasonableness and to evaluate the assumptions on which they are based [34]. The deliberation should be supported by extensive sensitivity analyses. The analytical results should not be the sole basis for decision making. As stated earlier, the decision-making process should be risk informed, not risk based.

In [49], it was found that the water treatment plants were the highest ranked vulnerabilities of the water-supply network both with respect to random failures and vandalism. This result was deemed to be reasonable because these plants are the sources of water for the entire infrastructure. In [50], the transmission lines are found to be the highest vulnerabilities due to their openness and remote locations (i.e. their extreme susceptibility to attacks).

### 5.4 Multiple Stakeholders

The evaluation of the PI, which is the central metric for risk ranking, depends on the decision maker in very important ways. The structure of the value tree and the corresponding numerical assignments (relative weights and disutilities) reflect the decision maker's values and preferences. In decision analysis, there are methods for eliciting preferences that aid an individual decision maker in making the necessary judgments [47].

In decisions involving infrastructures, the decision maker may be a private organization that owns the infrastructure or a government agency charged with protecting the national interest. In these cases of "societal" decision making the situation is much more complex.

A practical way of developing a consensus value tree is to consult with a few managers of the decision-making agency and use the analytical results as the basis for sensitivity analyses and deliberation. As an example, such an approach was employed in the evaluation of alternative sites for the disposal of nuclear waste in which the decision-making agency was the Office of Civilian Radioactive Waste Management of the US Department of Energy [57]. Another example involves the management of minor incidents in NPPs [58]. In [49], a small group of engineers developed the consensus value tree that was presumed to represent the water utility's values.

If, for whatever reason, consensus is not achieved, a number of evaluations using different value trees can serve as the basis for deliberation. In [50], five representatives of a regional electric utility were consulted. The group included two senior members of the management division. The stakeholders agreed on the structure of the value tree but differed in the weights they assigned to the PMs. Five rankings of the infrastructure elements were produced using the five different inputs. It turned out that the differences in the element rankings were minimal.

The value of the evaluations that we have discussed is better appreciated when we remember that the results are used to inform the decision-making process. The final decision should not be based on these results. These results and the appropriate sensitivity analyses should be input to a deliberative process that will lead to the final decision. A structured way for using analytical results from risk assessment to inform the deliberation is presented in [35].

### 5.5 Spatial Dependence

As discussed earlier, a useful PRA result, in addition to the ranking of accident sequences, is the ranking of individual events using importance measures. The latter may also be used in infrastructures to determine critical locations, that is, locations which, if attacked successfully, would affect multiple infrastructures. An example using the campus of the Massachusetts Institute of Technology (MIT) is presented in [59].

The concept of RAW, Eq. (11), has been extended to networks in [60]. For multiple Monte Carlo simulations, RAW is defined as

$$\mathrm{RAW}_{ykj} = \frac{U^{+}_{ykj}}{U_{kj}} \tag{14}$$

where $U_{kj}$ is the percent of simulations in which there is no path connecting the user $j$ to an infrastructure $k$ source and $U^{+}_{ykj}$ is the percent of simulations in which element $y$ (node or arc) of infrastructure $k$ *is failed* and there is no path connecting the user $j$ to an infrastructure $k$ source.

The importance measure $RAW_{ykj}$ describes the ratio of risk to user $j$ for infrastructure $k$ when element $y$ is always unavailable to the base-case risk to the user. Reference 59 combines this importance measure with the PI to define the valued worth of element $y$ of infrastructure $k$ as follows:

$$\mathrm{VW}_{yk} \equiv \sum_j \left[ \mathrm{RAW}_{ykj} \cdot \sum_{i=1}^{k_{\mathrm{PM}}} w_i d_{ijk} \right] \tag{15}$$

The valued worths represent the RAW-scaled potential disutility they evoke to all users of their respective infrastructure. The higher the valued worth, the more important the element $y$ of infrastructure $k$ is to the decision makers. It is important to note that these values represent the potential of an element's unavailability to fail the system and cause a certain amount of disutility; the failure of a high valued worth item may or may not lead to the loss of infrastructure service.

Geographic information systems (GIS) are programs that display geospatial information stored in a database in graphical form. They allow us to perform a network analysis and determine the valued worths for the elements of each infrastructure independently, and then, through GIS algorithms, we can find spatially close nodes/arcs, for example, parallel pipes within a certain distance from each other. Doing this "intersection analysis" after the network analysis allows us to easily change the "intersection distance", that is, how close different elements must be to be considered spatially coincident.

First, we develop a generic grid to be laid across the map of all the infrastructures. The side of each grid space (hexagon) is the size of the threat's radius of influence. We use a hexagonal closely packed grid across the entire region of analysis. Then, we use an internal GIS function to take the maximum valued worth of all elements of the same infrastructure that are located within each hexagon. We sum the maximum valued worth elements from each infrastructure for each hexagon and define the geographic valued worth (GVW) as follows:

$$\mathrm{GVW}_{xz} = \sum_k \max\left(\mathrm{VW}_{y_{xz}k}\right) = \sum_k \max\left[ \sum_j \left( \mathrm{RAW}_{y_{xz}kj} \cdot \sum_{i=1}^{k_{\mathrm{PM}}} w_i d_{ijk} \right) \right] \tag{16}$$

where $GVW_{xz}$ is the geographic valued worth of the grid space at coordinates $(x, z)$ and $\max\left(VW_{y_{xz}k}\right)$ is the maximum valued worth element $y$ out of all the elements of infrastructure $k$ that pass through grid element $(x, z)$

An example of the use of the GVW is shown in Figure 4 in which the lightest gray represents the lowest numerical GVW values and solid black the highest. These GVWs are conditional on a threat that destroys everything within a 7-m radius. The GVWs were calculated on a grid of hexagons with the height and width of two times the radius of influence. We observe that there is a high-GVW "loop" that services the users in the figure. There are lines for electric power, steam, water, and natural gas that all run under the same streets very close to each other to service the dorms that are present in this part of the MIT campus.

Conditional risk maps similar to that in Figure 4 are given to the decision maker who must, then, decide whether the susceptibility of the infrastructure elements in the dark areas of the map is such that the area may be declared a critical location. It is important

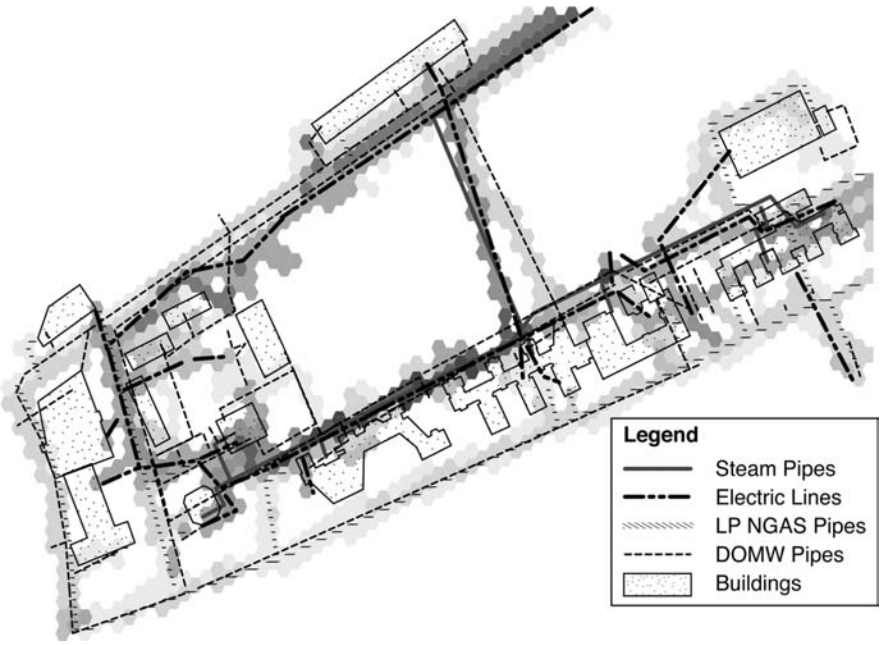



**FIGURE 4** GVW conditional risk map based on GVW for part of the MIT campus (reprinted from [59] with permission from Elsevier).

to note that locations of moderate importance to the networks, individually, may be of high importance if all infrastructures are considered together.

### 5.6 Future Research Directions

The rankings of the infrastructure elements that have been produced using the proposed framework are conditional on the assumption of a "minor" threat, for example, vandalism. For other kinds of threats, multiple elements may be damaged and the methodology needs to be extended to cover these cases.

The element rankings are relative. The absence of the probability of attack inhibits decision making. Just because an infrastructure element is ranked as the most important, it does not necessarily follow that something should be done about it. The absolute value of the infrastructure risk may already be very low therefore not justifying hardening this particular element. In other words, even assuming that society is willing to determine levels of "acceptable" or "tolerable" terrorism risks (a very strong assumption), we do not currently have the analytical tools that allow the quantification of the risk. Yet, resources must be allocated to counterterrorism measures; therefore, the need for developing such tools is high.

## REFERENCES

1. US Nuclear Regulatory Commission. (1990). *Severe Accident Risks: An Assessment for Five US Nuclear Power Plants*, Report NUREG-1150, Washington, DC.

2. National Research Council. (1997). Risk assessment and management at deseret chemical depot and the tooele chemical agent disposal facility. *Committee on Review and Evaluation of the Army Chemical Stockpile Disposal Program*. National Academy Press, Washington, DC.
3. Futron Corporation. (2001). *Probabilistic Risk Assessment of the International Space Station. Phase III–Stage 12A.1 Configuration*, Washington, DC.
4. Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Anal.* **1**, 11–27.
5. *SAPHIRE* is available at: http://saphire.inel.gov. RISKMAN is available at: http://www.absconsulting.com/riskmansoftware/index.html. RiskSpectrum is available at: http://www.relcon.se/.
6. Stamatelatos, M. G., Apostolakis, G., Dezfuli, H., Everline, C., Guarro, S., Moieni, P., Mosleh, M., Paulos, T., and Youngblood, R. (2002). *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, Version 1.1, Office of Safety and Mission Assurance. NASA Headquarters, Washington, DC.
7. Nuclear Regulatory Commission. (1982). *PRA Procedures Guide*, Report NUREG CR-2300, Washington, DC.
8. Swain, A. D., and Guttmann, H. E. (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, Report NUREG/CR-1278. Nuclear Regulatory Commission, Washington, DC.
9. Forester, J., Bley, D., Cooper, S., Lois, E., Siu, N., Kolaczkowski, A., and Wreathall, J. (2004). Expert elicitation approach for performing ATHEANA quantification. *Reliab. Eng. Syst. Saf.* **83**, 207–220.
10. Nuclear Regulatory Commission. (2000). *Technical Basis and Implementation Guidelines for A Technique for Human Event Analysis (ATHEANA)*, Report NUREG-1624, Washington, DC.
11. Moieni, P., and Spurgin, A. J. (2004). Advances in human reliability analysis methodology. *Reliab. Eng. Syst. Saf.* **44**, 27–66.
12. Julius, J., and Grobbelaar, J. (2006). Integrating Human Reliability Analysis Approaches in the EPRI HRA Calculator. *8th Probabilistic Safety Assessment and Management Conference (PSAM 8)*. sponsored by the International Association for Probabilistic Safety Assessment and Management, New Orleans, LA, (http://www.iapsam.org/).
13. Budnitz, R. J., Apostolakis, G., Boore, D. M., Cluff, L. S., Coppersmith, K. J., Cornell, C. A., and Morris, P. A. (1997). *Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts*, Report NUREG/CR-6372, Vols. 1 and 2, Nuclear Regulatory Commission, Washington, DC.
14. Nuclear Regulatory Commission and Electric Power Research Institute. (2005). *Fire PRA Methodology for Nuclear Power Facilities*, Report NUREG/CR-6850 (EPRI 1011989), vols. 1 and 2, Washington, DC/Palo Alto, CA.
15. Helton, J. C., Anderson, D. R., Basabilvazo, G., Jow, H.-N., and Marietta, M. G. (2000). Conceptual structure of the 1996 performance assessment for the waste isolation pilot plant. *Reliab. Eng. Syst. Saf.* **69**, 151–165.
16. Thompson, B. G. J., and Sagar, B. (1993). The development and application of integrated procedures for post-closure assessment, based upon Monte Carlo simulation: The Probabilistic Systems Assessment (PSA) approach. *Reliab. Eng. Syst. Saf.* **42**, 125–160.
17. Ghosh, S. T., and Apostolakis, G. E. (2006). Extracting risk insights from performance assessments for HLW repositories. *Nucl. Technol.* **153**, 70–88.
18. Tversky, A., and Kahneman, D. (1974). Judgments under uncertainty: heuristics and biases. *Science* **185**, 1124–1131.
19. Apostolakis, G. (1990). he concept of probability in safety assessments of technological systems. *Science* **250**, 1359–1364.

20. Winkler, R. L. (1996). Uncertainty in probabilistic risk assessment. *Reliab. Eng. Syst. Saf.* **54**, 127–132.
21. De Finetti, B. (1974). *Theory of Probability*, Vols. 1 and 2. John Wiley & Sons, New York.
22. Savage, L. J. (1972). *The Foundations of Statistics*. Dover Publications, New York.
23. Nuclear Regulatory Commission. (2002). *An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis*, Regulatory Guide 1.174, Revision 1, Washington, DC.
24. Keeney, R. L., and von Winterfeldt, D. (1991). Eliciting probabilities from experts in complex technical problems. *IEEE Trans. Eng. Manag.* **38**, 191–201.
25. Budnitz, R. J., Apostolakis, G., Boore, D. M., Cluff, L. S., Coppersmith, K. J., Cornell, C. A., and Morris, P. A. (1998). Use of technical expert panels: applications to probabilistic seismic hazard analysis. *Risk Anal.* **18**, 463–469.
26. Helton, J. C., Johnson, J. D., Sallaberry, C. J., and Storlie, C. B. (2006). Survey of sampling-based methods for uncertainty and sensitivity analysis. *Reliab. Eng. Syst. Saf.* **91**, 1175–1209.
27. Nuclear Regulatory Commission. (1990). *Severe Accident Risks: An Assessment for Five US Nuclear Power Plants*, Report NUREG-1150, Washington, DC, available at http://www.nrc.gov/.
28. Wilson, R., and Crouch, E. A. C. (2001). *Risk-Benefit Analysis*. Harvard University Press, Cambridge, MA.
29. Nuclear Regulatory Commission. (1986). *Safety Goals for the Operations of Nuclear Power Plants*. Federal Register, vol. 51, p. 30028, August 4.
30. United Kingdom Health and Safety Executive. (2001). *Reducing Risks, Protecting People. HSE's Decision-Making Process* . Her Majesty's Stationery Office, Norwich, available at http://www.hse.gov.uk/risk/theory/r2p2.pdf
31. Cheok, M. C., Parry, G. W., and Sherry, R. R. (1998). Use of importance measures in risk-informed regulatory applications. *Reliab. Eng. Syst. Saf.* **60**, 213–226.
32. Apostolakis, G. E. (2004). How useful is quantitative risk assessment? *Risk Anal.* **24**, 515–520.
33. Sorensen, J. N., Apostolakis, G. E., Kress, T. S., and Powers, D. A. (1999). On the role of defense in depth in risk-informed regulation. *Proceedings of PSA '99, International Topical Meeting on Probabilistic Safety Assessment*, Washington, DC, August 22–26. American Nuclear Society, La Grange Park, IL, pp. 408–413.
34. National Research Council. (1996). *Understanding Risk: Informing Decisions in a Democratic Society*. National Academy Press, Washington, DC.
35. Apostolakis, G. E., and Pickett, S. E. (1998). Deliberation: integrating analytical results into environmental decisions involving multiple stakeholders. *Risk Anal.* **18**, 621–634.
36. National Research Council. (2002). *Making the Nation Safer. The Role of Science and Technology in Countering Terrorism*. National Academy Press, Washington, DC.
37. Bley, D., Kaplan, S., and Johnson, D. (1992). The strengths and limitations of PSA: where we stand. *Reliab. Eng. Syst. Saf.* **38**, 3–26.
38. Bier, V. M. (1999). Challenges to the acceptance of probabilistic risk assessment. *Risk Anal.* **19**, 703–710.
39. Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate, Aldershot, Hampshire, UK.
40. Aldemir, T., Miller, D. W., Stovsky, M. P., Kirschenbaum, J., Bucci, P., Fentiman, A. W., and Mangan, L. T. (2006). *Current State of Reliability Modeling Methodologies for Digital Systems and Their Acceptance Criteria for Nuclear Power Plant Assessments*, Report NUREG/CR-6901, Nuclear Regulatory Commission, Washington, DC.

41. Nuclear Regulatory Commission. *Protecting Our Nation*. Available at www.nrc.gov.
42. Garrick, B. J., Hall, J. E., Kilger, M., McDonald, J., McGroddy, J., O'Toole, T., Probst, P., Rindskopf Parker, E., Rosenthal, R., Trivelpiece, A., Van Arsdale, L., and Zebroski, E. (2004). Confronting the risks of terrorism: making the right decisions. *Reliab. Eng. Syst. Saf.* **86**, 129–176.
43. Haimes, Y. Y. (2002). Roadmap for modeling risks of terrorism to the homeland. *J. Infrastruct. Syst.* **8**, 35–41.
44. Paté-Cornell, M. E., and Guikema, S. (2002). Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. *Mil. Oper. Res.* **7**, 5–20.
45. Bier, V. M., Nagaraj, A., and Abhichandani, V. (2005). Protection of simple series and parallel systems with components of different values. *Reliab. Eng. Syst. Saf.* **87**, 315–323.
46. Lye, K., and Wing, K. M. (2005). Game strategies in network security. *Int. J. Inf. Secur.* **4**, 71–86.
47. Clemen, R. T. (1996). *Making Hard Decisions: An Introduction to Decision Analysis*, 2nd ed. Duxbury Press, Belmont, CA.
48. Apostolakis, G. E., and Lemon, D. M. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Anal.* **25**, 361–376.
49. Michaud, D., and Apostolakis, G. E. (2006). Methodology for ranking the elements of water-supply networks. *J. Infrastruct. Syst.* **12**, 230–242.
50. Koonce, A. M., Apostolakis, G. E., and Cook, B. K. (2008). Bulk power grid risk analysis: ranking infrastructure elements according to their risk significance. *Int. J. Electr. Power Energy Syst*. **30**: 169–183.
51. Richardson, B. (2005). *Sandia Load Flow Simulation Model*. Sandia National Laboratories, Albuquerque, NM.
52. Saaty, T. L. (2000). *Fundamentals of Decision Making and Priority Theory*, Vol. VI. RWS Publications, Pittsburgh, PA.
53. Holder, R. D. (1990). Some comments on the analytic hierarchy process. *J. Oper. Res. Soc.* **41**, 1073–1076.
54. Forman, E. H. (1996). Facts and fictions about the analytic hierarchy process. In *The Analytic Hierarchy Process*, T. L. Saaty, Ed. RWS Publications, Pittsburgh, PA.
55. Stamatelatos, M., Dezfuli, H., and Apostolakis, G. (2006). A proposed risk-informed decision-making framework for NASA. Presented at the *8th International Conference on Probabilistic Safety Assessment and Management (PSAM 8)*. New Orleans, LA, 15–18 May. (www.iapsam.org).
56. Cox, L. A., Jr., Babayev, D., and Huber, W. (2005). Some limitations of qualitative risk rating systems. *Risk Anal.* **25**, 651–662.
57. Merkhofer, M. W., and Keeney, R. L. (1987). A multiattribute utility analysis of alternative sites for the disposal of nuclear waste. *Risk Anal.* **7**, 173–194.
58. Pagani, L., Smith, C., and Apostolakis, G. (2004). Making decisions for incident management in nuclear power plants using probabilistic safety assessment. *Risk Decis. Policy* **9**, 271–295.
59. Patterson, S. A., and Apostolakis, G. E. (2007). Identification of critical locations across multiple infrastructures for terrorist actions. *Reliab. Eng. Syst. Saf.* **92**: 1183–1203.
60. Zio, E., Podofillini, L., and Zille, V. (2006). A combination of Monte Carlo simulation and cellular automata for computing the availability of complex network systems. *Reliab. Eng. Syst. Saf.* **91**, 181–190.

# SCENARIO ANALYSIS, COGNITIVE MAPS, AND CONCEPT MAPS

KENNETH G. CROWTHER AND YACOV HAIMES
*Center for Risk Management of Engineering Systems, Department of Systems and Information Engineering, University of Virginia, Charlottesville, Virginia*

## 1 INTRODUCTION

In her book *Pearl Harbor: Warning and Decision* [1962] recently cited by the 9/11 Commission Report [1], Roberta Wohlstetter made the following comment [2]:

> It is much easier after the event to sort the relevant from the irrelevant signals. After the event, of course, a signal is always crystal clear; we can now see what disaster it was signaling since the disaster has occurred. But before the event it is obscure and pregnant with conflicting meetings.

Those same words, which describe the Japanese attack on Pearl Harbor in 1941, could be used 60 years later to describe many modern disasters. Nassim Taleb [3], in his highly provocative essay *The Black Swan: The Impact of the Highly Improbable*, confirms Roberta Wohlstetter's insight with one additional caveat—the hindsight understanding produced by assessing signals *after* an event is usually not general enough to yield insight, missing causal understanding, and often lacks meaningful impact on decisions. "Clear" hindsight without inventive foresight is insufficient to cope with risks of improbable and elusive events to the homeland. Moreover, it is the improbable, elusive events that result in the greatest impact (e.g. unimagined terrorist attacks with passenger planes in New York; implausible combinations of hurricane, infrastructure, and social demographics in New Orleans; unlikely underwater earthquakes and resulting tsunami in southeastern Asia; etc.).

By their definition, disasters constitute extreme and catastrophic events; thus, their probabilities and associated consequences defy any common expected value representation of risk. Many analysts and decision theorists are beginning to recognize a simple yet fundamental philosophical truth—in the face of such unforeseen or elusive calamities as bridges falling, dams bursting, airplanes crashing, tsunamis washing, and hurricanes landing with great force, we must acknowledge the importance of studying "extreme" events [4, 5].

## 2 OVERVIEW—SCENARIO ANALYSIS

Lowrance [6] described *risk* as "a measure of the *probability* and *severity* of *adverse effects*". Kaplan and Garrick [7] were the first to formalize a theory of quantitative risk assessment with the triplet:

What can go wrong?
What is the likelihood?
What are the consequences?

Risk assessments that answer the above triplet questions hinge on the ability to identify risk scenarios and organize them according to some understanding of their approximated consequences and perceived frequency. To begin such a risk assessment process, the analyst must clearly define the as-planned or success scenario [8]. The risk scenarios or *what-can-go-wrong* events are then defined as any deviation from the as-planned scenario. Kaplan et al. [9] present a Theory of Scenario Structuring (TSS) based on a systemic set of methods to decompose a system with respect to time, operation, process components, or other means to create a complete set of risk scenarios as a foundation of analysis. TSS is a generalized method into which most common risk assessment methods can be described, including [10]: (i) failure modes and effects analysis (FMEA), which divides a system into functional parts and derives risk scenarios from the failures of functional components (e.g. MIL-STD-1629A; Benbow et al. [11]), (ii) hazard and operations analysis (HAZOP), which divides a plant into physical sections and assesses the impacts of risk scenarios that result from various extreme operational conditions (e.g. Kletz [12]), (iii) event trees (ET), which seeks to assess cascades of errors or risk scenarios through time that derive from an initiating event (e.g. Smith [13]), (iv) fault trees (FT), which seeks the causes of predefined, undesirable end states or risk scenarios (e.g. Hoyland and Rausand [14] and US Nuclear Regulatory Commission [15]), (5) anticipatory failure determination (AFD), which assesses what an operator or agent can make go wrong to cause a risk scenario to occur [9], and (vi) hierarchical holographic modeling (HHM), which decomposes a system into hierarchal overlapping categories of operation and function on the basis of fundamental system structure and develops risk scenarios relevant to each overlapping category [5, 16, 17]. All of these methods are a form of scenario analysis—prescribing a systematic way of analyzing a system under a systemic set of conditions. The following subsections will focus on AFD and HHM as example resources in scenario analysis. Many of the other methodologies are supported by these methods and are described in other articles of this book.

### 2.1 Scenario Analysis—Anticipatory Failure Determination (AFD)

The TRIZ method, whose acronym in Russian stands for "Theory of Inventive Problem Solving", is a scenario structuring method developed to assist in stimulating the creation of new inventions and finding new solutions for real world problems [18]. An off-shoot tool of TRIZ is AFD method, which is used for failure analysis. Unlike traditional failure analysis methods, such as FMEA, which look for a cause of failure, AFD views failure as an intended consequence [19]. Analysts then try to devise ways of ensuring that failures always happen, thereby generating a list of causes. AFD asks the question "If I wanted to create a particular failure, how can I do it in the most effective way?" [10]. AFD provides a structure to the use of "red teaming" to identify weaknesses, which seems well documented [20–22].

### 2.2 Scenario Analysis—Hierarchical Holographic Modeling (HHM)

Real large-scale systems are complex in nature. Many large-scale systems exhibit characteristics, daunting to modelers, such as a large number of subsystems, a hierarchical

structure, multiple decision makers, and elements of risk and uncertainty. It may be impractical to use a single-model analysis to describe such large-scale systems, particularly in the context of identifying potential threat scenarios and other sources of risk. HHM [5, 16] is a holistic philosophy and methodology which captures and represents the essence of the inherent diverse characteristics and attributes of a system—its multiple aspects, perspectives, facets, views, dimensions, and hierarchies—and is suitable for describing complex, large-scale systems. Specifically, HHM has the capability of presenting risk scenarios from multiple overlapping perspectives, consistent with the overlapping view of the system [10].

The term *holographic* refers to the multiple perspectives with which a system can be described (as opposed to a single view or a flat planar image). The term *hierarchical* in HHM refers to describing the myriad levels of a system hierarchy—structurally or organizationally. Because it examines the system from multiple perspectives and decomposes those perspectives hierarchically into subsystems, HHM is a valuable tool for identifying the myriad sources of risks to a system. Sources of risk can be categorized by a number of perspectives, or HHM head-topics, such as hardware, software, organizational, temporal, and geographical. Sources of risk can manifest themselves at macroscopic and microscopic levels of a system or at various management levels of an organization, each described by HHM subtopics and further.

Recent applications of HHM in identifying sources of risk include defining types of hardening to reduce vulnerabilities in water systems partially shown in Figure 1 [17], enumerating the sources of risk in large-scale software acquisition [23], identifying risk scenarios as a tool in the TSS framework [10], identifying risks to information assurance [24], capturing risk scenarios for military operations other than war [25], cataloging risk issues encountered in space missions [5], and identification of possible transportation system disruptions [26].

### 2.3 Scenario Analysis—Collaborative Adaptive Multiplayer HHM (CAM-HHM)

If determining what can go wrong is the thesis (e.g. through HHM) and determining how can we make the system fail is the antithesis (e.g. through AFD), then their synthesis combines the efficacy of both for holistic analysis of risk scenarios. A recent extension of HHM, the collaborative adaptive multiplayer hierarchical holographic modeling (CAM-HHM), better establishes the collection of data from multiple perspectives and sources. Haimes and Horowitz [27] introduced the concept as the adaptive two-player HHM game, which allowed two teams (e.g. Red and Blue) with very different perspectives to generate risk scenarios for the purpose of intelligence collection and analysis. Developing two independent structures of risk scenarios provides (i) a more holistic view of the system created when the two models are aggregated, (ii) valuable benchmark information on the depth and breadth of the assessment, and (iii) greater self-understanding and knowledge of the opponent [27]. HHMs are created by each team and combined in an iterative process until convergence on a final, systemic HHM is generated.

The technique was designed to encourage collaboration among several experts from disparate backgrounds for identifying sources of risk to the system. The fundamental difference between the red team and blue team is their knowledge base, perspective, and experience. The Red Team approaches the problem from a terrorist perspective: What kind of threats can I create from publicly available or stolen intelligence data that will defeat the system? The Blue Team approaches the problem from a defensive perspective:

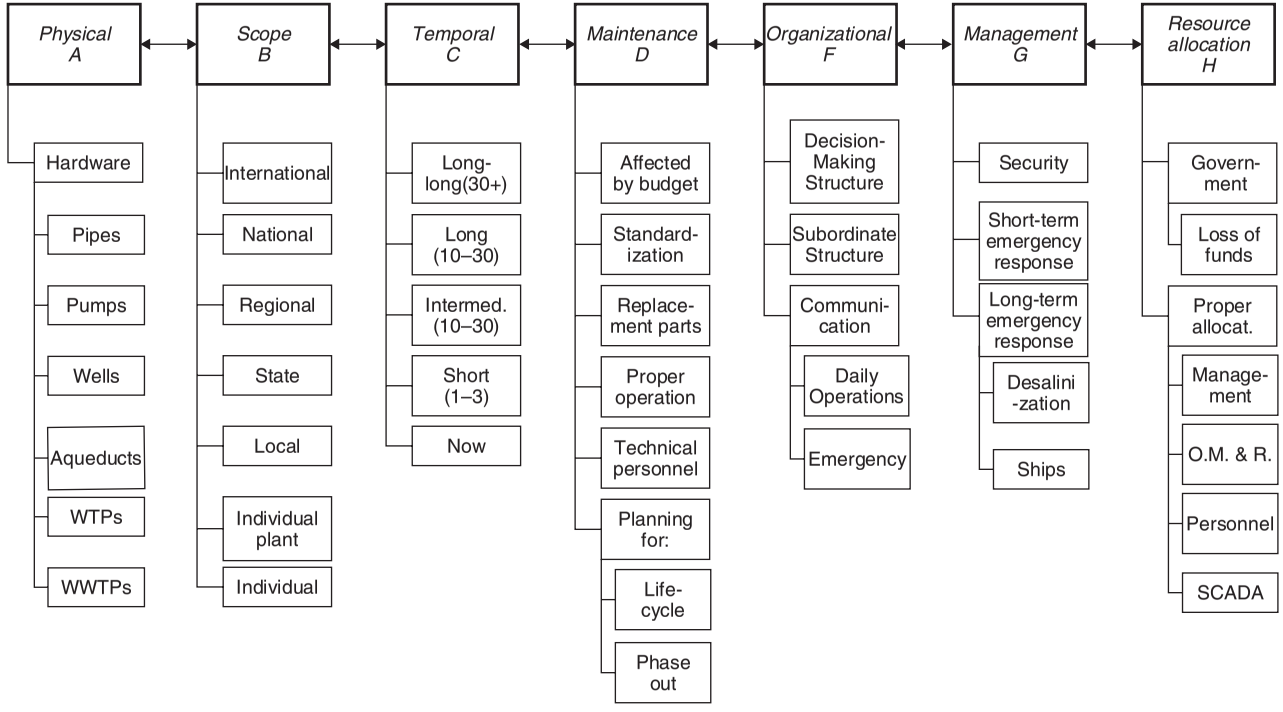



**FIGURE 1** Partial HHM structuring multiple perspectives on the hardening of the water-supply system [4, p. 121].

Using our internal or classified information, what weaknesses or vulnerabilities are present? [27] Collaboration across teams provides a more holistic collection of data from many perspectives and multiple hierarchical levels.

The two-player concept was extended to account for multiple Red Team and Blue team perspectives with the CAM-HHM. One of the first deployments of the CAM-HHM tool was in capturing a board perspective on risk in oil and gas infrastructures due to cyber threats for the Institute for Information Infrastructure Protection (I3P) [28]. In that example, sources of risk to supervisory control and data acquisition (SCADA) systems were gathered from four perspectives: attackers and hackers (representing Red Team interests), SCADA owners and operators (representing Blue Team interests), SCADA vendors, and stakeholders. In four parallel 40-min sessions, they created a taxonomy of 148 classes of industrial cyber risks [26].

A more recent deployment of the CAM-HHM tool dealt with identifying sources of risk to the 2006 Virginia gubernatorial inauguration [29]. Three teams were involved in the CAM-HHM game: officials from the transportation sector, officials with health care experience and others from the private sector, and members with experience in creating security plans (representing Red Team interests). The CAM-HHM game collaboratively produced 272 sources of risk of interest to security officials in planning for the inauguration. The results of the CAM-HHM fit into a larger scenario analysis framework, where risk scenarios are identified, qualitatively and quantitatively assessed, and risk management plans are developed to reduce or eliminate the sources of risk.

### 2.4 Scenario Analysis—Risk Filtering, Ranking, and Management (RFRM)

The objective of risk scenario structuring is to generate a comprehensive set of perspectives with which to view a system and its numerous sources of risks, potentially producing an unmanageable number of risk scenarios. Often, it is impractical to perform scenario analysis on hundreds of sources of risk. There is a need to discriminate among them in a systematic fashion according to the likelihood and severity of occurrence. To serve this purpose, the risk filtering, ranking, and management (RFRM) method was developed [5, 30].

The RFRM methodology systematically evaluates a comprehensive set of risk scenarios and then differentiates them according to the likelihood and severity of their consequences. The methodology effectively considers a variety of risk scenarios and integrates empirical and conceptual, descriptive and normative, as well as quantitative and qualitative methods and approaches to complete the scenario analysis process. The RFRM process is aimed at providing priorities in analyzing assets in the decision makers' domain of interest. This means exploring the more urgent sources of risks or scenarios first; it does not imply ignoring the sources of risks that have been filtered out earlier.

The RFRM process is systematically carried out in eight phases, as described below.

*Phase I: scenario identification.* An HHM is developed to describe the system in a comprehensive way, including all relevant risk scenarios.

*Phase II: scenario filtering.* The risk scenarios enumerated in the HHM produced in Phase I are filtered according to the interests and scope of the analysis.

*Phase III: bicriteria filtering and ranking.* The set of risk scenarios is further filtered with qualitative relative likelihoods and consequences.

*Phase IV: multicriteria evaluation.* The abilities of the remaining risk scenarios to defeat the defenses of the system are evaluated with a set of 11 criteria, including duration of effects, cascading effects, and complexity and emergent behaviors.

*Phase V: quantitative ranking.* Filtering and ranking of scenarios continues with a quantitative and qualitative matrix of likelihoods and consequences.

*Phase VI: risk management.* Risk management options are identified to deal with the sources of risks. Included are issues of costs and benefits in risk reduction.

*Phase VII: safeguarding against missing critical items.* The performance of the risk management options selected in Phase VI is evaluated against the scenarios previously filtered out during Phases II through V.

*Phase VIII: operational feedback.* The scenario filtering and decision processes of previous phases are refined using the experience gained in applying the risk management options.

The RFRM framework has been applied in several risk and scenario filtering contexts, including focusing limited resources on the most risky and uncertain sources of risk to military operations other than war [25], filtering over 900 sources of risk to US Army telecommunications systems information assurance [24], prioritizing the protection of transportation assets against terrorist attacks [31], and identifying and prioritizing risks to US Army critical assets relative to organizational goals [32]. In the 2006 VA Gubernatorial inauguration exercise, the original 272 HHM topics identified were prioritized into 77 scenarios based on their likelihoods and severity assessments. The prioritized set of risk scenarios then become the focus of resource allocation and other risk management actions and more detailed quantitative modeling.

### 2.5 Scenario Analysis—Risk Management

Haimes [4, 5] presents a second set of triplet questions that outline the fundamental tasks of risk management (see Phase IV of RFRM):

What can be done and what options are available?

What are the trade-offs in terms of costs, benefits, and risks?

What are the impacts of current decisions on future options?

Answers to these questions critically enhance the capacity to make appropriate decisions about acceptable levels of risk. Haimes [5] provides an extensive discussion of quantitative risk assessment and management. No single model can capture all the dimensions necessary to adequately evaluate the efficacy of risk assessments and management activities because of the impossible task of identifying all relevant state variables and their substates for adequately representing large and multiscale systems [5, 16, 33].

Scenario analysis legitimizes the exploration and experimentation of out-of-the-box and seemingly "crazy" ideas and ultimately discovers insightful implications that otherwise would have been completely missed and dismissed [26]. To illustrate, consider a hypothetical coastal region that clearly lies in a flood zone. Now consider several dimensions of the system that might be juxtaposed to result in adverse regional consequences, including rare hazards such as hurricanes, uncertain forecasts of the hurricanes, and demographic tension (such as racial). A scenario analysis focusing on a rare hurricane

that could potentially destroy a coastal region would cost millions, and might justify the appointment of an individual who constantly communicates with the national weather services. However, the uncertainty might result in a last minute capability to evacuate the region. Such uncertainty in the forecast would justify the utilization of an otherwise unused assets, such as school buses to aid in the evacuation from the coastal region. However, a focus in the scenario analysis that focus on demographic tensions might result in the justification of contracting charter buses through a prehurricane memorandum of understanding for last minute evacuation at a known cost. The output of the scenario structuring methods is a taxonomy of identified risk scenarios that are constructed from the multiple perspectives of a system for modeling (e.g. hazard, infrastructure, information, and demographics). Moreover, the output of the scenario analysis process is a justification or rationalization of mitigation against the improbable event, and investment in preparedness or learning activities to protect against critical forced changes or emergent risks—investment that might not otherwise have been approved. Through logically organized and systemically executed analyses, scenario analysis provides a reasoned experimental modeling framework with which to explore and thus understand the intricate relationships that characterize the nature of multiscale infrastructure and organizational systems. This philosophy rejects dogmatic problem solving that relies on a single modeling approach structured on one school of thinking. Rather, its modeling schema builds on the multiple perspectives gained through generating multiple scenarios. This leads to the construction of appropriate models to deduce tipping points as well as meaningful information for logical conclusions and future actions. Currently, models assess what is optimal, given what we know, or what we think we know. Scenario analysis extends this mind-set framework to answer other questions, such as (i) What do we need to know? (ii) What value might appear from risk reduction results having more precise and updated knowledge about complex systems, and (iii) Where is that knowledge needed for acceptable risk management and decision making?

Masterpieces are not usually created on the first painting, but are usually created by selecting themes and exploring those themes to develop knowledge and understanding the final product of which can then be carefully designed based upon what is learned through experience. Scenario analysis is a modeling paradigm that is congruent with and responsive to the uncertain and ever-evolving world of emergent systems. In this sense, it serves as an adaptive process, a learn-as-you-go modeling laboratory, where different scenarios (e.g. generated through the CAM-HHM, introduced in a previous section) of needs and developments for emergent systems can be explored and tested. In other words, to represent and understand the uncertain and imaginary evolution of a future emergent system, we need to deploy an appropriate modeling technology that is equally agile and adaptive.

FEMA's HAZUS-MH for hurricanes [34] is an example of the type of tool that has emerged to support scenario analysis. The tool construction has resulted from the integration of databases, models, and simulation tools that have been developed across many disciplines over the last several decades., As an integrated tool it can be used to study the impact of various hurricane scenarios on regions and their system states. At the basic modeling level there are databases of buildings, businesses, essential facilities, and other basic structural and regional knowledge that characterize the various system dimensions of the region under study. These databases are editable to enable explorations of agile properties of structures that may change the impact of hurricanes. Scientific models from decades of structural research estimate probabilistic structural damage from wind gusts to various structural vulnerabilities. Finally, there is a hazard model to estimate

peak wind gust given historical or user-defined catastrophes. The integration of databases, causal damage models, and flexible hazard simulations results in a tool that enables regions to fully explore ranges of improbable situations.

## 3 SCENARIO ANALYSIS, COGNITIVE MAPS, AND CONCEPT MAPS

Scenario analysis is a methodological process for developing such analyses that will have the flexibility to capture emergent behavior of both regional vulnerabilities and the threats. Moreover, these solutions to a scenario process result in a method to trace changes in problem definitions, critical variables, critical metrics, available data, and so on, in a way that enables us to measure learning, changing, and improvement in risk management activities over time. However, effective scenario analyses rely on the capability to ascertain the decision processes of a region, namely what assumptions are needed to make decisions, how decision makers connect information and map it to decisions, and how do groups of decision makers, which govern a region, assimilate new information to adapt their decision-making processes. Cognitive maps support our ability to understand how decision makers map understanding of the world. Concept maps have general use. In this article, we describe how concept maps can be used to represent and capture the cognitive maps in order to customize the filtering of the scenario analysis.

## 4 OVERVIEW—COGNITIVE MAPS

*Cognitive maps* is supplement and complement scenario analyses. Kitchin [35] synthesizes the use of the term *cognitive maps* through several decades of literature. Tolman [36] is credited as the earliest to use the term. Tolman [36] created the term to articulate his opposition to a commonly held viewpoint that rats learn through physiological changes, and proposed instead that rats form mental or psychological notions of their environment (i.e. cognitive maps) that evolve and adapt as they gain experience. Kitchin [35] describes how multiple uses of the terminology have developed over time to have explicit, analogical, metaphorical, and hypothetical meanings. For example, Lieblich and Arbib [37], describe parts of the brain that actually store topologies of the environment (i.e. explicit definition), whereas Downs [38] describes how our actions are consistent with a model of environmental processes *as if* we stored a mental map (i.e. metaphorical definition). Despite all these meanings, every person forms models of their environment through acquisition, storage, analysis, and synthesis of perceived environmental information. Developing cognitive maps are useful tools for analysis of factors that influence decision processes.

Axelrod [39] was the earliest to develop cognitive maps as a means of explaining phenomena that are caused by cognition and decisions. Walsh [40] provides an extensive review and organization of approximately 400 books and peer reviewed journal articles to describe how cognitive maps have been developed from multiple fields of psychology and management. Weick [41] describes cognitive mappings as a well-established technique for capturing the thinking of decision makers about situations, problems, and adverse events.

There are several approaches that have been used to elicit and depict cognitive maps. They are typically customized to the background of the individual researcher and the topic. See Walsh [40] for several examples. This article will focus on the utilization of concept maps to guide the elicitation and representation of cognitive maps.

## 5 OVERVIEW—CONCEPT MAPS

Concept maps are graphical tools to organize and represent knowledge. They are constructed from a focus question (i.e. a decision) and are constructed by identifying concepts and concept relationships that are believed to result in a capability to answer the focus question. Triplets of concepts and their relationships are propositions or semantic units of understanding. Data can be acquired to provide evidence concerning a concept or semantic unit on the map. Such evidence over time will result in a learning process that connects actions and occurrences to answers and questions. If the concept map represents the group cognitive map of a process, then the concept map is able to channel the occurrences to update the set of decisions that results from the scenario analyses. Novak and Musonda [41] describe that concept maps were developed in 1972 from a study of the growth of children's knowledge of science.

## 6 EXAMPLE APPLICATION OF CONCEPT MAPS TO CYBER SECURITY

To illustrate how one might capture cognitive maps through concept maps consider the following cyber security example. A team of executives, information technology managers, and security managers meet together and perform a scenario analysis that results in a demonstration that high leverage, low cost solutions (e.g. antivirus, intrusion detection, and patch management) are highly desired. Moreover, the scenario analysis identifies potential justification of encryption and key management technologies depending on the actual likelihood that intellectual property will be stolen. In order to provide a solution that implements a learning strategy in addition to high leverage, low cost security, the decision team constructs a concept map that captures the major assumptions and data needs that might be required to make a final justification decision for encryption and key management.

Figure 2 shows the focus question on the left, namely whether a certain portion of the IT budget should be invested in encryption and key management or in other portions of the IT budget that improve productivity. Across the team the decision depends on four general categories of knowledge that include the character of the risk of cyber theft, the effectiveness of encryption to mitigate the threat, the nominal market share of the corporation, and the effectiveness of other IT investment options in increasing productivity. All of these general categories are then further characterized with more specific concepts that define the categories. For example, the risk of cyber theft is defined by the probability that the particular theft might occur and the consequences if the theft is successful. The consequence of theft is the reduction in nominal market share of the company. Other relationships among the concepts can be defined as shown in Figure 2.

This concept map will not hold for all teams or all companies that face similar decisions, but rather represents the method of cognition of the individual team that creates it. The result is a set of concepts that represent the data requirement for making a decision concerning an investment related to a tipping point identified by the scenario analysis. If the HHM methodology (described in a previous section) is adapted for the scenario structure component of the scenario analysis, then the subcategories of the system will become a pool of concepts that can be utilized in the construction of concept maps.

This process applies broadly to homeland security and counterterrorism, where systems are large and complex and where the threats against the system are emergent and largely not well defined.

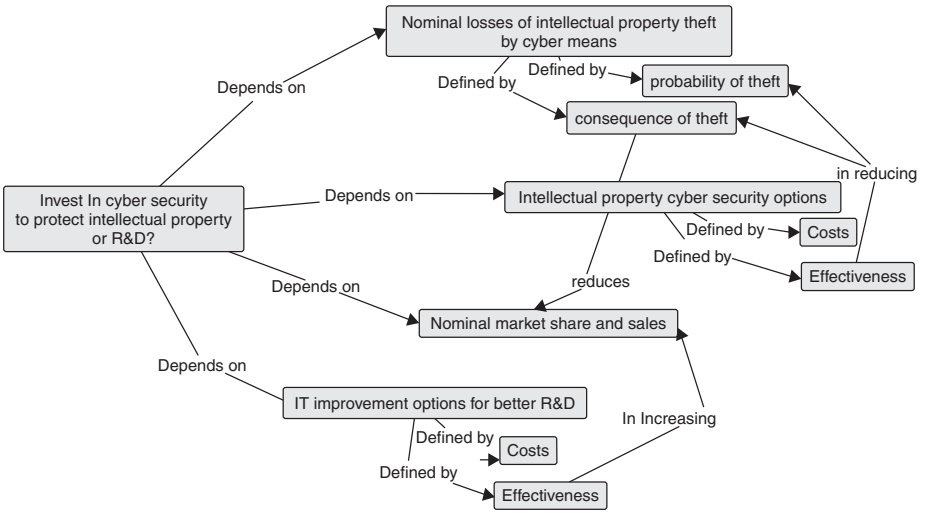



**FIGURE 2** Concept map for a cyber security investment question.

## REFERENCES


1. 9/11 Commission (2004). *The 9/11 Commission Report: Final Report of the national Commission on Terrorist Attacks upon the United States*, W.W. Norton and Company, New York.
2. Wohlstetter, R. (1962). *Pearl Harbor: Warning and Decision*, Stanford University Press, Stanford, CA.
3. Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*, Random House, New York.
4. Haimes, Y. Y. (1991). Total risk management. *J. Risk Anal.* **11**(2), 169–171.
5. Haimes, Y. Y. (2004). *Risk Modeling, Assessment, and Management*, 2nd ed., Wiley, Hoboken, NJ.
6. Lowrance, W. W. (1976). *Of Acceptable Risk: Science and the Determination of Safety*, William Kaufmann, Inc., Los Altos, CA.
7. Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Anal.* **1**(1), 11–27.
8. Kaplan, S. (1991). The general theory of quantitative risk assessment. In *Risk Based Decision Making in Water Resources V*, Y. Y. Haimes, D. A. Moser, and E. Z. Stakhiv, Eds. American Society of Civil Engineers, New York, pp. 11–39.
9. Kaplan, S., Haimes, Y. Y., and Garrick, B. J. (2001). Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk. *Risk Anal.* **21**(5), 807–819.
10. Benbow, D. W., Berger, R. W., Elshennaway, A. K., and Walker, H. F. (2002). *The Certified Quality Engineer Handbook*, ASQ Quality Press, Milwaukee, WI.
11. Kletz, T. A. (1999). *Hazop and Hazan*, 4th ed., CRC Press, Boca Raton, FL.
12. Smith, D. J. (2005). *Reliability, Maintainability, and Risk: Practical Methods for Engineers including Reliability Centered Maintenance and Safety-Related Systems*, 7th ed., Elsevier, New York.
13. Hoyland, A., and Rausand, M. (1994). *System Reliability Theory, Models, and Statistical Methods*, Wiley, New York.

14. US Nuclear Regulatory Commission (1981). *Fault Tree Handbook*, NUREG-81/0492, U.S. Nuclear Regulatory Commission, Washington, DC.

15. Haimes, Y. Y. (1981). Hierarchical holographic modeling. *IEEE Trans. Syst. Man Cybern.* **11**(9), 606–617.

16. Haimes, Y. Y., Matalas, N. C., Lambert, J. H., Jackson, B. A., and Fellows, J. F. R. (1998). Reducing the vulnerability of water supply systems to attack. *J. Infrastruct. Syst.* **4**(4), 164–177.

17. Kaplan, S. (1996). *An Introduction to TRIZ: The Russian Theory of Inventive Problem Solving*, Ideation International, Inc., Southfield, MI.

18. Clarke, D. W. Sr. (2000). Inventive troubleshooting. *Mach. Des.* **15**, 78–80.

19. Metz, S., and Johnson, D. V. II (2001). *Asymmetry and U.S. Military Strategy: Definition, Background and Strategic Concepts*, http://www.au.af.mil/au/awc/awcgate/ssi/asymetry.pdf. Accessed April 25, 2007.

20. Schneider, W. J., Gold, T., and Hermann, B. (2003). *The Role and Status of DoD Red Teaming Activities*, Defense Science Board, Washington, DC.

21. Bier, V. M., Nagaraj, A., and Abhichandani, V. (2005). Protection of simple series and parallel systems with components of different values. *Reliab. Eng. Syst. Saf.* **87**(3), 315–323.

22. Lambert, J. H., Haimes, Y. Y., Li, D., Schooff, R. M., and Tulsiani, V. (2001). Identification, ranking, and management of risks in a major system acquisition. *Reliab. Eng. Syst. Saf.* **72**(3), 315–325.

23. Haimes, Y. Y., Longstaff, T. A., and Lamm, G. A. (2002b). Balancing promise and risk with information assurance in Joint Vision 2020. *Mil. Oper. Res.* **7**(3), 31–46.

24. Dombroski, M., Haimes, Y. Y., Lambert, J. H., Schlussel, K., and Sulcoski, M. (2002). Risk-based methodology for support of operations other than war. *Mil. Oper. Res.* **7**(1), 19–38.

25. Haimes, Y. Y. (2007). Phantom system models for emergent multiscale systems. *J. Infrastruct. Syst.* **13**(2), 81–87.

26. Haimes, Y. Y., and Horowitz, B. M. (2004). Adaptive two-player hierarchical holographic modeling game for counterterrorism intelligence analysis. *J. Homeland Secur. Emerg. Manage.*, **1**(3), 302.

27. Haimes, Y. Y., Santos, J. R., Crowther, K. G., and Henry, M. H. Lian, C., and Yan, Z. (2007). Analysis of Interdependencies and Risk in Oil and Gas Infrastructure Systems, *Institute for Information Infrastructure Protection Research Report No. 11, June 2007*. Published online http://www.thei3p.org/docs/publications/researchreport11.pdf.

28. Agrawal, A. B. (2006). Integrated Risk Assessment and Management for the 2006 Virginia Gubernatorial Inauguration. *MS Thesis, University of Virginia, Charlottesville, VA*.

29. Haimes, Y. Y., Kaplan, S., and Lambert, J. H. (2002a). Risk filtering, ranking, and management framework using hierarchical holographic modeling. *Risk Anal.* **22**(2), 381–395.

30. Leung, M., Lambert, J. H., and Mosenthal, A. (2004). A risk-based approach to setting priorities in protecting bridges against terrorist attacks. *Risk Anal.* **24**(4), 963–984.

31. Anderson, C. W., Barker, K., and Haimes, Y. Y. (2008). Assessing and prioritizing critical assets for the United States Army with a modified RFRM methodology. *J. Homeland Secur. Emerg. Manage.* **5**(1), 5.

32. Haimes, Y. Y. (1977). *Hierarchical Analyses of Water Resources Systems: Modeling and Optimization of Large-Scale Systems*, McGraw-Hill, New York.

33. Federal Emergency Management Agency. (2003). *Multi-Hazard Loss Estimation Methodology Hurricane Model: HAZUS-MH Technical Manual*, Department of Homeland Security, Emergency Preparedness and Response Directorate, Federal Emergency Management Agency, Mitigation Division, Washington, DC.

34. Kitchin, R. M. (1994). Cognitive maps: what are they and why study them? *J. Environ. Psychol.* **12**(1), 1–19.
35. Tolman, E. C. (1948). Cognitive maps in rats and men. *Psychol. Rev.* **55**(4), 189–208.
36. Lieblich, I., and Arbib, M. A. (1982). Multiple representations of space underlying behaviour and associated commentaries. *Behav. Brain Sci.* **5**(4), 627–660.
37. Downs, R. M. (1976). Cognitive mapping and information processing: a commentary. In G. T. Moore, and R. G. Golledge, Eds. *Environmental Knowing*, Dowden, Hutchingson, and Ross, Stroudsburg, PA, pp. 67–70.
38. Axelrod, R. (1976). *Structure of Decision*, University of Princeton Press, Princeton, NJ.
39. Walsh, J. P. (1995). Managerial and organizational cognition: Notes from a trip down memory lane. *Organ. Sci.* **6**(3), 280–321.
40. Weick, K. E. (1995). *Sensemaking in Organizations*, Sage, Thousand Oaks, CA.
41. Novak, J. D., and Musonda, D. (1991). A twelve-year longitudinal study of science concept learning. *Am. Educ. Res. J.* **28**(1), 117–153.

# TIME-DOMAIN PROBABILISTIC RISK ASSESSMENT METHOD FOR INTERDEPENDENT INFRASTRUCTURE FAILURE AND RECOVERY MODELING

GEORGE H. BAKER
*James Madison University, Harrisonburg, Virginia*
CHARLES T. C. MO
*Northrop-Grumman IT, Los Angeles, California*

## 1 INTRODUCTION

The report of the President's Commission on Critical Infrastructures [1, 2] concluded that the nation's physical and economic security depend on critical energy, communications, and computer infrastructures. The Department of Homeland Security has issued national strategy documents for the protection of physical and cyber infrastructures that call for vulnerability assessments of critical infrastructure systems [3, 4]. Even in a world free of malicious activities, such assessments are exceedingly useful to help predict and hopefully prevent outages and costs resulting from natural disasters and normal accidents. Critical infrastructure networks and facilities are subject to many different failure modes. It is

important to anticipate these modes, the likelihood of their occurrence, and the relative seriousness of their consequences.

Failures may be due to many causes, intentional and nonintentional, including aging, accidents, and sabotage from insiders or external malefactors. Failures can propagate such that seemingly minor problems may lead to complete functional failure. Of particular concern is the presence of "single-point failure" locations in many known facilities and systems. A question of concern is which failure points or point combinations would lead to the most serious and "most to-be-avoided" consequences. Some serious failure modes may be counterintuitive. Assessments provide an important basis for determining the most serious failure modes, implementing cost-effective countermeasures, and planning for reconstitution [5].

It is worth noting that modeling infrastructure system interdependencies emerged at the top of National Science Foundation's research objectives at their 2006 Workshop on Resilient and Sustainable Infrastructures [6].

## 2 THE TIME-DOMAIN PROBABILISTIC RISK ASSESSMENT METHOD OVERVIEW

Most critical infrastructure modeling capabilities address the initial failure of critical systems. A major recent push has been developing the capability to model cascading failure of interdependent, interconnected infrastructures [1]. An important capability of interest that has not received wide attention, but is important for understanding and improving infrastructure resiliency is the ability to model the postfailure, recovery phase of infrastructure debilitation.

Infrastructure systems are functionally complex and their system-wide failure probabilities, modes, and consequences are often not obvious. A useful technique for assessing the infrastructure failure modes and their respective likelihoods has been probabilistic risk assessment (PRA) [7]. The technique admittedly does not enable study of detailed system operation that physics-based or agent-based system simulation tools offer. On the other hand, the method requires fewer input parameters and has a faster-turnaround making it a good choice for scoping or screening studies.

To analyze and quantify survivability, conventional PRA methods provide a snapshot of potential failure modes at a single point in time for certain initiating conditions. We have developed a method that extends PRA into the time domain. The method computes the evolution of overall system functionality in time by evaluating initial failure probabilities, effects onset times, and system repair/reconstitution times for single or combinations of critical systems. Using this technique, we can determine which types of failures have the highest probability of putting a critical system off-line for the longest period of time or for a time window of interest. The output thus measures the "resilience" of a system, or system of systems. Results are useful for decision-makers to determine where scarce resources may be invested for replacement parts, service personnel, and so on, to lessen risks and improve system resiliency. The technique provides information useful in weighing the advantages of buying protection to reduce initial failure probabilities (often a costly proposition) or accepting high initial failure probabilities and relying on emergency response contingencies.

The time-domain PRA technique enables a comparative evaluation of potential functional debilitation mode consequences, using realistically available system information

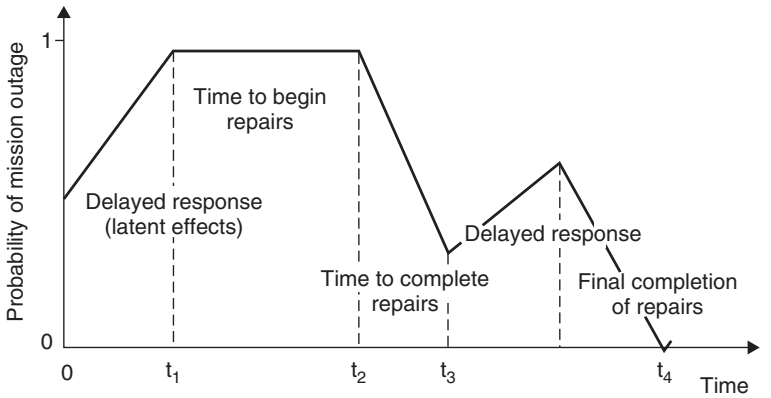



**FIGURE 1** Notional output of the time-domain probabilistic risk assessment (PRA) technique. Standard PRA techniques would provide the probability of effect value at $t = 0$.

augmented by reasonable engineering assumptions. The technique is designed to quantify the probability of mission outage ($P_e$) and outage longevity. The formulation provides output to the user in a simple plot of $P_e$ versus time. A notional output plot is shown in Figure 1.

The tool starts with the building blocks of traditional PRA. Mission outage modeling is accomplished by building a fault diagram. This construct includes a tree structure plus any closed loops and failure linkages among tree elements. The structure provides the hierarchy of systems and subsystems necessary for an infrastructure facility to perform its mission.

As an aid for developing fault trees for infrastructure facilities, it is helpful to divide facility systems into three categories according to their function as diagrammed in Figure 2: (i) Operations function, (ii) Protection function, and (iii) Support function. "Operation systems" perform mission-specific functions such as communication, manufacturing, storage, or materials/energy/transport inventory. "Protection systems" function to provide physical security, information security, fire protection, emergency services, and so on. "Support systems" provide the environment control, electric power, or communications necessary for the operation of mission and protection systems.

At first blush, the operational/mission systems appear to be the most critical to system performance. However, experience shows that the debilitation of support systems often has the most widespread effects on facility functionality [7]. If a saboteur is familiar with subsystem fault trees and interdependencies, he may be able to bring down an entire facility by attacking one subsystem of a support system. Mission systems tend to have more protection/security, making support systems the most accessible targets.

To address system resilience, the technique accounts for system and subsystem reconstitution times and constraints. Subsystems vary tremendously in their repair and replacement times. Some subsystem failures may also result in cascading effects exhibiting latent time delays. For example, the failure of a facility's environmental control supervisory control and data acquisition (SCADA) may cause room temperature to rise to a point in time where electronics begin to overheat. For this reason the formulation is designed to account for three subsystem time factors: (i) effects' onset delays, (ii) damage repair/replacement times, and (iii) repair commencement time bases on resource availability and system priority.

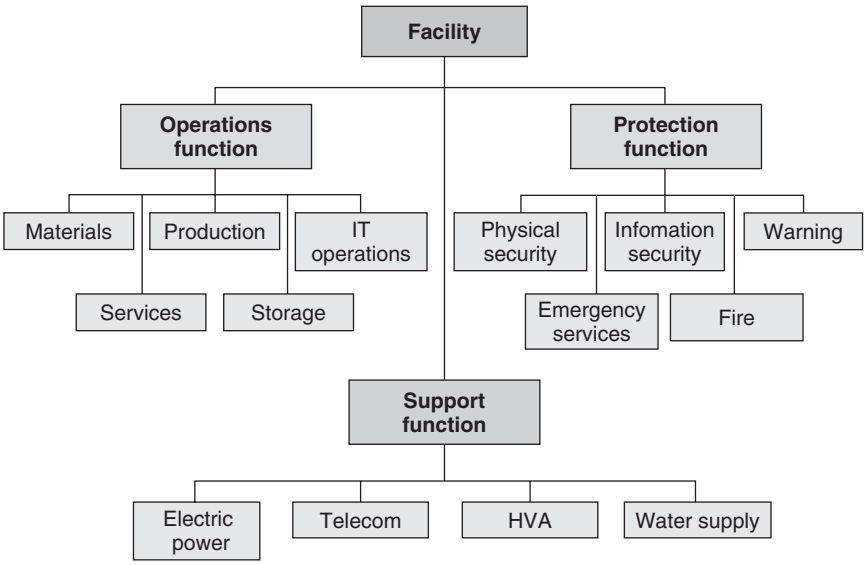



**FIGURE 2** Infrastructure facility generic functional diagram.

## 3 TIME-DOMAIN PRA MATHEMATICAL FORMULATION

Input information includes subsystem fault and function diagrams, scenario stresses on critical subsystems, subsystem component strengths (damage or disruption thresholds), subsystem effects onset probabilities and times, effects propagation paths and time lengths, and condition-constrained repair times. These inputs drive the computation of the probability of mission outage versus time. The method compares stresses to subsystem strengths, to determine the probability of effect at individual components. In cases where subsystem component's $P_e$'s are known, they can be input directly. These probabilities can be evaluated at any system point. They can also be calculated for a specified time of performance and for altered function diagrams. A diagram of the basic process flow is shown in Figure 3.

### 3.1 Probability of Effects Calculation at the Subsystem Level

Consider a system consisting of a number of subsystems with each subsystem consisting of many components. Let the components be the basic units for which we compare an environment-induced stress, **S**, with the component's physical damage threshold, **T**. The stress occurs at the weapon onset time ($t = 0$). **T** can be either a scalar quantity or a $K$-dimensional vector, where $K$ is the number of components. If a component $j$ sees $\mathbf{S} \geq \mathbf{T}$, defined as:

$$\{\min(\mathbf{S}_{jk} - \mathbf{T}_{jk}) \geq 0, k = 1 \ldots K\}$$

then it is counted as having suffered physical damage and will, at a latent time delay $\mathbf{TL}_j$ after the stress onset, not perform its function. Component $j$ is then defined as being in a state of "functional outage." Notice that the overall component mission state at any given

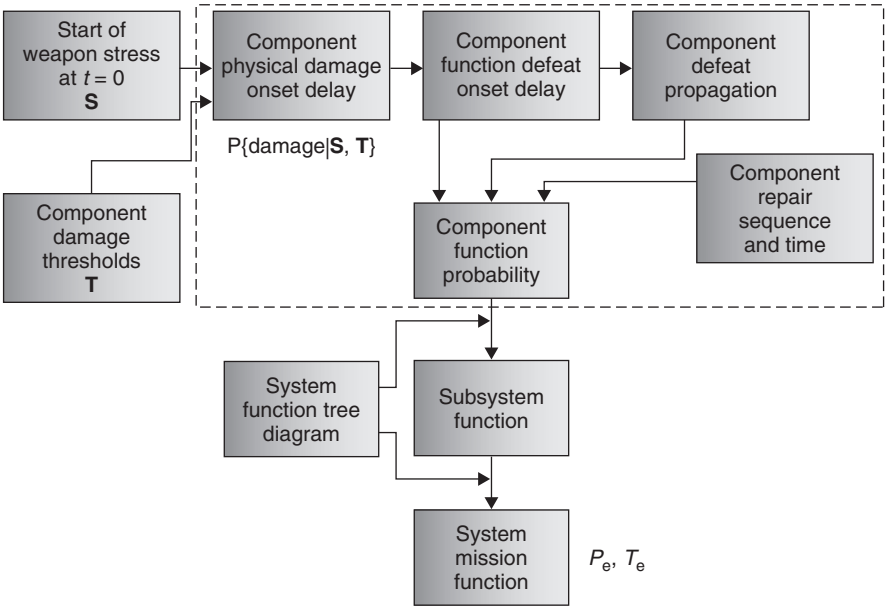



**FIGURE 3** Computational process flow.

time is modeled as a binary *functional* XOR *not-functional*. Gradual mission function degradation is very difficult to model due to the inherent nonuniqueness of associated system states and problems associated with aggregating such failures. Such degradation is beyond the capabilities of current fault-tree-based models.

The method uses parameter, $\mathbf{P}_{oj}$, to represent the probability that component $j$ is physically damaged as a consequence of the stress $\mathbf{S}_j$ exceeding the component's threshold $\mathbf{T}_j$ at $t = 0$. In mathematical notation:

$$\mathbf{P}_{oj} = Pr\{\mathbf{S}_j \geq \mathbf{T}_j\}$$

**S** and **T** are modeled as random variables, each with its own probability distribution determined on engineering and physical bases. These distributions, in practice, represent all estimated uncertainties and known variations. For different components, $\mathbf{S}_j$ may be statistically dependent due to physical proximity or other physical factors.

The model defines a functional outage status index variable, $\mathbf{I}_{dj}$. $\mathbf{I}_{dj} = 1$ if, and only if, component $j$ is in a state of functional outage and $\mathbf{I}_{dj} = 0$ if, and only if, the component is functional. This binary function status is a simplification. The variable could be graduated into "shades of gray" in the interval [0,1] quite straightforwardly, if required. The model includes a latent time delay, $\mathbf{TL}_j$ to account for the time duration necessary for component $j$'s physical damage to result in loss of its functionality. The model allows for uncertainty in latent time delay, by treating $\mathbf{TL}_j$ as a random variable with a probability distribution $f_j(t)$. This probability distribution may be scenario dependent.

At the subsystem level, any one of many sets of prespecified combinations of nonfunctional components serves to prevent subsystem function. And, any one set of prespecified combinations of subsystem outages constitutes overall debilitation of the system's mission.

### 3.2 Top-Level Functional Outage Computation

In order to quantify the infrastructure mission outage as a time varying probability, we define a state vector for each component $j$, $\mathbf{I}_j = (\mathbf{I}_{dj}, \mathbf{I}_{cj})$, where $\mathbf{I}_{dj}$ is the outage status index and $\mathrm{I}_{cj}$ tracks the outage time condition for component $j$. $\mathbf{I}_j = (0,0)$ if there is no physical damage and $\mathbf{I}_j = (0,TL)$ if it is damaged at effects onset time, but will manifest a latent functional outage at a later time. At the functional outage onset time, $\mathbf{t}_s$, $\mathbf{I}_j = (1, \mathbf{t}_s)$. Note that $\mathbf{t}_s$ is itself a function of time because a component can be damaged and repaired and damaged again due to functional outage propagation paths of other system components. If damaged, component $j$ may be repaired in time $\mathbf{TR}_j$, where $\mathbf{TR}_j$ is modeled as a random variable with a scenario-dependent probability distribution.

The repair start time may not commence immediately after a subsystem/component outage. The model accommodates situations where a repair sequence is needed, that is, certain components must be repaired before others can be fixed. The repair sequence is an explicit input and the model checks the sequence for preceding components' operational status and allows component $j$ to be repaired only if preceding components are functional.

It is also possible to model situations when, even if a subsystem is not damaged directly at $t = 0$, it can suffer a functional outage due to the accumulated outage of other "upstream" subsystems. An example would be electronics overheating due to the failure of heating, ventilation and air conditioning (HVAC) subsystems. Such outage propagation paths and times, $TP$ are accommodated by an additional layer of random variables with their uncertainty distributions as explicit inputs.

The probabilistic nature of system failure is implied by the input component stresses and thresholds, which are themselves described probabilistically. Likewise, the latent time delay, the propagated outage time, and the start and duration of repair times are described using probability distributions. Such distributions provide bounds for both the uncertainties in the exact physical description of a specific single system of interest, and system-to-system variations if more than one system is involved. The time factors result in a time varying probability of effects.

Theoretically, the fault-diagram representation maps each system state point $P(X)$, of the $2^N$ possible points in the component function space (where $N$ is the total number of components in the system), into a system function measure, 0 XOR 1. As time goes on, the state point, $P(X, t)$ traces a trajectory in the component function state space with its path influenced and controlled by all the physical constraints including damage, delay, propagation, and repair (see Section 2). The time changes occur in discrete time steps. Thus, the system functional state is a piecewise step function of time, with value 1 or 0. Because these physical constraints, including their initial values, are probabilistic, the method indicates the probability that the system is in a state of mission outage up to time $t$ based on the specified stress scenario.

The equivalent mathematical problem of coupled finite difference equations with stochastic "forces" is much more challenging to solve analytically in closed forms [8]. This method does it numerically, invoking a basic Monte Carlo simulation.

### 3.3 Practical Factors: Approximations and Uncertainties

With perfect knowledge of a system and its environment, one can predict certain system outages or functionalities, deterministically, as a function of time. Then there would be no need for a probabilistic formulation. Except in obvious, trivial cases, it is practically

infeasible to develop a rigorous, deterministic, analytical closed-form solution to quantify functional outage probabilities and their mathematical-statistical inference from data. This is particularly true if a classical frequency probability approach is used. At the other extreme, if too wide a range of weapon scenarios or facility variations are included in a probabilistic formulation, the quantification loses practical meaning. Also, purely subjective formulations lack consistency and credibility.

We have attempted to achieve a balanced approach, retaining the frequency interpretation as much as possible and using probability theory as a tool to treat and propagate the uncertainties. If necessary, the model can accept expert estimates, both explicitly and numerically.

Infrastructure modeling using any approach is nontrivial. With the time-domain PRA approach the following factors require particular care.

- The mission function must be specified and the necessary and sufficient component subset disablement to achieve functional outage must be determined.
- Determining the level of detail, and basic components to include in functional diagrams requires care.
- **S** and **T** are nonscalar in nature. Stresses at different components, and their uncertainties, are often not independent.
- There is often a latent time delay between component physical damage and the onset of functional outage.
- The propagation path and associated time delay from one component to another must be included.
- Component and subsystem repair times and inherent repair sequences must be specified. Also, the effect of human resource constraints and scenarios must be factored into the repair/reconstitution ability.
- The uncertainties associated with all input values and assumptions must be specified

The difficulty of specifying the joint probability distribution of mutually dependent and time-dependent stresses, thresholds, internal damage propagation, and repairs makes an analytically explicit solution infeasible. Nevertheless, the model is set up to provide a logical and defendable range of results based on available system information and reasonable engineering approximations.

### 3.4 Method Validity and Limitations

Incomplete knowledge of the facility/system functional components, their interrelationships and outage mechanisms can limit the accuracy of the calculation in two ways:

1. If an in-parallel functional component, which contributes to system performance redundancy, is omitted from the model, then the true effect on system operation is less than or equal to that assessed. In this case, the assessed effect measure is defense-conservative.
2. If an in-series functional component exists, which contributes to system vulnerability, but is omitted from modeling due to lack of information, then the true effect measure may be more serious than assessed. That is, the assessed results are offense-conservative.

Thus, the completeness of the set of identified model components results in uncertainties in the output probability in both directions of under- and overestimating system effects. This property can be helpful in performing sensitivity studies. The method can be used to investigate sensitivity to model completeness by selectively omitting from and adding to a system's component ensemble.

A critical part of the system assessment is to determine which components or combination of components must be nonfunctional to negate the system's mission capability. In some PRA literature this is referred to as a *cut set*, in that cutting off any one of its members, the set is invalidated as a sufficient cause of mission outage. Another concept useful for ensuring assessment realism involves identifying the minimum sufficient set of components that ensures functional performance if all its members perform their respective functions. This is equivalent to an "all component in series" functional diagram and is sometimes referred to as a *path set* in PRA literature, because a functional path through all of the set members constitutes a system function.

A theoretically trivial, but important and sometimes tricky consideration is the avoidance of double counting. This is a special case of correlated-cause component dependencies. In cases where one component's operational status appears in different sets, the model must ensure that the component is modeled as one and the same.

Model validation can be performed using logical implication checks. This involves running self-consistency and special limiting-case checks. Because of the general inability to do multiple system copy pass–fail experiments, validation must be indirect and relative. This is a general problem for all PRA models of complicated systems.

## 4 CRITICAL NEEDS ANALYSIS

It is very important to understand the risk of cascading failures and interacting infrastructures. Understanding the interactions and failure correlations among critical systems allows us to understand the consequences of failure of any one of the systems. Analysis of past high consequence infrastructure failures suggests that the risk of failure in one system can be significantly affected by fairly weak coupling with other systems.

Furthermore, it is not sufficient to merely predict the risk of system failure. Understanding system resilience requires the ability to predict system recovery timelines. Because it is cost-prohibitive to completely prevent system failures, understanding recovery processes and timelines emerges as arguably the most important aspect of assuring system resiliency. The time-domain PRA approach incorporates the ability to model system risk of failure at the initial time of stress and the subsequent time-line for system recovery.

There is a need for models at a high level of system abstraction for screening studies, because they make it possible to look at many different scenarios and long-time system interaction dynamics including system failure and recovery processes. The time-domain PRA approach offers a reduced, relatively simple approach to system modeling to complement full-physics system simulation models. Full-physics system simulations tend to be impractical for problems in which multiple scenarios need to be examined. Large, multiple-trial parameter studies can be computationally intractable in full-physics and agent-based models. Simplified system models that do not incorporate all system details offer a useful, complementary approach.

The time-domain PRA method offers the ability to evaluate the probability and duration of infrastructure system mission outages with a relatively limited set of system information. Required input information includes system fault trees, effect "stress" and subsystem/component "strength," and subsystem repair times and repair sequences. The approach also allows specification of latent time delay effects associated with the onset of damage. The method allows specification of variances for all input parameters. Input data may be empirical or estimated based on reasonable engineering approximations. Scenarios may include intentional physical or cyber attacks, Radio Frequency (RF) weapons, natural disasters, or normal accidents. The model enables comparison of the effectiveness of alternative mitigation strategies and techniques, and enables location of most serious failure points from the standpoint of highest probability of effect and longest duration functional outage. Output is provided in the form of probability of effects versus time output facilitates estimation of recovery times.

## 5 RESEARCH DIRECTIONS

The time-domain PRA approach has received attention only relatively recently. A simple, basic prototype of the method has been formulated using MATHCAD software. The method has been successfully demonstrated by modeling Electromagnetic Pulse (EMP) effects on a simple communication facility and blast effects on a national command center (classified study). These problems demonstrated the usefulness of the approach both computationally and as a "gedanken framework" for understanding prime system failure points and mechanisms.

Future research is needed to build on and generalize this introductory work, including:

- development of a fast-running production version of the method for application to larger infrastructure systems and networks;
- demonstration of the method on a problem of national interest, for example, interdependencies between the power grid and telecommunications grid [9]; and
- development of outage cost analysis algorithms based on system debilitation timelines.

On a broader scale, this approach should be beneficial for the development of:

- more complex "global" functional failure propagation and causation of interdependent infrastructures;
- techniques for system performance self-diagnosis and repair prioritization;
- dynamic sensitivity studies to develop more robust designs of complex systems and networks; and
- quantification of continuous instead of binary system performance degradation.

## REFERENCES

1. Rinaldi, S. (2004). Modeling and simulating critical infrastructure interdependencies. *Proceedings of the 37$^{th}$ Annual Hawaii Conference on System Sciences*, Hawaii.

2. Robert T. Marsh (1997). *Critical foundations: Protecting America's Infrastructures*. Report of the President's Commission on Critical Infrastructure Protection (PCCIP), Chairman, Washington, DC, 1997.
3. U.S. Department of Homeland Security. (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, U.S. Department of Homeland Security, February 2003.
4. U.S. Dept of Homeland Security. (2003). *The National Strategy to Secure Cyberspace*, U.S. Dept of Homeland Security, February 2003.
5. Baker, G. (2005). *A Vulnerability Assessment Methodology for Critical Infrastructure Facilities*, Department of Homeland Security R&D Partnerships Symposium, Boston, MA.
6. National Science Foundation. (2006). *Resilient and Sustainable Infrastructures Workshop*, Arlington, VA, 4-5 December 2006.
7. Kumamoto, H. and Henley, E.. (1996). *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd ed. IEEE Press, New York.
8. Baker, G. (2005). *A Vulnerability Assessment Methodology for Critical Infrastructure Facilities*, Department of Homeland Security R&D Partnerships Symposium, Boston, MA.
9. Kohlberg, I., Clark, J., Morrison, P.. (2007). Dynamics of recovery of coupled infrastructures following a natural disaster or malicious insult. *Proceedings of the James Madison University/Federal Facilities Council Symposium on Cascading Infrastructure Failures*. National Research Council, Washington, D.C., May 2007.

## FURTHER READING

Alliance, L. (2006). *Power Systems, Transportation and Communications Lifeline Interdependencies*, FEMA-National Institute of Building Sciences, March 2006, Washington, DC.

Amin, M. (2000). National infrastructures as Complex Interactive Networks. In *Automation, Control, and Complexity: An Integrated Approach*, Samad, T. and Weyrauch, J., Eds. John Wiley and Sons, New York, pp. 263–286.

Bruneau, M., Chang, S., Eguchi, R., Lee, G., O'Rourke, T., Reinhorn, A., Shinozuka, M., Tierney, K., Wallace, W., and von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra* **19**(4), 733–752.

Gnedenko, B., Belyayev, Y., and Solovyev, A. (1969). *Mathematical Methods of Reliability Theory*. Academic Press, New York.

Henley, E. and Kumamoto, H. (1992). *Probabilistic Risk Assessment*, IEEE Press, New York.

Koubatis, A., Schonberger, J. (2005). Risk management of complex critical systems. *Int. J. Crit. Infrastructures* **1**(2/3), 195–215.

National Research Council. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* . The National Academies Press, Washington, DC.

Nozick, L. and Turnquist, M. (2004). Assessing the performance of interdependent infrastructures and optimizing investments. *Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii.

Peerenboom, J. (2001). *Infrastructure Interdependencies: Overview of Concepts and Terminology*. Argonne National Laboratory Pamphlet.

Rinaldi, S. (2004). Modeling and simulating critical infrastructures and their interdependencies. *Proceedings of the 37th Hawaii International Conference on System Sciences,* Hawaii.

U.S. Department of Homeland Security. (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003.

Wolthusen, S. D. (2004). Modeling critical infrastructure requirements. *Proceedings of the 2004 IEEE Workshop on Information Assurance and Security,* June 2004, Charlotte, NC.

# RISK TRANSFER AND INSURANCE: INSURABILITY CONCEPTS AND PROGRAMS FOR COVERING EXTREME EVENTS

HOWARD C. KUNREUTHER AND ERWANN O. MICHEL-KERJAN
*Center for Risk Management and Decision Processes, the Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania*

## 1 INTRODUCTION

The United States has extensive experience with natural catastrophes. But the hurricanes that occurred in the Gulf Coast during the 2004 and 2005 seasons have changed the landscape forever. Coupled with the terrorism attacks of September 11, 2001, there is recognition by both the public and private sectors that one needs to rethink our strategy for dealing with these low probability but extreme consequence events.

The 2002 White House National Strategy defines homeland security as "the concerted effort to prevent attacks, reduce America's vulnerability to terrorism, and minimize the damage *and* recover from attacks that do occur". To succeed, homeland security must be a national and comprehensive effort. Moreover, that definition must apply to technological and natural disasters as well.

While protecting residential and commercial construction and critical infrastructure services (transportation, telecommunications, electricity and water distribution, etc.) in risky areas may limit the occurrence and/or the impacts of major catastrophes, we know that major disasters will still occur. In these situations one must provide adequate emergency measures and rapidly restore critical services. The question as to who will provide financial protection to victims (residents and commercial enterprises) will take center stage. The insurance infrastructure will then play a critical role [1].

This article discusses some fundamentals of the operation of insurance as well as some of the insurance programs that have been established in the United States to cover economic losses due to large-scale catastrophes.

## 2 HOW DOES INSURANCE WORK AND DOES NOT WORK

### 2.1 Determining Premiums and Coverage

***2.1.1 Basic Concepts.*** The insurance business, like any other business, has its own vocabulary. A *policyholder* is a person who has purchased insurance. A *premium* is the amount that a policyholder pays in return for the promise of a payment from the insurer should he suffer a loss covered by his policy. The term *benefit* denotes the payment by the insurer to the policyholder given that he has suffered a reduction in wealth due to a

loss. A *claim* means that the policyholder is seeking to recover financial payments from the insurer for damage covered by the policy. A claim will not result in a payment by the insurer if the amount of the insured's financial loss is below the stated *deductible* (i.e. the amount or proportion of an insured loss that the policyholder agrees to pay before any recovery from the insurer) or if the loss is subject to policy exclusions (e.g. war or insurrection). However, insurers will still incur expenses for investigating the claim.

Insurer *capital* represents the net worth of the company (assets minus liabilities). Capital enables the insurer to pay any losses above those that were expected. It serves as a safety net to support the risk that an insurer takes on by writing insurance and helps ensure that the insurer will be able to honor its contracts. As such, it supports the personal safety nets of homeowners, business owners, workers, dependents of heads of households, and others who rely on insurance to provide financial compensation to rebuild their lives and businesses after covered losses occur. Insurer capital is traditionally referred to as *policyholders' surplus*. Despite the connotation of the term *surplus*, there is nothing superfluous about it—it is, in fact, an essential component supporting the insurance promise. The cost of that capital is an insurer expense that must be considered in pricing insurance, along with expected losses, sales, and administrative expenses for policies written.[1]

The capital needed by an insurer varies directly with the risk that the insurer takes on. If an insurer wishes to take on more risk, it must have capital to support that risk. *Insurance regulators* and *rating agencies* in their efforts to assure policyholders that insurers will be able to pay their losses, devote significant efforts toward evaluating the adequacy of insurer capital relative to the amount and types of risk they are taking on. Holding an adequate level of capital is critical to the continued viability of an insurer.

Insurance markets function best when the losses associated with a particular risk are independent of each other and the insurer has accurate information on the likelihood of the relevant events occurring and the resulting damage. By selling a large number of policies for a given risk, the insurer is likely to have an accurate estimate of claim payments it expects to make during a given period of time. To illustrate this point with a simple example, consider an insurer who offers a fire insurance policy to a set of identical homes each valued at $100,000. Based on past data, the insurer estimates that the likelihood that the home will be destroyed by fire next year is 1/1000 and that this is the only loss that can occur. In this case the expected annual loss for each home would be $100 (i.e. 1/1000 × $100,000).

If the insurer issued only a single policy to cover the full loss from a fire, then there would be a variance of approximately $100 associated with its expected annual loss.[2] As the number of policies issued, $n$, increases, the variance of the expected annual loss, or the mean loss per policy, decreases in proportion to $n$. Thus, if $n = 10$, the variance of the mean loss will be approximately $10. When $n = 100$ the variance decreases to $1, and with $n = 1000$ the variance is $0.10. It is thus not necessary to issue a very large number of policies to reduce significantly the variability of expected annual losses

[1]Consider, for example, insurance for property damage caused by hurricanes. An insurer's expected losses are relatively low, because in a typical year, the policyholder will not suffer a hurricane loss. However, it is possible that losses will be quite high—far in excess of those expected at the time policies are priced. In the event of a serious hurricane, a substantial portion of the loss must be paid from insurer capital. For terrorism coverage, maximum losses are extremely high relative to expected losses, so the capital issue is critical.

[2]The variance for a single loss $L$ with probability $p$ is $Lp\ (1-p)$. If $L$ = $100,000 and $p$ = 1/1000, then $Lp(1-p)$ = $100,000 (1/1000)(999/1000), or $99.90.

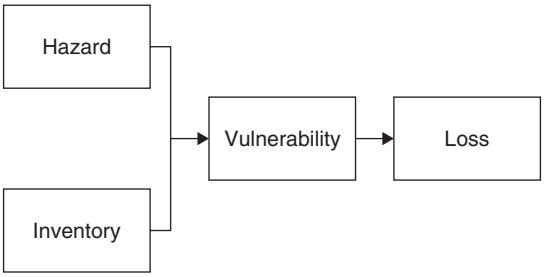



**FIGURE 1** Structure of catastrophe models.

per policy if the risks are independent. This model of insurance works well for risks such as fire, automobile, and loss of life where the above assumptions of independence and ability to estimate probabilities and losses are satisfied. As will be shown below, terrorism risk does not satisfy the above conditions, so it is more problematic to insure.

***2.1.2 Catastrophe Models[3].*** Before insurance providers are willing to offer coverage against an uncertain event they feel they must be able to identify and quantify, or at least partially estimate the chances of the event occurring and the extent of losses likely to be incurred. Such estimates can be based on past data (e.g., loss history of the insurer's portfolio of policyholders, loss history in a specific region) coupled with data on what experts know about a particular risk through the use of catastrophe models.

The four basic components of a catastrophe model are hazard, inventory, vulnerability, and loss, as depicted in Figure 1, and illustrated for a natural hazard such as a hurricane. First, the model determines the risk of the *hazard* phenomenon, which in the case of a hurricane is characterized by its projected path and wind speed. Next, the model characterizes the *inventory* (or portfolio) of properties at risk as accurately as possible. This is done by first assigning geographic coordinates such as latitude and longitude to a property based on its street address, zip code, or another location descriptor, and then determining how many structures in the insurer's portfolio are at risk from hurricanes of different wind speeds and projected paths. For each property's location in spatial terms, other factors that characterize the inventory at risk are the construction type, the number of stories in the structure, and its age.

The hazard and inventory modules enable one to calculate the *vulnerability* or susceptibility to damage of the structures at risk. In essence, this step in the catastrophe model process quantifies the physical impact of the natural hazard phenomenon on the property at risk. How this vulnerability is quantified differs from model to model. On the basis of this measure of vulnerability, the *loss* to the property inventory is evaluated. In a catastrophe model, loss is characterized as direct or indirect in nature. Direct losses include the cost to repair and/or replace a structure. Indirect losses include business interruption impacts and relocation costs of residents forced to evacuate their homes.

Catastrophe models were introduced in the mid-1980s but did not gain widespread attention until after Hurricane Andrew hit southern Florida in August, 1992, causing insured losses of over $21.5 billion (in 2004 prices). Until 9/11 this was the largest single loss in the history of insurance. Nine insurers became insolvent as a result of their

[3]This section is based on [2].

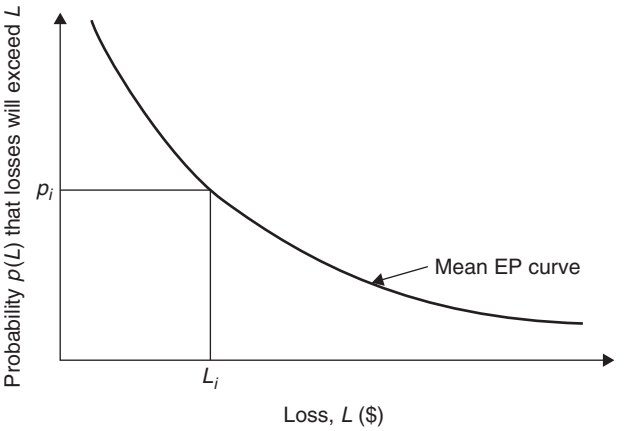



**FIGURE 2** Sample mean exceedance probability curve.

losses from Hurricane Andrew. Insurers and reinsurers thought that, in order to increase the chances of remaining in business, they needed to estimate and manage their natural hazard risk more precisely. Many companies turned to the modelers of catastrophe risks for decision support.

***2.1.3 Exceedance Probability Curves[4].*** On the basis of the outputs of a catastrophe model, the insurer can construct an exceedance probability (EP) curve that specifies the probabilities that a certain level of losses will be exceeded. The losses can be measured in terms of dollars of damage, fatalities, illness, or some other unit of analysis.

To illustrate with a specific example, suppose one were interested in constructing an EP curve for an insurer with a given portfolio of insurance policies covering wind damage from hurricanes in a southeastern US coastal community. Using probabilistic risk assessment, one would combine the set of events that could produce a given dollar loss and then determine the resulting probabilities of exceeding losses of different magnitudes. On the basis of these estimates, one can construct a mean EP curve such as the one depicted in Figure 2. The x-axis measures the loss to insurer in dollars and the y-axis depicts the probability that losses will exceed a particular level. Suppose the insurer focuses on a specific loss $L_i$. One can see from Figure 2 that the likelihood that insured losses exceed $L_i$ is given by $p_i$.

An insurer utilizes its EP curve for determining how many structures it will want to include in its portfolio given that there is some chance that there will be hurricanes causing damage to some subset of its policies during a given year. More specifically, if the insurer wanted to reduce the probability of a loss from hurricanes that exceeds $L_i$ to be less than $p_i$ it will have to determine what strategy to follow. The insurer could reduce the number of policies in force for these hazards, decide not to offer this type of coverage at all (if permitted by law to do so) or increase the capital available for dealing with future hurricanes that could produce large losses.

Federal and state agencies may want to use EP curves for estimating the likelihood that losses to specific communities or regions of the country from natural disasters in the coming year will exceed certain levels in order to determine the chances that it will

[4]This section is based on material in [3].

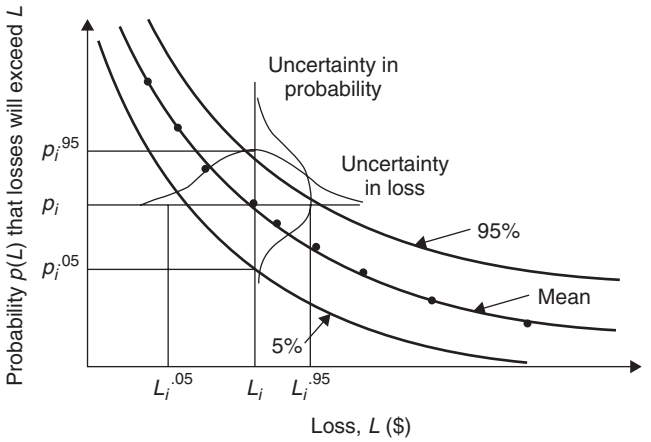



**FIGURE 3** Confidence intervals for a mean exceedance probability (EP) curve.

have to provide disaster assistance to these stricken areas. At the start of the hurricane season in 2004, Florida could have used an EP curve to estimate the likelihood of damage exceeding $23 billion. Although this probability would have been extremely low, we now know that a confluence of events (i.e., Charley, Frances, Ivan, and Jeanne) produced an outcome that exceeded this dollar value.

The uncertainty associated with the probability of an event occurring and the magnitude of dollar losses of an EP curve is reflected in the 5 and 95% confidence interval curves in Figure 3. The curve depicting the uncertainty in the loss shows the range of values, $L_i^{0.05}$ and $L_i^{0.95}$ that losses can take for a given mean value, $L_i$, so that there is a 95% chance that the loss will be exceeded with probability $p_i$. In a similar vein one can determine the range of probabilities, $p_i^{0.05}$ and $p_i^{0.95}$ so that there is 95% certainty that losses will exceed $L_i$. For low probability-high consequence risks, the spread between the 5 and 95% confidence intervals depicted in Figure 3 shows the degree of indeterminacy of these events.

The EP curve serves as an important element for evaluating risk management tools. It puts pressure on experts to make explicit the assumptions on which they are basing their estimates of the likelihood of certain events occurring and the resulting consequences.

## 2.2 Determining Whether to Provide Coverage

On the basis of their knowledge of likelihood and outcome, an insurer has to make a decision as to whether to cover the risk (unless they are required to do so by law). In his study on insurers' decision rules as to when they would market coverage for a specific risk, Stone [4] develops a model whereby firms maximize expected profits subject to satisfying a constraint related to the survival of the firm.[5] An insurer satisfies its survival constraint by choosing a portfolio of risks with an overall expected probability of total claims payments greater than some predetermined amount ($L^*$) that is less than some threshold probability, $p_1$. This threshold probability reflects the trade-off between the

[5]Stone also introduces a constraint regarding the stability of the insurer's operation. Insurers have traditionally not focused on this constraint in dealing with catastrophic risks but reinsurers have, as discussed in the next article.

expected benefits of another policy and the costs to the firm of a catastrophic loss that reduces the insurer's surplus by $L^*$ or more. This threshold probability does not necessarily correspond to what would be efficient for society. The value of $L^*$ is determined by an insurer's concern with insolvency and/or a sufficiently large loss in surplus that will lead a rating agency to downgrade its credit rating.

A simple example illustrates how an insurer would utilize its survival constraint to determine whether a particular portfolio of risks is insurable with respect to hurricanes. Assume that all homes in a hurricane-prone area are identical and equally resistant to damage such that the insurance premium, $P$, is the same for each structure. Furthermore assume that an insurer has $S$ dollars in current surplus and wants to determine the number of policies it can write and still satisfy its survival constraint. Then, the maximum number of policies, $n$, satisfying the survival constraint is given by Eq. (1):

$$\text{Probability [claims payments } (L^*) > (n \cdot P + S)] < p_1 \tag{1}$$

The insurer will use the survival constraint to determine the maximum number of policies it is willing to offer, with possibly an adjustment in the amount of coverage and premiums, and/or a transfer of some of the risk to others in the private sector (e.g. reinsurers or capital markets). It may also rely on state or federal programs to cover its catastrophic losses.

Following the series of natural disasters that occurred at the end of the 1980s and in the 1990s, insurers focused on the survival constraint to determine the amount of catastrophe coverage they were willing to provide because they were concerned that their aggregate exposure to a particular risk did not exceed a certain level. Rating agencies, such as A.M. Best, focused on insurers' exposure to catastrophic losses as one element in determining credit ratings, so insurers paid attention to this risk.

### 2.3 Setting Premiums

If the insurer decides to offer coverage, it needs to determine a premium rate that yields a profit and satisfies its survival constraint given by Eq. (1). State regulations often limit insurers in their rate-setting process. Competition can play a role as well as to what premium can be charged in a given marketplace. Even in the absence of these influences, an insurer must consider problems associated with the *ambiguity of the risk*, asymmetry of information (*adverse selection* and *moral hazard*), and degree of *correlation* of the risk in determining what premium to charge. We briefly examine each of these factors in turn.

***2.3.1 Uncertainty of the Risk.*** The infrequency of major catastrophes in a single location implies that the loss distribution is not well specified. The ambiguities associated with the probability of an extreme event and with the outcomes of such an event raise a number of challenges for insurers with respect to pricing their policies. As shown by a series of empirical studies, actuaries and underwriters are averse to ambiguity and want to charge much higher premiums when the likelihood and/or consequences of a risk are highly uncertain than if these components of risk are well specified [5].

Figure 4 illustrates the total number of loss events from 1950 to 2000 in the United States for three prevalent hazards: earthquakes, floods, and hurricanes. Events were selected that had at least $1 billion of economic damage and/or over 50 deaths [6].

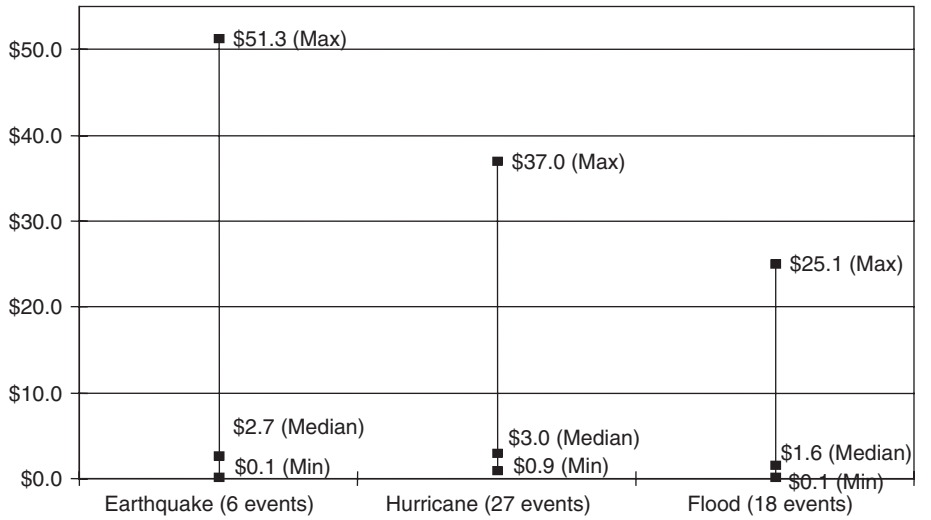



**FIGURE 4** Historical economic losses in $ billions versus type of significant US natural disaster for the 50-year period from 1950 to 2000.

Looking across all the disasters of a particular type (earthquake, hurricane, or flood), for this 50-year period, the median loss is low while the maximum loss is very high. Given this wide variation in loss distribution, it is not surprising that insurers are concerned about the uncertainty of the loss in estimating premiums, or even providing any coverage in certain hazard prone areas.

The 2004 and 2005 seasons have already dramatically changed the upper limits in Figure 4. Hurricane Katrina is estimated to have caused between $150 billion and $170 billion in economic losses, more than four times higher than the most costly hurricane between 1950 and 2000. On the other hand, no hurricane hit the US landfall this year, despite predictions earlier in the year indicated higher than normal intensive season.

***2.3.2 Adverse Selection.*** If the insurer cannot differentiate the risks facing two groups of potential insurance buyers and each buyer knows his/her own risk, then the insurer is likely to suffer losses if it sets the same premium for both groups by using the entire population as a basis for this estimate. If only the highest risk group is likely to purchase coverage for that hazard and the premium is below its expected loss, the insurer will have a portfolio of "bad" risks. This situation, referred to as *adverse selection*, can be rectified by the insurer charging a high enough premium to cover the losses from the bad risks. In so doing, the good risks might purchase only partial protection or no insurance at all because they consider the price of coverage to be too expensive relative to their risk[6].

This was the argument made by private insurers regarding the noninsurability of flood risk that led to the creation of the National Flood Insurance Program (NFIP). Indeed, insurers thought that family who had lived in a specific flood-prone area for many years had a much better knowledge of the risk than any insurer would have unless it invested in costly risk assessment tools.

[6]For a survey of adverse selection issues, see [7].

In the context of hurricane, however, it is not clear whether there is any adverse selection. Indeed, there is no evidence that those at risk have an informational advantage over the insurer. In fact, the opposite might be true: if insurance companies spend a lot of resources estimating the risk (what they actually do) they might gain an informational advantage over their policyholders who cannot afford or want to do so. Over the past 5 or 6 years, there has been a growing literature studying the impact of insurers being *more* knowledgeable about the risks than the insured themselves. Research in this field reveals that insurers might want to exploit this "reverse information asymmetry", which results in low risk agents being optimally covered while high risks are not [8].

***2.3.3 Moral Hazard.*** This refers to an increase in the expected loss (probability or amount of loss conditional on an event occurring) caused by insurance-induced changes in the behavior of the policyholder. An example of moral hazard is more careless behavior *vis-à-vis* natural hazards or other types of risk as a result of purchasing coverage. Providing insurance protection may lead the policyholder to change behavior in ways that increase the expected loss from what it would have been without coverage. If the insurer cannot predict this behavior and relies on past loss data from uninsured individuals to estimate rates, the resulting premium is likely to be too low to cover losses.

Even after the insurer is aware that people with insurance have higher losses, its inability to observe loss-enhancing behavior may create problems of moral hazard. The introduction of specific deductibles, coinsurance or upper limits on coverage can be useful tools to reduce moral hazard by encouraging insureds to engage in less risky behavior, as they know they will have to incur part of the losses from an adverse event.

***2.3.4 Correlated Risks.*** For extreme events, the potential for high correlation between the risks will have an impact on the tail of the distribution. In other words, at a predefined probability $p_i$, the region below the EP curve is likely to expand for higher correlated risks covered by insurers. This requires additional capital for the insurer to protect itself against large losses. Insurers normally face spatially correlated losses from large-scale natural disasters. State Farm and Allstate Insurance paid $3.6 billion and $2.3 billion in claims, respectively, in the wake of Hurricane Andrew in 1992 due to their high concentration of homeowners' policies in the Miami/Dade County area of Florida. Given this unexpectedly high loss, both companies began to reassess their strategies of providing coverage against wind damage in hurricane-prone areas [9].

Hurricanes Katrina and Rita that devastated the US Gulf Coast in August and September 2005 impacted dramatically on several lines, including life, property damage, and business interruption. Edward Liddy, chairman of Allstate, which provided insurance coverage to 350,000 homeowners in Louisiana, Mississippi, and Alabama, declared that "extensive flooding has complicated disaster planning . . . and the higher water has essentially altered efforts to assess damage. We now have 1100 adjusters on the ground. We have another 500 who are ready to go as soon as we can get into some of the most-devastated areas. It will be many weeks, probably months, before there is anything approaching reliable estimates" [10].

***2.3.5 Role of Capital Costs.*** The importance of capital and its need to secure an adequate rate of return is often not sufficiently understood. In particular, the prices charged for catastrophe insurance must be sufficiently high to cover the expected claims costs and other expenses, but must also cover the costs of allocating risk capital to underwrite

this risk. Moreover, because the large amounts of risk capital are needed to underwrite catastrophe risk relative to the expected liability, the capital cost built into the premium is high, often dominating the expected loss cost. Thus, an insurer usually needs to charge high prices relative to its loss expenses, simply to earn a fair rate of return on equity and thereby maintain its credit rating.

To illustrate, we construct a hypothetical example that is somewhat conservative by ignoring taxes. Consider a portfolio that has 1000 in expected liabilities, $E(L)$. Since actual losses will not equal expected losses, the insurer needs to hold considerable capital. Here we will assume that \$1 of capital is needed for each \$1 of expected liability to maintain the insurer's credit rating. Thus the insurer needs capital, $E(L) = 1000$. In addition to paying claims, the insurer has an additional 200 in upfront-expected expenses that include commissions to agents and brokers, and underwriting expenses. Moreover, given the risk characteristics of the portfolio, investors require a rate of return ($ROE$) of 15% on their investment to compensate for risk. The insurer invests its funds in lower risk vehicles that yield an expected return, $r$, of 10%. What premium $P$ would the insurer have to charge to secure a return of 15% for its investors?

The formula for the premium can be expressed as a function of the cash flows, the return on investment and the required return on equity ($k$ is the ratio of equity to expected losses)

$$P = \frac{X(1+r) + E(L)}{(1+r) - k(ROE - r)}$$

$$P = \frac{200(1+0.05) + 1000}{(1+0.05) - 1(0.15 - 0.05)} = 1210$$

Premiums need to be 1210 to generate this required 15% return on equity.

This calculation is very sensitive to the ratio of capital to expected liability, $k$, needed to preserve credit. In the above example, the ratio was one dollar of capital for one dollar of expected liability. This ratio is in the ballpark for many property liability insurers for their combined books of business. However, for catastrophe risk, with its very high tail risk (which severely affects credit risk), the capital to liability ratio needs to be considerably higher. Indeed, the capital to liability ratio depends on volatility (particularly, the downside or tail risk) of the catastrophe liability and its correlation with the insurer's remaining portfolio. For higher layers of cat risk, the expected loss is often quite low and the volatility very high. At these layers, the required capital to liability ratio can be considerably greater than unity as shown in this example. An increase in the capital to liability ratio will increase the premium required to generate a fair return on equity.

A second issue with catastrophe risk is that it can be expensive to underwrite since it requires extensive modeling. Many companies will buy commercial models and/or use their own in-house modeling capability. If we rework the above premium calculation now with the transaction costs set at 100% of expected losses and 4:1 capital to expected liability ratio the required premium is now 3154:

$$P = \frac{1000(1+0.05) + 1000}{(1+0.05) - 4(0.15 - 0.05)} = 3154$$

For very high layers even more capital may be needed, thus further increasing the premium. There are other considerations that can dramatically leverage upwards the

capital cost, notably the impact of double taxation [11] have simulated the tax burden over many parameterizations and show that tax costs alone can reasonably be as much as the claim cost and lead to further increases in premiums. When we account for all these factors (i.e. high capital inputs, transaction costs, and taxes), catastrophe insurance premiums often are several multiples of expected claims costs.

### 2.4 Role of Rating Agencies

During the past few years, rating agencies have played increasing attention to the impact that catastrophic risks will have on their view of the financial stability of insurers and reinsurers. The rating given to a company will affect their ability to attract business and hence their pricing and coverage decisions.

To illustrate how ratings are determined consider A.M. Best. It undertakes a quantitative analysis of an insurer's balance sheet strength, operating performance, and business profile. Evaluation of catastrophe exposure plays a significant role in the determination of ratings, as these are events that could threaten the solvency of a company. Projected losses of disasters occurring at specified return periods (a 100-year windstorm/hurricane or a 250-year earthquake) and the associated reinsurance programs to cover them are two important components of the rating questionnaires that insurers are required to complete.

For several years now, A.M. Best has been requesting such information for natural disasters. Their approach has been an important step forward in the incorporation of catastrophe risk into an insurer's capital adequacy requirements. Up until recently the rating agency has been including probable maximum loss (PML) for only *one* of these severe events (100-year windstorm/250-year earthquake, depending on the nature of the risk the insurer was mainly exposed to) in its calculation of a company's risk-adjusted capitalization. In 2006 A.M. Best introduced a second event as an additional stress test. The PML used for the second event is the same as the first event in the case of hurricane (a 1-in-100 year event; the occurrence of one hurricane is considered to be independent of the other one). If the main exposure facing the insurer is an earthquake, the second event is reduced from a 1-in-250 year event to a 1-in-100 year event [12]. These new requirements have increased the amount of risk capital that insurers have been forced to allocate to underwrite this risk and have made them more reluctant to provide this coverage unless they are able to raise premiums sufficiently to reflect these additional costs.

In March 2006, Standard and Poor's, another rating agency, indicated that it would revise criteria for measuring cat risk which has traditionally been based on premium charges. But the new criteria will measure catastrophe risk based on exposure of the insurer. This will include an exposure-based capital charge for insurers similar to what it does for reinsurers based on net expected annual aggregate property losses for all perils at 1-in-250 year return period. There will be a 6–12 month phase period to allow companies to adjust risk profiles [13].

### 2.5 Role of Market State Regulation

In the United States, insurance is regulated at the state level with the principal authority residing with insurance commissioners. Primary insurers are subject to solvency regulation and rate and policy form regulation, whereas domestic reinsurers are subject only to solvency regulation (the price and terms of reinsurance transactions are not subject

to regulation). Solvency regulation addresses the question as to whether the insurer or reinsurer is sufficiently capitalized to fulfill its obligations if a significant event occurs and inflicts major losses on its policyholders.

Insurance commissioners regard solvency as a principal objective even if it means requiring higher premiums or other insurer adjustments (e.g. reducing their catastrophe exposures). On the other hand, insurance regulators face political pressure to keep insurance premiums "affordable" and coverage readily available. In balancing solvency and consumer protection goals, insurance regulators are required by state laws to ensure that rates are adequate but not excessive and not unfairly discriminatory. Regulators' assessment of insurers' rates and other practices involves some degree of subjectivity that can result in rate restrictions that reduce the supply of insurance or cause other market problems and distortions. "Parameter uncertainty" and different opinions on the level of risk of loss can lead to disagreements between insurers and regulators over what constitutes adequate rates and appropriate underwriting practices.[7]

State legislatures, governors, and the courts also play a significant role in the regulation of insurers and insurance markets. Consequently, insurance regulators are subject to a number of constraints on their authority and discretion and the other branches of state government may impose their preferences on how state laws, regulations, and policies govern insurers and insurance markets. Ultimately, all elected officials and their appointees are subject to the will of the voters—if government officials act contrary to the preferences of voters, they are subject to being replaced by people who will obey the voters, even if their actions are economically unsound.

## 3 US FEDERAL AND STATE CATASTROPHE PROGRAMS

We now turn to the important role that the federal and state governments in the United States play in supplementing or replacing private insurance with respect to natural disasters, nuclear accidents, and other catastrophic losses. This section provides a brief overview of several of these programs to illustrate the types of public–private partnerships that have been implemented in the past.

### 3.1 Flood and Hurricane Insurance

***3.1.1 Flood.*** Insurers have experimented over the years with providing protection against water damage from floods, hurricanes, and other storms. After the severe Mississippi Floods of 1927, they concluded that the risk was too great, and refused to provide private insurance again. As a result, Congress created the NFIP in 1968, whereby homeowners and businesses could purchase coverage for water damage. Private insurers market flood policies, and the premiums are deposited in a federally operated Flood Insurance Fund, which is then responsible for paying claims. The stipulation for this financial protection is that the local community makes a commitment to regulate the location and design of future floodplain construction to increase safety from flood hazards. The federal government established a series of building and development standards for floodplain construction to serve as minimum requirements for participation

[7]See [14–16] for more detailed discussions of insurance regulatory policies in general and specific to natural disaster risk.

in the program. The creation of the Community Rating System in 1990 has linked mitigation measures with the price of insurance in a systematic way [17].

The number of claims paid by the NFIP differs from year to year, but between 1980 and 2002 was never higher than 62,400, which was the count in 1995. The severity of flood losses from the 2004 hurricane season led to 75,000 claims, a new record in the history of the program. The breach in the New Orleans levees from Hurricane Katrina coupled with the flood losses from Hurricanes Katrina, Rita, and Wilma triggered some 239,000 claims with the NFIP in 2005, 80% of which were from Hurricane Katrina. It is estimated that the NFIP will pay in excess of $23 billion in flood claims for the 2005 hurricane season, the equivalent of 10 years of premiums. This raises major questions regarding the future of the program. Two bills are currently being discussed in Congress as to how modify its operation so it fits better with this new loss dimension.

***3.1.2 Hurricane Insurance.*** The need for hurricane insurance is most pronounced in the state of Florida. Following Hurricane Andrew in 1992, nine property-casualty insurance companies became insolvent, forcing other insurers to cover these losses under Florida's State Guaranty Fund. Property insurance became more difficult to obtain as many insurers reduced their concentrations of insured property in coastal areas. During a special session of the Florida State Legislature in 1993 the Florida Hurricane Catastrophe Fund (FHCF) was created to relieve pressure on insurers to reduce their exposures to hurricane losses. The FHCF, a tax-exempt trust fund administered by the State of Florida, is financed by premiums paid by insurers that write policies on personal and commercial residential properties. The fund reimburses a portion of insurers' losses following major hurricanes (above the insurer's retention level) and enables insurers to remain solvent [10]. The four hurricanes that hit Florida in the fall of caused an estimated $29 billion in insured losses, with only about $2.6 billion paid out by the fund. Each hurricane was considered a distinct event, so that retention levels were applied to each storm before insurers could turn to the FHCF.

As this article goes to press, the future of hurricane and flood insurance in the United States is being analyzed as part of a research initiative between the Wharton School, Georgia State University, and the Insurance Information Institute, in partnership with over 15 insurers and reinsurers, trade associations, and federal agencies.

## 3.2 Earthquake Insurance

The history of earthquake activity in California convinced legislators that this risk was too great to be left in the hands of private insurers alone. In 1985, a California law required insurers writing homeowners coverage on one to four unit residential buildings to also offer earthquake coverage. Since rates were regulated by the state, insurers felt they were forced to offer coverage against older structures in poor condition, with rates not necessarily reflecting the risk. Following the 1994 Northridge earthquake, huge losses on insured property created a surge in demand for coverage. Insurers were concerned that if they satisfied the entire demand, as they were required to do by the 1985 law, they would face an unacceptable level of risk and become insolvent following the next major earthquake. Hence, many firms decided to stop offering coverage or restricted the sale of homeowners' policies in California.

In order to keep earthquake insurance alive in California, the State legislature authorized the formation of the California Earthquake Authority (CEA) in 1996. The CEA is

a state-run insurance company that provides earthquake coverage to homeowners. The innovative feature of this financing plan is the ability to pay for a large earthquake while committing relatively few dollars up front. There is an initial assessment of insurers of $1 billion to start the program and then contingent assessments to the insurance industry and reinsurers following a severe earthquake. Policyholders absorb the first portion of an earthquake through a 15% deductible on their policies [18]. However, 8 years after the creation of the CEA, the take-up rate for homeowners is about 15%, down from 30% when the California State Legislature created the CEA [19]. It is questionable how effective this program will be in covering losses should a major earthquake occur in California.

### 3.3 Nuclear Accident Insurance[8]

The Price-Anderson Act, originally enacted by Congress in 1957, limits the liability of the nuclear industry in the event of a nuclear accident in the United States. At the same time, it provides a ready source of funds to compensate potential accident victims, which would not ordinarily be available in the absence of this legislation. The Act covers large power reactors, small research and test reactors, fuel reprocessing plants, and enrichment facilities for incidents that occur through plant operation as well as transportation and storage of nuclear fuel and radioactive wastes.

Price-Anderson sets up two tiers of insurance. Each utility is required to maintain the maximum amount of coverage available from the private insurance industry—currently $300 million per site. In the United States, this coverage is written by the American Nuclear Insurers, a joint underwriting association or "pool" of insurance companies. If claims following an accident exceed that primary layer of insurance, all nuclear operators are obligated to pay up to $100.59 million for each reactor they operate payable at the rate of $10 million per reactor, per year. As of February 2005, the US public had more than $10 billion of insurance protection in the event of a nuclear reactor incident. More than $200 million has been paid in claims and costs of litigation since the Price-Anderson Act went into effect, all of it by the insurance pools. Of this amount, approximately $71 million has been paid in claims and costs of litigation related to the 1979 accident at Three Mile Island.

In February 2003, Congress extended the law for power reactors licensed by the Nuclear Regulatory Commission (NRC) to the end of 2003.[9] Coverage for facilities operated by the Department of Energy has been extended until the end of 2006 in a separate legislative action. Congress is now considering further extension of the law as part of comprehensive energy legislation.

### 3.4 Federal Aviation Administration Third Party Liability Insurance Program

Since the terrorist attacks of September 11, 2001, the US commercial aviation industry can purchase insurance for third party liability arising out of aviation terrorism. The

[8]For more details on nuclear accident insurance see Nuclear Energy Institute "Price-Anderson Act Provides Effective Nuclear Insurance at No Cost to the Public", February 2005.

[9]Although the existing law has technically expired, its provisions are "grandfathered" and continue to apply to all existing NRC licensees, that is to say, to power reactor operators with operating licenses issued prior to the expiration date. Personal Correspondence with John Quattrocchi July 21, 2005.

current mechanism operates as a pure government program, with premiums paid by airlines into the Aviation Insurance Revolving Fund managed by the Federal Aviation Administration (FAA).

As the program carries a liability limit of only $100 million, losses paid by government sources in the event of an attack will almost surely exceed those available through the current insurance regime. In that case, either the government would need to appropriate additional disaster assistance funds as it did in the aftermath of September 11th, or victims would be forced to rely on traditional sources of assistance [20].

### 3.5 International Terrorism Risk Insurance Program (TRIA)

Although the United States has been successful since 9/11 in preventing terrorist attacks on its own soil, the impact on the economy of another mega-attack or series of coordinated attacks will cause serious concerns to the government, the private sector and citizenry [21, 22]. With security reinforced around federal buildings, the commercial sector constitutes a softer target for terrorist groups to inflict mass casualties and stress on the nation. These threats require that the country as a whole develops strategies to prepare for and recover from a (mega-)terrorist attack. Insurance is an important policy tool for consideration in this regard.

Quite surprisingly, even after the terrorist attack on the World Trade Center in 1993 and the Oklahoma City bombing in 1995, insurers in the United States did not view either international or domestic terrorism as a risk that should be explicitly considered when pricing their commercial insurance policy, principally because losses from terrorism had historically been small and, to a large degree, uncorrelated. Thus, prior to September 11, 2001, terrorism coverage in the United States was an unnamed peril included in most standard all-risk commercial and homeowners' policies covering damage to property and contents.

The terrorist attacks of September 11, 2001, killed over 3000 people from over 90 countries and inflicted insured losses currently estimated at $32.5 billion that was shared by nearly 150 insurers and reinsurers worldwide. Reinsurers (most of them European) were financially responsible for the bulk of these losses. These reinsurance payments came in the wake of outlays triggered by a series of catastrophic natural disasters over the past decade and portfolio losses due to stock market declines. Having their capital base severely hit, most reinsurers decided to reduce their terrorism coverage drastically or even to stop covering this risk.

In response to such concerns, the Terrorism Risk Insurance Act (TRIA) of 2002 was passed by Congress and signed into law by President Bush on November 26, 2002.[10] It constitutes a temporary measure to increase the availability of risk coverage for terrorist acts [23]. TRIA is based on risk sharing between the insurance industry, all policyholders (whether or not they have purchased terrorism insurance) and the federal government (taxpayers) up to $100 billion of insured losses on US soil. President Bush signed into law a 2-year extension of TRIA on December 22, 2005, the Terrorism Risk Insurance Extension Act (TRIEA) that expanded the private sector role and reduced the federal share of compensation for terrorism insured losses. Since TRIA was passed prices have stabilized in most industries and take-up rate continuously increased. Today, over 60%

[10]The complete version of the Act can be downloaded at: http://www.treas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/claims_process/program.shtml.

of large commercial firms have some type of terrorism insurance coverage [24]. As we write this article in January 2007, it is unclear what type of long-term terrorism insurance program, if any, will emerge at the end of 2007 for dealing with the economic and social consequences of terrorist attacks.

## 4 CONCLUDING REMARKS

The past 5 years have demonstrated that the United States can suffer today catastrophic losses from disasters that far exceed those from events that occurred prior to 2000. Insurance has played a critical role in the recovery process, but these recent catastrophes have raised questions as to under which conditions the private sector can continue to provide coverage (and will want to) and the role that the public sector should play in dealing with these events. One limiting factor of the programs we discussed in this article is that the premiums they charge are often not based on risk, reducing the economic incentive to invest in cost-effective mitigation measures. Implementing reforms that will have premiums based on risk is certainly one way to start.

Also, so far, the country has responded by developing specific programs for each type of catastrophes. Whether this is the best way to go remains an open question. Other countries have developed some coverage that protects homeowners and businesses against all types of disasters: wind, flood, terrorist attacks, and so on [25]. This idea has been proposed for the United States many years ago [26] and has been resurrected following Hurricane Katrina[11]. Whether a risk-based all-hazard disaster insurance is now more appropriate given the events of the past 5 years is an issue for the new US Congress to study in more detail.

## REFERENCES

1. Auerswald, P., Branscomb, L., LaPorte, T., and Michel-Kerjan, E., Eds. (2006). *Seeds of Disasters, Roots of Response. How Private Action Can Reduce Public Vulnerability*. Cambridge University Press, New York, p. 504.
2. Grossi, P. and Kunreuther, H., Eds. (2005). *Catastrophe Modeling: A New Approach to Managing Risk*, Chapter 2. Springer, New York.
3. Kunreuther, H. Meyer, R., and van den Bulte, C. (2004). *Risk Analysis for Extreme Events: Economic Incentives for Reducing Future Losses*. NIST Monograph GCR 04-871.
4. Stone, J. (1973). A theory of capacity and the insurance of catastrophic risks: part I and part II. *J. Risk Insur.* **40**, 231–243, (Part I); 339–355, (Part II).
5. Kunreuther, H., Meszaros, J., Hogarth, R., and Spranca, M. (1995). Ambiguity and underwriter decision processes. *J. Econ. Behav. Organ.* **26**, 337–352.
6. American Re. (2002). *Topics: Annual Review of North American Natural Catastrophes 2001*.
7. Dionne, G., Doherty, N., and Fombaron, N. (2000). Adverse selection in insurance markets. In *Handbook of Insurance*, G. Dionne, Ed. Chapter 7. Kluwer, Boston.
8. Henriet, D. and Michel-Kerjan, E. (2006). *Optimal Risk-Sharing under Dual Reversed Asymmetry of both Information and Market Power: A Unifying Approach*, Working Paper,

[11]For a more detailed discussion of this proposal see [27].

Center for Risk Management and Decision Processes, The Wharton School, Philadelphia, PA.

9. Lecomte, E. and Gahagan, K. (1998). Hurricane insurance protection in Florida. In *Paying the Price: The Status and Role of Insurance Against Natural Disasters in the United States*, H. Kunreuther and R. Roth Sr., Eds. Joseph Henry Press, Washington, DC, pp. 97–124.
10. Francis,T. (2005). CEO says allstate adjusts storm plan. Interview of Edward Liddy. *Wall St. J.* C1–C3.
11. Harrington,S. E. and Niehaus,G. (2001). Government insurance, tax policy, and the affordability and availability of catastrophe insurance. *J. Insur. Regul.* **19**(4), 591–612.
12. Best, A. M. (2006). *Methodology: Catastrophe Analysis in AM Best Ratings*, April.
13. Insurance Journal. (2006). *S&P to Implement New Way to Assess Insurer Cat Risk*, March 31, 2006.
14. Klein, R. (1995). Insurance regulation in transition. *J. Risk Insur.* **62**, 263–404.
15. Grace, M., Klein, R., and Liu, Z. (2005). Increased hurricane risk and insurance market responses. *J. Insur. Regul.* **24**, 2–32.
16. Klein, R. W. (2006). *Catastrophe Risk and the Regulation of Property Insurance Markets*, working paper.Georgia State University, November for a more detailed discussion of insurance regulatory policies in general and specific to natural disaster risk.
17. Pasterick, E. (1998). The national flood insurance program. In *Paying the Price: The Status and Role of Insurance Against Natural Disasters in the United States*, H. Kunreuther and R. Roth Sr., Eds. Chapter 6. Joseph Henry Press, Washington, DC.
18. Roth, R., Jr. (1998). Earthquake insurance protection in California. In *Paying the Price: The Status and Role of Insurance Against Natural Disasters in the United States*, H. Kunreuther and R. Roth Sr., Eds. Chapter 4. Joseph Henry Press, Washington, DC.
19. Risk Management Solutions. (2004). *The Northridge, California Earthquake. A 10-Year Retrospective*.
20. Strauss, A. (2005). *Terrorism Third Party Liability Insurance for Commercial Aviation, Federal Intervention in the Wake of September 11* . The Wharton School, Center for Risk Management and Decision Processes, Philadelphia, PA.
21. Kunreuther, H. and Michel-Kerjan, E. (2004). Challenges for terrorism risk insurance in the united states. *J. Econ. Perspect.* **18**(4), 201–214.
22. Kunreuther, H. and Michel-Kerjan, E. (2005). *Insurability of (mega)-Terrorism, Report for the OECD Task Force on Terrorism Insurance, in OECD (2005)*, July 5, Terrorism Insurance in OECD Countries, Organization for Economic Cooperation and Development, Paris.
23. U.S. Congress. (2002). *Terrorism Risk Insurance Act of 2002* . HR 3210.Washington, DC, November 26.
24. Michel-Kerjan, E. and Pedell, B. (2006). How does the corporate world deal with mega-terrorism? Puzzling evidence from terrorism insurance markets. *J. Appl. Corp. Finance* **18**(4), 61–75.
25. Michel-Kerjan,E. and deMarcellis-Warin,N. (2006). Public-private programs for covering extreme events: the impacts of information distribution and risk sharing. *Asia Pac. J. Risk Insur.* **1**(2), 21–49.
26. Kunreuther, H. (1968). The case for comprehensive disaster insurance. *J. Law Econ.*
27. (a) Kunreuther, H. (2006). Has the time come for comprehensive natural disaster insurance? In *On Risk and Disaster*, R. Daniels, D. Kettl, and H. Kunreuther, Eds. University of Pennsylvania Press, Philadelphia, PA; (b) Kunreuther, H. and Michel-Kerjan E. (in press). Improving homeland security in the wake of large-scale disasters: would risk-based all-hazard disaster insurance help in the post-Katrina world? *Economic and Risk Assessment of Hurricane Katrina*, Routledge.

# QUANTITATIVE REPRESENTATION OF RISK

BILAL M. AYYUB AND MARK P. KAMINSKIY
*Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland*

## 1 INTRODUCTION

Risk representation is defined as the description of risk in an appropriate manner for a decision-making situation. The representation of risk that would retain an appropriate level of information is essential to decision makers, and should be tailored for specific applications and types of decision-making situations under consideration.

Risk is defined as the potential for loss or harm to systems due to the likelihood of an unwanted event and its adverse consequences. The term *potential* is used in the definition to imply uncertainty as a central notion to risk. Uncertainties are inherent in both the likelihood of the unwanted event and in the consequences including their nature and severity. Loss or harm includes all negative consequences, including both tangible effects such as human casualties and/or financial losses and less tangible impacts such as political instability, decreased morale, and reduced operational effectiveness. The term *event* represents the occurrence that triggers scenarios and the consequences. While consequences of an event can be both advantageous and/or adverse, risk considers only the adverse consequences—meaning that risk is a function of perspective. Risk to us is opportunity to our adversaries. The term *likelihood* refers to both the occurrence of the event and its potential adverse consequences. Probability is a quantitative measure of likelihood [1].

Each of homeland security risks can be classified into three components of threat, vulnerability, and potential consequences that should be analyzed in a systems framework. Analytically and computationally, risk assessment requires the following estimates:

- threat analysis to define and assess the likelihood of an attack by an adversary according to some threat scenario;
- vulnerability analysis to assess the likelihood that the adversary attack is successful (i.e. overcoming the security and physical protection systems) given an attack; and
- consequence analysis to assess the consequences given a successful adversary attack.

Risk assessment can involve a range of qualitative and quantitative methods [1]. For quantitative analysis, the first two likelihoods may be assessed as probabilities and multiplied to calculate the probability of an adversary's successful attack. In risk applications (e.g. natural hazards) and homeland security applications, combining these three elements into a single measure of risk would deprive a decision maker from the full information that might be critical for rational decision making.

The representation of risk that would retain an appropriate level of information is essential to decision makers, and should be tailored for specific applications and types of decision-making situations under consideration.

The above scenario can be viewed as a cause and, if it occurs, may result in consequences with severities. The representation of risk is essential for risk communication and decision making. The objective of this article is to provide a summary of risk representation methods, including random variables relating to losses, occurrence rates, and moments and parameters. The methods include qualitative and quantitative representations of risk. Loss exceedance probability (EP) distributions, loss exceedance rates, probability density functions (PDFs), and descriptive point estimates are included for this purpose. Computational examples are used to illustrate these methods. The selection of an appropriate method should be based on the decision-making situation under consideration.

## 2 RISK MEASURES AND REPRESENTATION

Risk results from an event or sequence of events, called a *scenario*, with occurrence likelihood. A scenario can be viewed as a cause and, if it occurs, may result in consequences with severities, called *losses*. A risk measure accounts for both the probability of occurrence of a scenario and its consequences. Both the probability and consequences could be uncertain. This section provides fundamental cases for representing risks to prepare readers for subsequent sections.

### 2.1 Fundamentals of Risk Representation

The representation or display of risk may include risk matrices (or tables), risk plots (or graphs), and probability distributions of adverse consequences in the form of cumulative probability distributions or EP distributions [1]. The choice of representation techniques depends on the type of analysis (qualitative or quantitative) and stakeholder/decision maker preferences. The risk display becomes the baseline for comparison of the effectiveness of risk management alternatives. It is important to recognize that the probability of the event is not plotted as a function of its potential adverse consequences. Rather, the two elements of risk are plotted separately on their own axes. Uncertainties in both the elements of risk are represented by line segments, which form a cross that depicts the risk of the event.

### 2.2 Probability Trees for Defining Scenarios

Probability trees can be used to develop scenarios and associated branch probabilities ($p_i$) and consequences (i.e. losses) $L_i$. In this section, simple cases are used to illustrate the development of scenarios. Figure 1 shows a generic probability tree related to homeland security applications. A sequence of events constitutes a scenario in this tree. By following a series of branches under each of the headings shown in the figure, a scenario can be identified (or developed). The scenario probability as indicated in the figure can be evaluated as the product of the conditional probabilities of the branches appearing in the scenario. The conditional probability for a branch is the probability of occurrence of the branch under the assumed conditions that all the branches leading to this particular branch in the scenario have occurred. This product can be viewed as the best (or point)

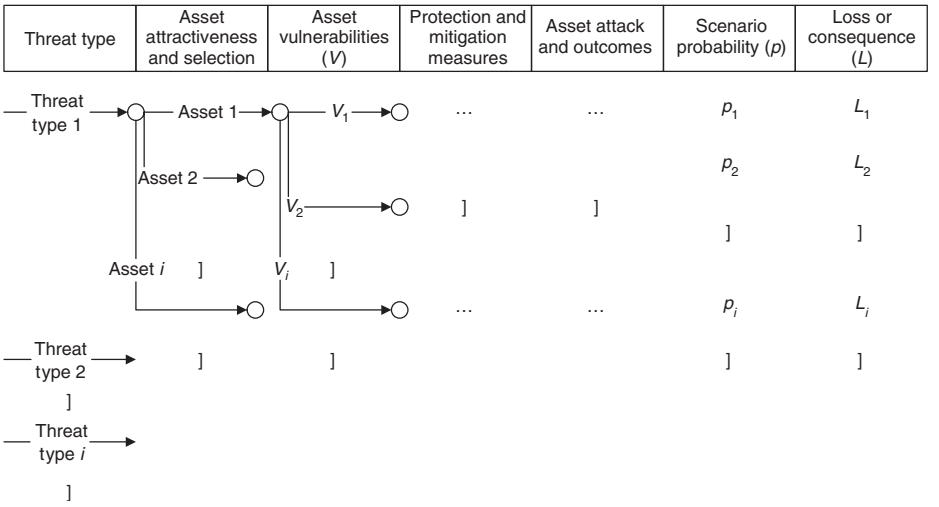



**FIGURE 1** Construction of a generic probability tree.

estimate of the scenario probability. The loss or consequence associated with a scenario is also conditional on the occurrence of the scenario, and can be provided either as a best (i.e. point) estimate or a probability distribution. A percentile interval can be used instead, and converted into a probability distribution once a distribution type is assumed.

### 2.3 One-Scenario Representation

For a scenario $i$, the risk pair $(p_i, L_i)$ can be represented in any of the forms provided in Figure 2 reflecting the type of data available: (i) point estimates, (ii) interval estimates, and/or (iii) probability distributions. A percentile interval can be used, and converted to a probability distribution once a distribution type is assumed.

### 2.4 Multiscenario Representation

Probability trees similar to Figure 1 lead to multiscenario cases, which is a simple generalization of the case of one-scenario shown in Figure 2. All these scenarios are based on point estimate data types. For other data types, that is, intervals or probability distributions, they can be converted to point estimates. Uncertainty modeling can be used at the end of any analytical process, such as probability exceedance distributions presented in the following section, to propagate these uncertainties based on the data types to assess their effects on the outcomes of the analytical process.

## 3 EXCEEDANCE PROBABILITY DISTRIBUTIONS

### 3.1 Definitions

Risk can be represented using *EP distributions* (*or curves*) [2]. The EP curve gives the probabilities of specified levels of loss exceedance. The notion "losses" can be expressed in terms of dollars of damage, number of fatalities, casualties, and so on.

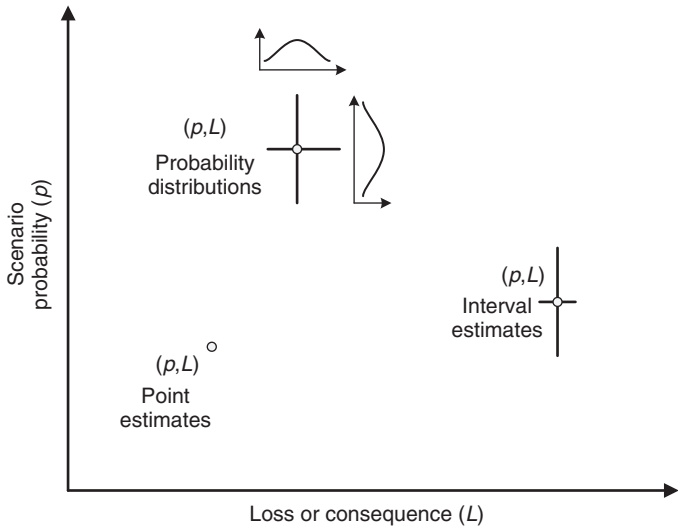



**FIGURE 2** Risk plots and data types.

The construction of an EP curve begins with the data that might be empirically obtained or produced using simulation methods. An example by Kunreuther et al. [2] illustrates the empirical construction of an EP curve based on a set of loss-producing events. In this example, an EP curve is constructed for a portfolio of residential earthquake policies in Long Beach, California, and based on dollar losses to homes in Long Beach from earthquake events. The objective is to combine these loss-producing events, and then to determine respective return periods and annual probabilities of exceeding losses of different magnitudes. On the basis of these estimates, the EP, or mean EP, is developed as shown in Figure 3. According to this figure with a particular loss $L_i$, the curve provides the probability that the loss as a random variable exceeds $L_i$ with the respective $y$-axis value $p_i$. Thus the $x$-axis measures the loss value in given units, and the respective $y$-axis value is the probability that the loss exceeds a given value.

Using an EP curve, the effects of countermeasures and mitigation strategies can be examined based on the shifts of the EP curve downward. In other words, the EP curves can be used to estimate benefit–cost effect of these strategies.

The EP curves can also express uncertainty associated with the probability of occurrence of an undesirable event and the magnitude of the respective loss as a result of uncertainties in specified values as inputs. Such uncertainties can be expressed using the *percentile* EP curves. For example, the 5th and 95th percentile EP curves depict uncertainties associated with losses as well as the uncertainties associated with respective probabilities. In our case, the EP curve depicting uncertainties in losses would show the interval $(L_i^{0.05}, L_i^{0.95})$, which can include the loss related to a given mean value $L_i$ associated with probability $p_i$. Similarly, the EP curve depicting uncertainties in probabilities shows the percentiles $(p_i^{0.05}, p_i^{0.95})$ associated with loss mean value $L_i$.

It should be noted that due to data availability, constructing EP curves is much easier for the problems dealing with natural disasters (such as earthquakes and floods) compared to the risk assessment problems relating to homeland security where data are limited or nonexistent.

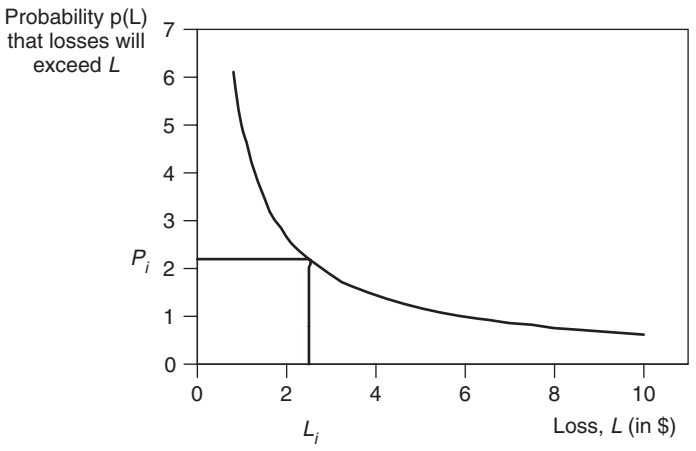



**FIGURE 3** Sample mean exceedance probability curve [2].

### 3.2 Constructing Exceedance Probability Distributions

The available data are assumed to be collected as a set of $n$ disaster events, $E_i$, $i = 1, 2, \ldots, n$ with respective annual probabilities of occurrence $p_i$. Also, estimates of the respective losses ($L_i$) associated with these events are made after the occurrence of these events. Coming back to the example discussed in the previous section, the events are earthquakes with magnitudes that can be physically measured in the form of ground accelerations. If one deals with floods, the respective events can be physically defined as well, for example, water-level elevation. An example of such earthquake data including 15 events is given in Table 1.

Some of the entries in Table 1 are for events having equal (or almost equal) values of losses, but with respective annual probabilities that are different, such as for $Event_{10}$, and $Event_{11}$. These two events correspond to earthquakes of different magnitudes occurring, perhaps, at different locations with different populations at risk and producing the same loss estimates.

In order to apply the notions of annual probability and random variable, the disaster events must be, to an extent, *repeatable*, which is, to an extent, true in the case of natural disasters such as earthquakes, floods, hurricanes, and so on. On the other hand, it should be noted that identification of events is not necessarily straightforward in the case of terrorist actions. Nevertheless, the respective events can be identified. For example, they might be defined as explosions committed in public communication systems, like metro, railway stations, and so on.

The loss associated with a given disaster event can be treated as a continuous random variable, whereas the number of events occurring in some specified period of time, such as a year, can be treated as a discrete random variable. Table 1 provides loss data estimates for these events. These loss values can be considered as best estimates for the respective events, and can be treated as central-tendency point estimates of the continuous random variable.

For a set of natural disaster events, $E_i$, $i = 1, \ldots, n$, each event has an annual probability of occurrence, $p_i$, and an associated loss estimate, $L_i$. The number of events per year is not limited to one; numerous events can occur in the given year. Fifteen such

**TABLE 1 Constructing Exceedance Probability Curves**

| Event ($E_i$) | Annual Probability of Occurrence ($p_i$) | Loss ($L_i$) | Exceedance Probability ($EP(L_i)$) | $E(L) = (p_i L_i)$ | Rate of Occurrence ($\lambda(L_i)$) |
|---|---|---|---|---|---|
| $Event_1$ | 0.002 | 25,000,000 | 0.0020 | 50,000 | 0.0020 |
| $Event_2$ | 0.005 | 15,000,000 | 0.0070 | 75,000 | 0.0070 |
| $Event_3$ | 0.010 | 10,000,000 | 0.0169 | 100,000 | 0.0170 |
| $Event_4$ | 0.020 | 5,000,000 | 0.0366 | 100,000 | 0.0373 |
| $Event_5$ | 0.030 | 3,000,000 | 0.0655 | 90,000 | 0.0677 |
| $Event_6$ | 0.040 | 2,000,000 | 0.1029 | 80,000 | 0.1086 |
| $Event_7$ | 0.050 | 1,000,000 | 0.1477 | 50,000 | 0.1598 |
| $Event_8$ | 0.050 | 800,000 | 0.1903 | 40,000 | 0.2111 |
| $Event_9$ | 0.050 | 700,000 | 0.2308 | 35,000 | 0.2624 |
| $Event_{10}$ | 0.070 | 500,000 | 0.2847 | 35,000 | 0.3351 |
| $Event_{11}$ | 0.090 | 500,000 | 0.3490 | 45,000 | 0.4292 |
| $Event_{12}$ | 0.100 | 300,000 | 0.4141 | 30,000 | 0.5346 |
| $Event_{13}$ | 0.100 | 200,000 | 0.4727 | 20,000 | 0.6400 |
| $Event_{14}$ | 0.100 | 100,000 | 0.5255 | 10,000 | 0.7455 |
| $Event_{15}$ | 0.283 | 0 | 0.6597 | 0 | 1.0779 |

events are listed in Table 1, ranked in descending order of the amount of loss. Event 15 was defined to be encompassing of all other zero-loss events so that the set of all events is collectively exhaustive. In order to keep this example simple, these events were chosen so that the set is exhausted, that is, the sum of the probabilities for all the events equals one.

The events in Table 1 are assumed to be independent Bernoulli random variables with the following probability mass functions:

$$P(E_i \text{ occurs}) = p_i \tag{1a}$$

$$P(E_i \text{ does not occur}) = 1 - p_i \tag{1b}$$

The expected loss ($E$) for a given event $E_i$ is

$$E(L) = p_i L_i$$

Indexing the events in reverse order of their losses (i.e. $L_i \geq L_{i+1}$), and assuming that only one disaster can occur during a given year, the mean (expected) EP for a given loss $EP(L_i)$ can be found as

$$\begin{aligned} EP(L_i) &= P(L > L_i) = 1 - P(L \leq L_i) \\ &= 1 - \prod_{j=1}^{i} (1 - p_j) \end{aligned} \tag{2}$$

Equation (2) shows that the resulting annual EP that the loss exceeds a given value $L_i$ is one minus the probability that losses below or equal the value $L_i$ have not occurred.

The *EP* curve based on the data from Table 1 is shown in Figure 3. In general, the summation of the probabilities of Events 1–14 can exceed one, since they are independent Bernoulli events.

### 3.3 Curve Fitting to Exceedance Probabilities

Procedures to fit a curve to EPs, that is, mainly applied to insurance problems, are not considered by Kunreuther et al. [2]. In contrast to the insurance applications, for the problems related to the risk representation for homeland security, fitting of EP curves is essential due to data unavailability or limited availability that might represent the results of expert opinion elicitation processes.

In this section, a special approach to fitting the EP curves is suggested, assuming that limited data is available in the form discussed in the previous section, that is, as a set of couples of $p_i$ and $L_i$.

The suggested choice of EP curve functional form is based on meeting general trends expected for probabilistic reasoning. The function used for EP curve fitting must be simple and concave upward (Figures 3 and 4). Such function should be positive and limited from the above by unity. These requirements are satisfied for the survivor function of Pareto distribution, which (for the random variable $L$) can be written as

$$P(L) = \left(\frac{d}{L}\right)^{c} \tag{3a}$$

where $c$ and $d$ are the positively defined shape and scale parameters, respectively. It should be noted that the Pareto distribution has support on $L > d$, which is very important from the standpoint of the parameters estimation. Another form of the Pareto distribution having support that $L > 0$ is given by the following survivor function [3, 4]:

$$P(L) = \left(1 + \frac{L}{d}\right)^{-c} \tag{3b}$$

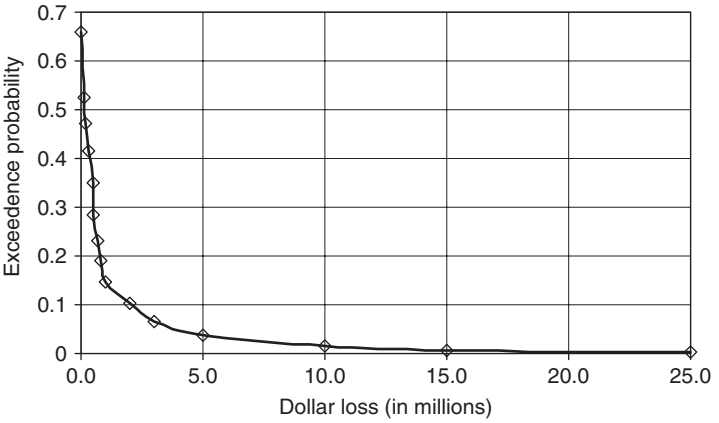



**FIGURE 4** Mean exceedance probability curve based on data from Table 1.

The Pareto distribution is used to model variables relating to a random time to failure. For example, consider a population of components with an exponential time to failure ($T$) distribution. The parameter of the exponential distribution ($\lambda$) is supposed to be random and distributed according to the gamma distribution with parameters $\alpha$ and $k$. A new random variable closely related to the time to failure $T$ is introduced as $\tau = (T/\alpha + 1)$. It can be shown that the introduced variable $\tau$ is distributed according to the Pareto distribution with the scale parameter equal to 1, and the shape parameter equal to $k$.

It is also interesting to note that Eq. (3a), at least formally, coincides with the model used for fitting of the so-called $S-N$ or Wohler curves, where $S$ is stress amplitude and $N$ is time to failure in cycles, such that:

$$N = kS^{-b} \tag{4}$$

where $b$ and $k$ are material parameters estimated from the data. Because of the probabilistic nature of fatigue life, one has to deal with not only one $S-N$ curve, but with a family of $S-N$ curves so that each curve is related to a probability of failure as the parameter of the model. These curves are called $S-N-P$ curves or curves of constant probability of failure.

Figure 5 displays the results of Eq. (3a) loglinear least squares (LS) fitting based on the data given in Table 1. The results of Eq. (3a) nonlinear LS fitting using Gauss–Newton method for the same data are shown in Figure 6. Finally, the results of fitting the model provided in Eq. (3b) nonlinear LS fitting using Gauss–Newton method for the same data are shown in Figure 7. The estimates of the models parameters and $R^2$ statistics

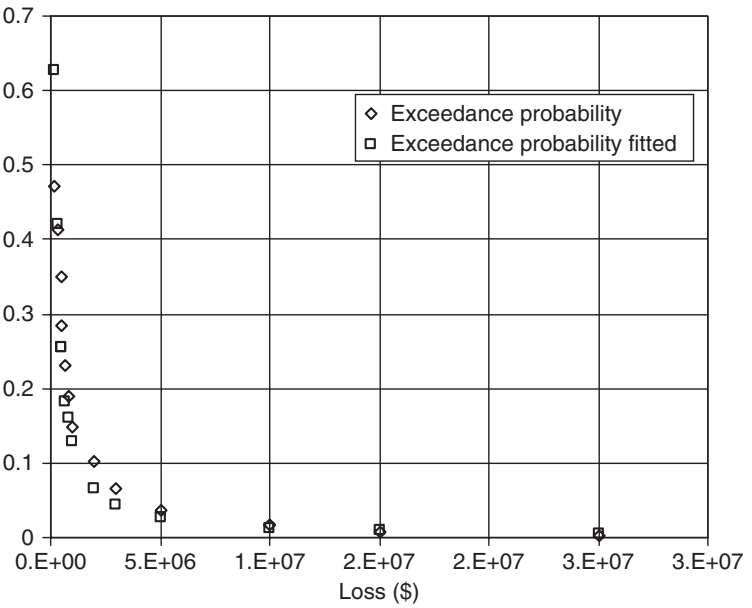



**FIGURE 5** Results of Eq. (3a) loglinear LS fitting for data given in Table 1.

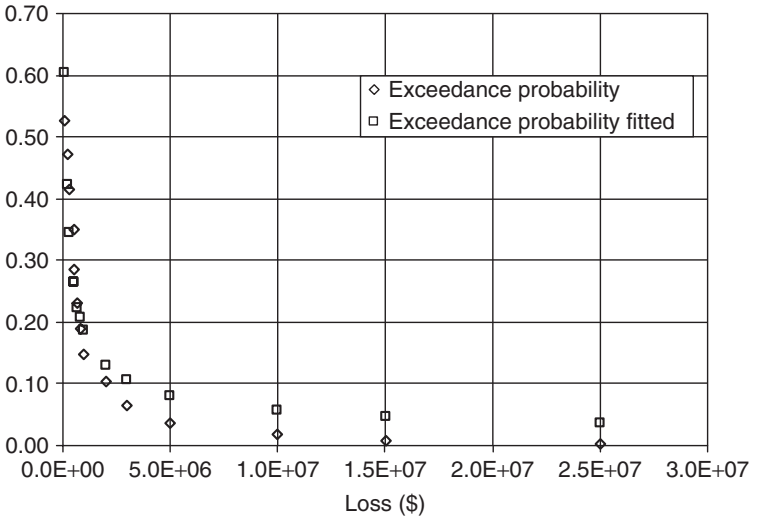



**FIGURE 6** Results of Eq. (3a) nonlinear LS fitting using Gauss–Newton method for data given in Table 1.

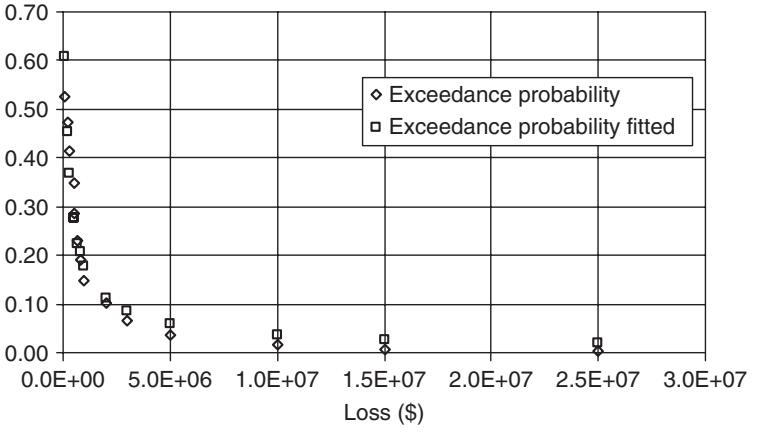



**FIGURE 7** Results of Eq. (3b) nonlinear LS fitting using Gauss–Newton method for data given in Table 1.

(representing the fraction of variation explained by the fitted model) for each fitted model are given in Table 2. By analyzing the table, one might draw a conclusion that Eq. (3b) provides the best fit.

## 4 OCCURRENCE RATES OF EVENTS

The objective of this section is to relate the EP curves to the rates of occurrence of loss events that are of particular interest [1, 5].

**TABLE 2 Parameters Estimates of Models**

| Model | Fitting Procedure | Estimates of Parameters | | $R^2$ |
|---|---|---|---|---|
| | | $c$ | $d$ | |
| Eq. (3a) | Loglinear LS | 0.984 | 124,514 | 0.930 |
| Eq. (3a) | Nonlinear LS | 0.512 | 37,256 | 0.934 |
| Eq. (3b) | Nonlinear LS | 0.724 | 101,412 | 0.959 |

### 4.1 Nonrandom Rates

At this point, it should be noted that any point of the mean EP curve $EP(L)$ can be related to an event resulting in loss $>L$. These events could be related to specific real events.

In order to assess how the losses are evolving in time, one needs to recall that, strictly speaking, the considered *EPs* are, in essence, *annual EPs*. The annual probability is considered as the probability (equal to EP) that a given event occurs in the time interval (0, 1], where 1 is 1 year. The *annual probabilities of occurrence* ($p$) can be related to the *rate of occurrence of disaster events* resulting in a loss exceeding $L$ in a stochastic process. In the situation considered, the only reasonable model for the stochastic process is the homogeneous Poisson process.

It should be noted that the homogeneous Poisson process is a widely used model for the insurance and security applications. It is reasonable to assume that the cumulative distribution function (CDF) is exponential that is the time between events, each resulting in loss $>L$, is distributed as a function of time according to the exponential distribution. For any value of loss $L_i$ the parameter $\lambda$ of this distribution can be simply evaluated as

$$\lambda(L_i) = -(1/t)\ ln(1 - EP(L_i)) \tag{5}$$

where $t = 1$ year. The parameter $\lambda(L)$ can be considered as the rate of occurrence. Its numerical values for the above discussed example are exhibited in the right column of Table 1. One can notice that the values of $\lambda(L_i)$ are very close to $p_i$ for the small values of $p_i$. The higher the value of $p_i$, the wider the difference between $p_i$ and $\lambda(L_i)$. It can be easily explained using the two-term Tailor expansion: $EP = 1 - \exp(-\lambda t) = 1 - \exp(-p)$. For $p \to 0$, one gets $EP \approx 1 - 1 + p = p$.

The occurrence rate of the events for which loss lies in a two-sided interval can be found in the following way. The situation that the rate $\lambda$ related to the event associated with a loss interval $(L_l, L_u)$ is considered. By introducing the width of the respective probability interval $\Delta = EP(L_u) - EP(L_l)$, Eq. (5) takes the form

$$\begin{aligned} \lambda(\Delta) &= -(1/t)\ \ln(1 - (EP(L_u) - EP(L_l)) \\ &= -(1/t)\ \ln(1 - \Delta) \end{aligned} \tag{6}$$

where $t = 1$ year for the annual probabilities considered throughout this section.

In order to better reveal the probabilistic meaning of Eq. (6), let us make a rather realistic assumption that $\Delta$ is small enough (e.g. $\Delta = 0.1$) such that the Taylor expansion

for $\ln(1 - \Delta)$ can be applied. The respective approximation yields

$$\lambda(\Delta) \approx \Delta/t \tag{7a}$$

$$\approx EP(L_l)/t - EP(L_u)/t \tag{7b}$$

$$\approx \lambda(L_l) - \lambda(L_u) \tag{7c}$$

Finally, for the complementary event that the loss does not exceed a given value $L_i$, that is, $NEP(L_i) = P(L < L_i)$, one can get the following equation for the respective occurrence rate:

$$\lambda(L_i) = -(1/t)\ \ln(1 - (1 - EP(L_i))) \tag{8}$$

### 4.2 Accumulated Loss as a Function of Occurrence Rate

The rate ($\lambda$) was initially considered as a nonrandom quantity. Randomness in the rate can be added to the model as provided by Ayyub [1].

Now let us assume that the number of event occurring during a nonrandom time interval is governed by homogeneous Poisson process. The loss associated with each event is modeled using a continuous random variable $S$ with the CDF $F_S(s)$. The CDF of the accumulated damage (loss) during a nonrandom time interval $[0, t]$ is given by

$$F(s; t, \lambda) = \sum_{n=0}^{\infty} \mathrm{e}^{-\lambda t} \frac{(\lambda t)^n}{n!} F_S^{(n)}(s) \tag{9}$$

where $F_S{}^{(n)}(s)$ is the $n$-fold convolution of $F_S(s)$. In other words, $F_S{}^{(n)}(s)$ is the probability that the total loss accumulated over $n$ events (during time $t$) does not exceed $s$. For $n = 0$, $F_S{}^{(0)}(s) = 1$ and for $n = 1$, $F_S{}^{(1)}(s) = F_S$. For $n = 2$, the twofold convolution $F_S{}^{(2)}(s)$ can be evaluated using conditional probabilities as

$$F_S^{(2)}(s) = \int_0^{\infty} F_S(s - x)\ \mathrm{d}F_S(x) \tag{10}$$

In the case of a normal probability distribution, the twofold convolution $F_S{}^{(2)}(s)$ can be evaluated as follows:

$$F_S^{(2)}(s) = P(S + S < s) = F_S(s; 2\mu, \sqrt{2}\sigma) \tag{11}$$

where $P$ is the probability and $F_S\ (s; 2\mu,\ \sqrt{2}\ \sigma)$ is the CDF of $S + S$ that can be evaluated using normal CDF of $S$ with a mean value of $2\mu$ and a standard deviation of $\sqrt{2}\ \sigma$ for independently and identically distributed losses. For other distribution types, the distribution of the sum $S + S$ needs to be used. In general for the case of $S + S$, the following special relations can be used:

- $S + S$ is normally distributed if $S$ is normally distributed;
- $S + S$ has a gamma distribution if $S$ has an exponential distribution; and
- $S + S$ has a gamma distribution if $S$ has a gamma distribution.

The threefold convolution $F_S{}^{(3)}(s)$ is obtained as the convolution of the distributions of $F_S{}^{(2)}(s)$ and $F_S(s)$ for independently and identically distributed losses represented by a normal probability distribution as follows:

$$F_S^{(3)}(s) = P(S + S + S < s) = F_S(s; 3\mu, \sqrt{3}\sigma) \tag{12}$$

Higher-order convolution terms can be constructed in a similar manner for the independently and identically distributed losses represented by a normal probability distribution as follows:

$$F_S^{(n)}(s) = P(\overbrace{S + S + \cdots + S}^{\text{n times}} < s) = F_S(s; n\mu, \sqrt{n}\sigma) \tag{13}$$

Therefore, Eq. (9) can be written for independently and identically distributed losses represented by a normal probability distribution as follows:

$$F(s; t, \lambda) = \sum_{n=0}^{\infty} e^{-\lambda t} \frac{(\lambda t)^n}{n!} F_S(s; n\mu, \sqrt{n}\sigma) \tag{14}$$

If $\lambda$ is random with the PDF $f_\lambda(\lambda)$, Eq. (9) can be modified to

$$F(s; t) = \int_0^{\infty} \left( \sum_{n=0}^{\infty} e^{-\lambda t} \frac{(\lambda t)^n}{n!} F_S^{(n)}(s) \right) f_\lambda(\lambda)\, \mathrm{d}\lambda \tag{15}$$

where $F_S^{(n)}(s)$ is the $n$-fold convolution of $F_S(s)$.

## 5 RISK DESCRIPTORS

### 5.1 Probability Distributions

As it was discussed in Section 2, an EP curve can be treated as the survivor function of the respective distribution of losses. Thus, one can write the following equation for the CDF of losses, $F(L)$,

$$F(L) = 1 - S(L) \tag{16}$$

where $S(L)$ is the fitted survivor function of losses.

It should be noted that this distribution of losses is related to 1 year, that is, it is *annual distribution* of losses. On the basis of the CDF of losses, $F(L)$, the respective PDF can be easily found.

The Pareto distribution is further used to illustrate the suggested methodology. In this case, the CDF of losses $F(L)$ takes on the following form:

$$F(L) = 1 - \left(\frac{d}{L}\right)^c \tag{17}$$

where $L > d$. The corresponding PDF of losses, $f(S)$, is given by

$$f(L) = \frac{cd^c}{L^{c+1}} \tag{18}$$

It should be noted that the above distribution parameters $d$ and $c$ are obtained as a result of the respective EP curve fitting (Section 2.3). These point estimates of the loss distribution parameters are used in the following section for evaluation of the main risk descriptors.

### 5.2 Risk Descriptors and Functions

By evaluating the PDF of losses, one can find the main loss descriptors. For example, the *mean value of loss* (*expected loss*), $E(L)$, can be evaluated as

$$E(L) = \int_0^\infty l f(l)\ \mathrm{d}l \tag{19}$$

For the Pareto distribution, mean value of loss is given by the following equation:

$$E(L) = \frac{cd}{c-1} \tag{20}$$

The *variance of loss* $Var(L)$ is evaluated as

$$Var(L) = \int_0^\infty [l - E(L)]^2 f(l)\ \mathrm{d}l \tag{21}$$

For the considered Pareto distribution, this variance is given by

$$Var(L) = \frac{cd^2}{(c-1)^2(c-2)} \tag{22}$$

Other useful descriptors such as median, percentiles, and interpercentile ranges can be obtained in a similar way.

The nonrandom hazard rates $\lambda$ associated with one-sided and two-sided loss intervals are considered in Section 4.1 and the respective formulas are given by Eqs. (5–7).

Having the annual distribution of losses (i.e. Eq. 16) available and using Eq. (9), one can estimate the accumulated random damage during time $t$, introduced in Section 3.2, as a function of time $t$ (in years) and the respective annual occurrence rate $\lambda$.

In this case, the annual occurrence rate $\lambda$ can be estimated using the Apostolakis–Mosleh estimate suggested for the rate of the precursor events of the core damage in nuclear power plants [6]

$$\lambda = \frac{N(T)}{T} \tag{23}$$

where in the case considered, $T = 1$ year, and $N(T)$ is given by

$$N(T) = \sum_{i=1}^{n} p_i$$

where $n$ is the number of events observed during time $T$ (a year) and $p_i$ are their respective probabilities.

It should be noted that the probabilities of events included in the above sum are related to the same events, which were used for constructing the respective EP curve. For example, based on Table 1, the annual occurrence rate $\lambda$ is estimated as 0.717 events per year.

If the annual occurrence rate $\lambda$ is treated as *random*, and its PDF $f(\lambda)$ is available, for example, as a result of expert opinion elicitation, the accumulated random damage can be evaluated using Eq. (15).

## ACKNOWLEDGMENTS

The authors are please to thank the anonymous reviewer and Dr Bruce Colletti for their thoughtful and constructive comments and suggestions.

## REFERENCES

1. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*. Chapman & Hall/CRC Press, London.
2. Kunreuther, H., Meyer, R., and Van den Bulte, C. (2004). *Risk Analysis for Extreme Events: Economic Incentives for Reducing Future Losses*, NIST Report GCR 04-871 National Institute of Standards and Technology (NIST).
3. Hoyland, A., and Rausand, M. (1994). *System Reliability Theory*. John Wiley & Sons, New York.
4. Frees, E., and Valdez, E. (2001). Understanding relationships using copulas. *N. Am. Actuar. J.* **2**(1), 1–25.
5. Ayyub, B. M., and McCuen, R., (2003). *Probability, Statistics and Reliability for Engineers and Scientists*, 2nd ed. Chapman & Hall/CRC Press, Boca Raton, FL.
6. Apostolakis, G., and Mosleh, A., (1979). Expert opinion and statistical evidence: an application to reactor core melt frequency. *Nucl. Sci. Eng.* **70**, 135.

## FURTHER READING

Modarres, M., Kaminskiy, M., and Krivtsov, V. (1999). *Reliability Engineering and Risk Analysis: A Practical Guide*. Marcel Dekker, New York, Basel.

Modarres, M., Martz, H., and Kaminskiy, M. (1996). The accident sequence precursor analysis: review of the methods and new insights. *Nucl. Sci. Eng.*, **123**, 238–258.

Pate-Cornell, E. (2004). On signals, response, and risk mitigation. In *Accident Precursor Analysis and Management*, J. R. Phimister, V. M. Bier, H. C. Kunreuther Eds. The National Academic Press, Washington, DC.

# QUALITATIVE REPRESENTATION OF RISK*

GARY R. SMITH
*Logical Decisions, Fairfax, Virginia*
JAMES SCOURAS
*Defense Threat Reduction Agency, Ft. Belvoir, Virginia*
ROBERT M. DEBELL
*Gaithersburg, Maryland*

## 1 INTRODUCTION

A risk representation is an attempt to describe or clarify a particular risk. A qualitative risk representation describes or clarifies without the explicit use of numbers. A qualitative risk representation can be used to communicate the results of a qualitative risk assessment or summarize a quantitative risk assessment. Qualitative risk representations can be used to describe individual risks or to compare the relative severity of different risks.

Risk can be defined as the potential for injury or loss. This definition has two parts: the potential (or likelihood) and the loss (usually called a *consequence in risk analysis*). Quantitative representations describe likelihood with probabilities and loss using numeric scales such as dollars or fatalities. Alternatively, qualitative representations can be used for the likelihood, the loss, or for the risk as a whole.

All risk representations are subject to misinterpretation. This can be due to poor definition of the risk being represented or lack of caveats regarding the underlying analysis. Qualitative risk representations are further subject to misinterpretation due to the imprecision inherent in language and due to imperfect alignment between qualitative representations and underlying quantitative assessments. It is also important to avoid the temptation to do inappropriate mathematical manipulations with qualitative risk representations. For example, one should not arbitrarily establish a rule that two "low" risks add to become a "medium" risk.

Qualitative risk representation is not a formal field of scientific study. Disciplines that touch on qualitative risk representation include risk analysis, measurement theory, psychology, sociology, and linguistics. More specialized researchers investigate risk communication, but seldom distinguish between qualitative and quantitative representations.

*The views expressed in this article represent those of the authors; they do not necessarily represent the views of any governmental or commercial entity.

## 2 VERBAL RISK REPRESENTATIONS

Verbal representations describe risk or risk components with words. We use verbal here in the sense of "communicated with words" rather than "spoken out loud". Verbal risk representations are the most common type of qualitative risk representation, but not the only one. Other types of qualitative risk representations, such as pictorial, graphical, and cartographic, are not discussed here.

The simplest verbal representations are warnings such as "smoking may be hazardous to your health". Warnings can be useful, but generally provide little information about the degree of risk or how the risk compares or relates to other risks.

More sophisticated verbal risk representations use two general approaches—scales and risk comparisons. Scales are a standardized way of describing individual risks by assigning to each risk one of a predefined set of descriptions. Risk comparisons directly compare risks with one another or with standardized reference risks.

## 3 RISK REPRESENTATIONS USING SCALES

Stevens [1] classifies scales of measurement (both verbal and numeric) into four different types—nominal, ordinal, interval, and ratio.

The simplest scale of measurement is a nominal scale or categorization. Categorizations describe the nature of the risk without attempting to describe its magnitude. For example, "chemical, biological, radiological, nuclear, and explosive" is a common risk categorization. The major limitation of categorizations is that they do not provide any ordering of risks. It is not possible to use a categorization to say that one risk is greater than another.

The next simplest scale of measurement is an ordering. More formally, orderings are called *ordinal scales*. The archetypical ordinal scale is "high, medium, and low". By definition, ordinal scales provide a partial ordering of risks. What they do not provide is an indication of the relative degree of risk. There is no way to tell how much worse a high risk is than a medium risk or whether the change from low to medium is greater or lesser than the change from medium to high. In addition, the ordering is only partial since there is no way to determine the order of two risks assigned the same scale point.

Adjusting an ordinal scale such that each scale degree represents the same amount of change results in an interval scale. Interval verbal scales have almost all of the properties of integer numbers, except that they do not have an explicit zero point. Practically, it is very difficult to develop a purely qualitative interval scale. It will usually be necessary to tie a verbal scale to an underlying numeric scale to ensure that the changes between scale points are equal.

If one of the descriptions in an interval risk scale represents zero risk, then the scale is a ratio scale. The integers are an example of a ratio scale. While the Fahrenheit and Centigrade temperature scales are interval scales since their zero points do not correspond to a complete absence of temperature, the Kelvin temperature scale is a ratio scale since its zero point *can* be interpreted that way. Ratio scales allow statements like "risk A is twice as severe as risk B".

Risk presenters are often not as careful as they should be about the type of scale they are using and the operations and inferences that are valid for each scale type. Valid

**TABLE 1 Valid Operations and Results for Scale Types**

| Scale | Valid Operations | Results |
|---|---|---|
| *Nominal* | Count | Frequency distribution |
| *Ordinal* | Greater than<br>Less than<br>Equal to | Rank<br>Median |
| *Interval* | Add<br>Subtract<br>Multiply by a constant | Mean<br>Standard deviation |
| *Ratio* | Divide elements | Ratio |

operations and results for each scale type are shown in Table 1. (The operations for simpler types are all allowed for more complex types.)

Nominal and ordinal scales should generally be verbal, since the normal rules of arithmetic cannot be applied and the use of numbers would be confusing. Interval and ratio scales should generally be numeric since arithmetic operations are allowed. Verbal interval and ratio scales would typically be tied to an underlying numeric scale and used principally for risk communication.

When using verbal scales, imprecision in the scale point descriptions can make it difficult to determine which scale point to assign. For example, *moderate* consequences to one person might be classified as *severe* by another, leading to disagreements on what should go where. Thus, verbal scales require more elaborate—sometimes quite elaborate—definitions to allow consistent assignment and interpretation.

### 3.1 Verbal Likelihood Scales

Verbal descriptions are often used to represent the first component of risk—likelihood. If the consequence is clearly defined (e.g. death), then the verbal representation of likelihood is equivalent to a verbal representation of risk.

One widely used likelihood scale was developed by Kent [2] for use in intelligence analysis. The ordinal scale, shown in Table 2, associates verbal descriptions with probability ranges. An interesting feature of this scale is that it is asymmetric, with, for example, 63–87% represented by "probable" and 20–40% represented by "probably not." Curiously, the Kent scale has some gaps in probability, notably between the categories "almost certainly not" and "probably not."

Though the Kent scale is associated with numbers, it is not an interval scale, since the scale points do not represent equal changes. Another commonly used verbal likelihood scale, the Juster scale [3], spreads its scale points much more evenly. Originally developed for use in marketing studies, the Juster scale combines an 11-point interval scale (with minor exceptions in the first and last categories) with a set of verbal descriptions and associated probabilities, as shown in Table 3. If the top and bottom scale points were redefined as "certain (100 in 100 chance)" and "no chance (0 in 100 chance)", respectively, the Juster scale would be a ratio scale.

**TABLE 2 The Kent Scale**

| Range of Probability | Verbal Description |
|---|---|
| *100%* | Certainty |
| *93% give or take about 6%* | Almost certain |
| *75% give or take about 12%* | Probable |
| *50% give or take about 10%* | Chances about even |
| *50% give or take about 10%* | Chances about even |
| *30% give or take about 10%* | Probably not |
| *7% give or take about 5%* | Almost certainly not |
| *0%* | Impossibility |

**TABLE 3 The Juster Scale**

| Score | Verbal Description |
|---|---|
| *10* | Certain, practically certain (99 in 100 chance) |
| *9* | Almost sure (9 in 10 chance) |
| *8* | Very probable (8 in 10 chance) |
| *7* | Probable (7 in 10 chance) |
| *6* | Good possibility (6 in 10 chance) |
| *5* | Fairly good possibility (5 in 10 chance) |
| *4* | Fair possibility (4 in 10 chance) |
| *3* | Some possibility (3 in 10 chance) |
| *2* | Slight possibility (2 in 10 chance) |
| *1* | Very slight possibility (1 in 10 chance) |
| *0* | No chance, almost no chance (1 in 100 chance) |

Other verbal representations that are not explicitly linked to probability numbers have been used in various settings. A difficulty with these representations is the wide range of interpretations of various terms used to describe likelihood. Numerous studies have documented this. (See Hillson [4] and Wallsten and Budescu [5] for reviews of this literature.) Hillson presents survey results from over 500 respondents that link verbal terms with the probabilities perceived to be associated with them. The results summarized in Figure 1 demonstrate a wide range of variation in interpretation of verbal probability terms. Note also some apparent inconsistencies in the responses. “Better than even”, is interpreted by some respondents, to be associated with probabilities lower than 50%. Also, “definite” and “impossible” are associated with probabilities less than 100% and greater than 0, respectively. Note that these interpretation difficulties may persist even for scales such as the Juster scale that explicitly tie words to numbers. It is not clear if users of the scale will interpret it using the numbers or using their preexisting interpretation of the words in the scale.

Verbal representations of the likelihood of a terrorist attack have also been developed. The most well known of these is the Homeland Security Advisory System administered by the US Department of Homeland Security (DHS) [6]. This system, introduced in March 2002 [7], is an ordinal scale of five colors (threat levels) and associated text descriptions, as shown in Figure 2. Although the scale refers to various levels of “risk”, this is not

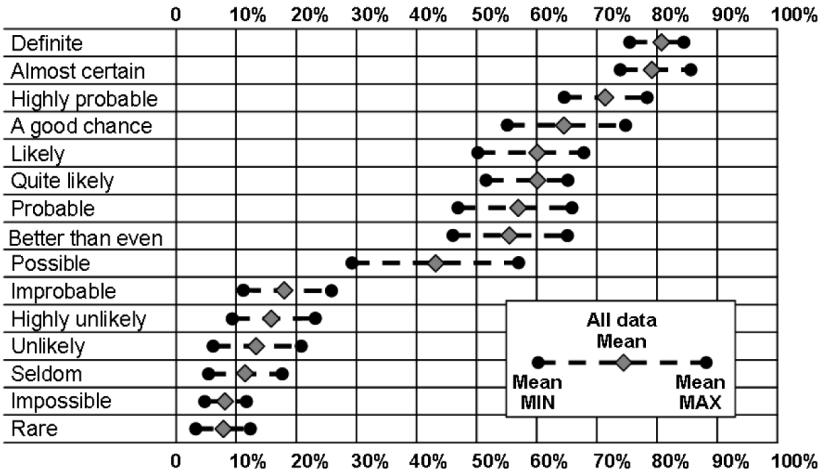



**FIGURE 1** Perceptions of probability represented by common words. Source [4].


**FIGURE 2** DHS Homeland Security Advisory System.

an accurate usage in the sense of the definition provided above. Rather, as used in the scale, risk refers to the likelihood of the associated consequence being "terrorist attacks". There are no published guidelines that establish how the threat level is determined, but DHS has developed guidelines for government agencies [8] and civilians [9] on how to respond to different announced threat levels. The United Kingdom has developed a similar five-point ordinal scale, though it is not color coded [10].

### 3.2 Verbal Consequences Scales

Verbal representations are also frequently used for describing consequences. These types of scales are perhaps most often used in association with natural disasters such as earthquakes and hurricanes.

The modified Mercalli scale [11] shown in Table 4 qualitatively describes the consequences of earthquakes. This 12-point ordinal scale is composed of a category number, a brief category description, and a longer discussion of consequences. One advantage of this type of scale is that historical earthquakes that occurred before the development of the quantitative Richter scale can be estimated on the modified Mercalli scale using contemporary descriptions. Similar intensity scales have also been developed for hurricanes (the Saffir–Simpson scale developed in 1969 by Herbert Saffir and Bob Simpson) and tornados (the Fujita scale developed in 1971 by Dr Ted Fujita [12]).

Qualitative consequences scales have also been developed in the computer industry. Microsoft [13], for example, developed the ordinal scale shown in Table 5 to characterize the potential consequences of reported vulnerabilities in Microsoft products. A consequences scale developed by Symantec is discussed in the next section.

A common problem with consequence scales for terrorist attacks is that the full spectrum of consequences includes effects on life and health, the economy, social institutions, and individual psychology. Some of these elements are quantifiable; others are not. Verbal scales with rigorous definitions are difficult in both cases. Combining these effects into a single scale is an even more daunting challenge. Thus, often only one element of consequences—typically the most readily quantifiable element such as lives lost or economic damage—is considered in a terrorism risk assessment.

### 3.3 Verbal Scales that Combine Likelihood and Consequences

Verbal representations of risk combine likelihood and consequences into a single description. This is commonly done either with a single scale or in a risk matrix with likelihood on one dimension and consequences on the other. The two methods are discussed further in the following sections.

### 3.4 One-Dimensional Combined Risk Scales

One-dimensional verbal risk representations combine likelihood and consequences information into a single scale. This is often done by developing text descriptions that include both likelihood and consequences information. An excellent example of this is the Torino impact hazard scale originally developed by Dr Richard Binzel [14, 15]. This scale indicates the risk posed by an asteroid that could potentially collide with earth. The representation consists of 11 verbal descriptions organized into five color-coded categories, as shown in Figure 3. The scale descriptions indicate the likelihood of an event, the potential consequences, and the actions that are recommended to be taken.

Similar scales have been developed for information technology (IT) risks. For example, Symantec Corporation developed a security response threat severity assessment scale [16] that evaluates the risk from threats such as viruses and worms. The scale addresses likelihood by examining the extent to which the threat is already present "in the wild" and the rate at which it spreads. The scale addresses consequences by describing the damage that the threat could cause. These three risk aspects are combined into a five-point risk scale that includes brief descriptions (very low, low, moderate, severe, and very severe),

**TABLE 4 The Modified Mercalli Scale for Earthquakes**

| Category | Category Description | Level of Damage |
|---|---|---|
| I | Instrumental | Not felt except by a very few under especially favorable conditions |
| II | Feeble | Felt only by a few persons at rest, especially on upper floors of buildings. Delicately suspended objects may swing |
| III | Slight | Felt quite noticeably by persons indoors, especially on the upper floors of buildings. Many do not recognize it as an earthquake. Standing motor cars may rock slightly. Vibration similar to the passing of a truck. Duration estimated |
| IV | Moderate | Felt indoors by many, outdoors by few during the day. At night, some awakened. Dishes, windows, doors disturbed; walls make cracking sound. Sensation like heavy truck striking building. Standing motor cars rocked noticeably. Dishes and windows rattle |
| V | Rather strong | Damage negligible. Small, unstable objects displaced or upset; some dishes and glassware broken |
| VI | Strong | Damage slight. Windows, dishes, glassware broken. Furniture moved or overturned. Weak plaster and masonry cracked |
| VII | Very strong | Damage slight moderate in well-built structures; considerable in poorly built structures. Furniture and weak chimneys broken. Masonry damaged. Loose bricks, tiles, plaster, and stones will fall. |
| VIII | Destructive | Structure damage considerable, particularly to poorly built structures. Chimneys, monuments, towers, elevated tanks may fail. Frame houses moved. Trees damaged. Cracks in wet ground and steep slopes. |
| IX | Ruinous | Structural damage severe; some will collapse. General damage to foundations. Serious damage to reservoirs. Underground pipes broken. Conspicuous cracks in ground; liquefaction. |
| X | Disastrous | Most masonry and frame structures/foundations destroyed. Some well-built wooden structures and bridges destroyed. Serious damage to dams, dikes, embankments. Sand and mud shifting on beaches and flat land. |
| XI | Very disastrous | Few or no masonry structures remain standing. Bridges destroyed. Broad fissures in ground. Underground pipelines completely out of service. Rails bent. Widespread earth slumps and landslides. |
| XII | Catastrophic | Damage nearly total. Large rock masses displaced. Lines of sight and level distorted. |

more detailed text descriptions, and references to the threat's rating on its three individual risk components.

### 3.5 Representing Consequence and Likelihood Scales Using a Risk Matrix

The risk matrix is a technique commonly employed to display risk. Its essential feature is that it does not combine the two elements of risk—likelihood and consequences. Rather,

**TABLE 5 The Microsoft Severity Rating System**

| Rating | Definition |
|---|---|
| Critical | A vulnerability whose exploitation could allow the propagation of an internet worm without user action |
| Important | A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources |
| Moderate | Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation |
| Low | A vulnerability whose exploitation is extremely difficult, or whose impact is minimal |

| | | |
|---|---|---|
| Normal (Green Zone) | 1 | A routine discovery in which a pass near the earth is predicted that poses no unusual level of danger. Current calculations show the chance of collision is extremely unlikely with no cause for public attention or public concern. New telescopic observations very likely will lead to re-assignment to Level 0. |
| Meriting Attention by Astronomers (Yellow Zone) | 2 | A discovery, which may become routine with expanded searches, of an object making a somewhat close but not highly unusual pass near the Earth. While meriting attention by astronomers, there is no cause for public attention or public concern as an actual collision is very unlikely. New telescopic observations very likely will lead to re-assignment to Level 0. |
| | 3 | A close encounter, meriting attention by astronomers. Current calculations give a 1% or greater change of collision capable of localized destruction. Most likely, new telescopic observations will lead to re-assignment to Level 0. Attention by public and by public officials is merited if the encounter is less than a decade away. |
| | 4 | A close encounter, meriting attention by astronomers. Current calculations give a 1% or greater chance of collision capable of regional devastation. Most likely, new telescopic observations will lead to re-assignment to Level 0. Attention by public and by public officials is merited if the encounter is less than a decade away. |
| Threatening (Orange Zone) | 5 | A close encounter posing a serious, but still uncertain threat of regional devastation. Critical attention by astronomers is needed to determine conclusively whether or not a collision will occur. If the encounter is less than a decade away, governmental contingency planning may be warranted. |
| | 6 | A close encounter by a large object posing a serious but still uncertain threat of a global catastrophe. Critical attention by astronomers is needed to determine conclusively whether or not a collision will occur. If the encounter is less than three decades away, governmental contingency planning may be warranted. |
| | 7 | A very close encounter by a large object, which if occurring this century, poses an unprecedented but still uncertain threat of a global catastrophe. For such a threat in this century, international contingency planning is warranted, especially to determine urgently and conclusively whether or not a collision will occur. |
| Certain Collisions (Red Zone) | 8 | A collision is certain, capable of causing localized destruction for an impact over land or possibly a tsunami if close offshore. Such events occur on average between once per 50 years and once per several 1000 years. |
| | 9 | A collision is certain, capable of causing unprecedented regional devastation for a land impact or the threat of a major tsunami for an ocean impact. Such events occur on average between once per 10,000 years and once per 100,000 years. |
| | 10 | A collision is certain, capable of causing a global climatic catastrophe that may threaten the future of civilization as we know it, whether impacting land or ocean. Such events occur on average once per 100,000 years, or less often. |

**FIGURE 3** The Torino Impact Hazard Scale.

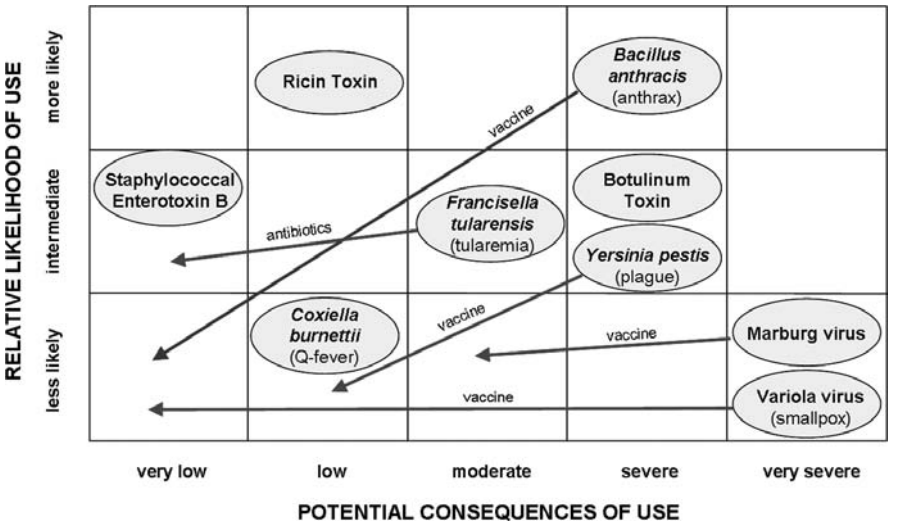



**FIGURE 4** Risk assessment for selected biological agents.

these elements define the two dimensions of the risk matrix. An example of risk matrix is presented in Figure 4 to provide focus for the discussion in this section. It displays the risks of a terrorist attack with a biological weapons agent. The practical issues in developing a risk matrix, and advantages and limitations of the resultant display are discussed.

In contrast to a quantitative risk graph that would utilize continuous numerical scales for both dimensions, a qualitative risk matrix divides both dimensions into bins defined by verbal scales. As discussed above, verbal scales often require detailed descriptions to ensure consistency.

For example, both likelihood and consequences of terrorist use of biological agents have multiple factors that need to be combined into a single scale to define the dimensions of the risk matrix.

Some of the factors that affect consequences include agent stability and persistence in the environment, infectivity, communicability, availability of clinical therapies, and duration of effects and lethality. In combining these factors into a scale, there is a trade-off between fewer and more scale points. Fewer scale points make the assessment job easier, but are less discriminating. More scale points can describe more variations in the factors, but make the matrix more complex. In practice, risk matrices typically have 3–6 rows and columns.

We have combined the consequence factors into the following five-point scale:

*Very low.* A biological agent preparation that would likely be incapacitating with little or no associated lethality. Such an agent would not likely be communicable, not persistent for more than a few days in the environment, and cause no permanent or long-lasting effects. Effective clinical treatments would be available to limit or eliminate disease effects.

*Low.* An incapacitating agent with a low level of associated lethality (less than 10%). Clinical treatments for such an agent would be available, but possibly difficult to

distribute. The agent would not likely be communicable, but could be persistent in the environment and cause only rare instances of permanent effects.

*Moderate.* A lethal agent with an associated moderate level of lethality (at least 10%, but less than 35%). Clinical treatments would likely be available, but limited by quantities or logistics for distribution. This agent could be communicable through direct contact with an infected individual, especially for prolonged periods. The agent could be stable in the environment and persistent either because it may be protected as in the case of spores or because carried by vectors.

*Severe.* An extremely lethal agent preparation with no or very limited clinical therapies available. The agent would be communicable through direct contact with infected individuals or families, and would likely be stable in the atmosphere, but not necessarily persistent for long periods.

*Very severe.* An extremely lethal agent preparation with no available effective clinical therapy. The agent would likely be highly communicable, stable, and persistent in the atmosphere, with a low infectivity.

Even this attempt to precisely define a consequences scale is inadequate since we have not covered all the different possible combinations of factors. In addition, most agents do not fit every aspect of these definitions for any single category, so the analyst will have to decide which scale point provides the closest fit for each agent. Also note that quantitative elements have sometimes crept into the qualitative descriptions.

The other dimension of the risk matrix—likelihood—has a similar set of definitional problems. The factors that affect likelihood of use for a given agent as a biological weapon include availability of materials, financial resources, expertise needed, safety precautions necessary, ease of cultivation, production and storage, practicality of dissemination, and anticipated consequences of use. Note that since the anticipated consequences will influence likelihood of use, the likelihood and consequences scales are not independent.

Continuing our example of a terrorist attack with a biological weapons agent, the following three-point scale for relative likelihood of use based on these factors is developed:

*More likely.* Agents are easy to acquire and commonly available almost anywhere in the world. These agents would also be quite easy to produce in desired quantities and would not require high-level containment. Individuals could employ simple protocols for production and would use protective clothing and available therapies such as vaccines for protection. These agents would not be communicable. The consequences for the use of such agents would vary depending on the efficacy of the preparation and the method for dissemination.

*Intermediate.* Agents are easy to acquire as these may have a wide distribution, but not necessarily global. Individuals would not have great difficulties acquiring such agents, although the agents most frequently would occur in endemic areas. The protocols needed to produce such agents would be technically challenging, but with adequate equipment and sufficient expertise, needed quantities of agent could be produced. Because clinical therapies may or may not be available and because such agents could be communicable, containment facilities would be needed. The consequences for the use of such agents would have a wide range of variation depending on the agent, as well as the ability to produce stable, effective preparations.

*Less likely.* Agents are difficult to find in the environment and difficult to produce in usable quantities. These agents would likely produce serious diseases for which

there may not be adequate therapies. Thus, these agents would require high-level containment and high-level expertise to be able to manage production or cultivation. These agents could be highly communicable, and the consequences for the use of such agents might be very severe.

Although a considerable effort is made to ensure that our scales are comprehensive and accurate, we note some shortcomings. Many of the agents are hybrids of these categories. For example, in Figure 4 *Yersinia pestis*, the causative agent of plague, is shown to be an intermediate threat on the matrix. There is no vaccine available to prophylactically protect individuals, but effective antibiotics do exist. If the plague organism is successfully disseminated, and because it is communicable from person-to-person and animal-to-person, it could potentially cause severe consequences. However, actual consequences could be significantly less, depending on whether antibiotics could be effectively distributed to the affected population. Thus, defining the risk likelihood is difficult and problematic.

Note that the likelihood scale of the risk matrix depicts relative, rather than absolute, likelihood. Although an agent assigned to a bin immediately above another means that the agent is assessed to be more likely to be used, it does not indicate *how much* more likely. Nor does the scale imply that the bins are equally separated in likelihood. Thus the likelihood scale in the risk matrix is an ordinal scale. The same is true of the consequences scale.

Once we have overcome all the difficulties in defining our risk matrix and we have placed our selected biological agents on the matrix, how can it be used? The primary value of a risk matrix is a communication tool. It provides an overview of a broad-spectrum of diverse threats and allows quick identification of the most severe relative risks (which are those in the upper right-hand corner of the matrix). This can provide a starting point for discussions on how to mitigate the risks by either reducing the consequences or reducing the likelihood of individual risks. For example, potential risk reduction measures (use of vaccines and antibiotics, which do not apply to toxins) are shown on the matrix as arrows linking the cells to an item that would be located in before and after application of the measure.

Note that we have not assigned the matrix cells to levels on an overall risk scale that combines likelihood and consequences. The reasons for this are discussed further in the next section.

### 3.6 Caveats about Combining Qualitative Risk Scales

Many qualitative risk analyses develop qualitative scales for likelihood and consequences, and then combine those scales to arrive at an overall qualitative risk scale [17, 18]. A typical approach is shown in Table 6, where three-level qualitative scales for likelihood and consequences are combined into a three-level qualitative scale for overall risk. Of course, information is necessarily lost when two pieces of data are combined into one. This is especially problematic in risk assessment since the underlying concepts of likelihood and consequences are more easily comprehended than the abstract concept of risk.

In the table, the level of the likelihood scale is determined by the row and the level on the consequences scale is determined by the column. The word in each cell is the level on the overall risk scale. As was demonstrated by Cox et al. [19], even in this simple case reasonable assignments of qualitative labels to likelihoods and consequences can

**TABLE 6 Example of Combining Two Qualitative Scales into an Overall Qualitative Risk Scale**

| | | *Consequences* | | |
|---|---|---|---|---|
| | | ***Low*** | ***Medium*** | ***High*** |
| ***Likelihood*** | ***High*** | Medium | High | High |
| | ***Medium*** | Low | Medium | High |
| | ***Low*** | Low | Low | Medium |

result in the same label for risk being assigned to quite different underlying situations. One remedy to this problem is to use formal elicitation techniques to identify the relative rankings of the different combinations of likelihood and consequences.

## 4 RISK COMPARISONS

Many individuals find it difficult to intuitively understand probability and risk estimates. Because of this, estimates are often presented as comparisons to other, more familiar and therefore presumably better known and understood, risks. Comparisons are an ordinal representation of risk that can be considered qualitative since ordering is the only operation that is used. Risk comparisons can be completely verbal without specifying the underlying risk. For example, the risk of dying from lung cancer is greater for smokers than nonsmokers. In practice, however, the risks are generally presented as part of the comparison if they are known.

Hoerger [20] states that providing a sense of perspective about risks being estimated through analogy is a desirable attribute of a risk assessment report. Fiering and Wilson [21] describe various methods used for estimating risk by comparisons with other similar risks. Common examples are the use of results in laboratory animals to estimate the analogous risk in humans and the use of past history as an analogy for the future. They state that the process of using the analogy introduces another layer of uncertainty in representing risk.

Comparative risk representations can be problematic if the comparisons are not appropriate. Inappropriate comparisons include comparing voluntary risks (such as skydiving) with nonvoluntary risks (such as air pollution) and comparing risks with personal control (such as driving) with uncontrollable risks (such as flying in a commercial aircraft) [22].

Covello et al. criticize commonly used risk comparisons such as comparisons to the risk of death in traffic accidents [23]. They developed five categories, shown in Table 7, that order comparisons from most to least suitable.

The usefulness and acceptability of a risk comparison depend on the rank of the comparison as defined in Table 7, the context of the comparison, and the audience of the comparison. If the comparison is made simply to give a feel for the magnitude of the numbers, then wider latitude should be granted. If the comparison is made for decision-making purposes, for example, to determine acceptability or to prioritize mitigation measures, a greater effort to ensure that the risks are truly comparable should be made.

**TABLE 7 Categories for Risk Comparisons Developed by Covello et al [23]**

*First-Rank Risk Comparisons* (most acceptable)
- a. Comparisons of the same risk at two different times
- b. Comparisons with a standard
- c. Comparisons with different estimates of the same risk

*Second-Rank Risk Comparisons* (less desirable)
- a. Comparisons of the risk of doing and not doing something
- b. Comparisons of alternative solutions to the same problem
- c. Comparisons with the same risk as experienced in other places

*Third-Rank Risk Comparisons* (even less desirable)
- a. Comparisons of average risk with peak risk at a particular time or location
- b. Comparisons of the risk from one source of a particular adverse effect with the risk from all sources of that same adverse effect

*Fourth-Rank Risk Comparisons* (marginally acceptable)
- a. Comparisons of risk with cost or of one cost/risk ratio with cost/risk ratio
- b. Comparisons of risk with benefit
- c. Comparisons of occupational with environmental risks
- d. Comparisons with other risks from the same source
- e. Comparisons with other specific causes of the same disease, illness, or injury

*Fifth-Rank Comparisons* (rarely acceptable—use with extreme caution!)
- a. Comparisons of unrelated risks

## 5 CONCLUSIONS

Natural language is the medium used for most qualitative risk representations. This provides both advantages and disadvantages. The advantages include simplicity and widely used terminology. However, care must be exercised in the use of qualitative risk representations. Audiences often have differing understandings of common risk and probability terms and misunderstandings will occur unless, and perhaps even if, the precise meaning of the terms used is explained.

Useful verbal scales have been developed for both likelihood and consequences. These scales must be tailored to the particular risk being discussed. When developing scales, a balance must be struck between fully describing multiple relevant factors and conciseness. Ordinal verbal scales are common, but conclusions drawn from them are limited to those based on counting and rank ordering.

The risk matrix is a useful technique for presenting likelihood and consequence in a single display without aggregating them. Aggregation of consequence and likelihood scales is not recommended unless care is taken to ensure the aggregated scale does not obscure relevant information.

Risk comparisons are commonly used to place unfamiliar risks in the context of more familiar risks. When comparing risks, the comparison must be as close as possible for

results to be accepted. In particular, comparisons of risks with very different levels of acceptability (e.g. voluntary vs. involuntary risks) are less likely to be valid.

## REFERENCES


1. Stevens, S. S. (1946). On the theory of scales of measurement. *Science* **103**, 677–680.
2. Kent, S. (1964). Words of estimative probability. *Stud. Intell.* **8**, 49–65.
3. Juster, F. T. (1966). *Consumer Buying Intention and Purchase Probability*. National Bureau of Economic Research, Columbia University Press, Los Angeles, CA.
4. Hillson, D. A. (2005). Describing probability: the limitations of natural language. *Proceedings of the EMEA PMI Global Congress*, Edinburgh, UK.
5. Wallsten, T. S., and Budescu, D. V. (1995). A review of human linguistic probability processing: general principles and empirical evidence. *Knowl. Eng. Rev.* **10**, 43–62.
6. U.S. Department of Homeland Security. (2006). Web site, http://www.dhs.gov/dhspublic/display?theme=29.
7. Ridge, T. (2006). Remarks quoted in White House press release. March 12, 2002.
8. U.S. Department of Homeland Security. (2006). Web site, http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0046.xml.
9. U.S. Department of Homeland Security. Citizen Guidance on the Homeland Security Advisory System. Retrieved from http://www.dhs.gov/xlibrary/assets/CitizenGuidanceHSAS2.pdf, October 16, 2008.
10. Reid, J. (2006). *Threat Levels: the System to Assess the Threat from International Terrorism*. The Stationary Office, Norwich, UK.
11. Wood, H. O., and Neumann, F. (1931). Modified Mercalli intensity scale of 1931. *Bull. Seismol. Soc. Am.* **21**, 277–283.
12. Fujita, T. T. (1971). *Proposed Characterization of Tornadoes and Hurricanes by Area and Intensity*, Satellite and Mesometeorology Research Project Report 91, The University of Chicago.
13. Microsoft Corporation. (2006). Web site, http://www.microsoft.com/technet/security/bulletin/rating.mspx.
14. Binzel, R. P. (1995). A near-earth object hazard index. Near-Earth Objects, the United Nations International Conference. *Proceedings of the International Conference held April 24–26*, New York; Remo, J. L. Eds. *Ann. N.Y. Acad. Sci.* 822, 545.
15. Morrison, D., Chapman, C. R., Steel, D., and Binzel R. P. (2004). *Impacts and the Public: Communicating the Nature of the Impact Hazard. Mitigation of Hazardous Comets and Asteroids*, M. J. S. Belton, T. H. Morgan, N. H. Samarasinha and D. K. Yeomans, Eds. Cambridge University Press.
16. Symantec Corporation. (2006). Web Site, http://www.symantec.com/avcenter/threat.severity.html.
17. FDA. (2003). *Guidance for Industry 152 – Evaluating the Safety of Antimicrobial New Animal Drugs with Regard to their Microbiological Effects on Bacteria of Human Health Concern*, October 23, 2003 Available at http://www.fda.gov/cvm/guidance/fguide152.pdf.
18. American Petroleum Institute. (2004). *Security Vulnerability Assessment Methodology for the Petroleum Industry*, 2nd ed., October 2004.
19. Cox, L. A., Babayev, D., and Huber, W. (2005). Some limitations of qualitative risk rating systems. *Risk Anal.* **25**(3), pp. 651–662.
20. Hoerger, F. (1990). Presentation of risk assessments. *Risk Anal.* **10**(3), pp. 359–361.

21. Fiering, M., and Wilson, R. (1983). Attempts to establish a risk by analogy. *Risk Anal.* **3**(3), pp. 207–216.
22. Starr, C. (1969). Social benefit versus technological risk. *Science* **165**(3899), pp. 1232–1238.
23. Covello, V. T., Sandman, P. M., and Slovic, P. (1988). *Risk Communication, Risk Statistics, and Risk Comparisons: A Manual for Plant Managers*. Chemical Manufacturers Association, Washington, DC.

# TERRORISM RISK

GORDON WOO
*Risk Management Solutions, London, United Kingdom*

## 1 SCIENTIFIC OVERVIEW

Einstein remarked that nature is subtle, but not malicious. There is no universal definition of terrorism, but all such acts are recognized as being malicious. Also, not all terrorist campaigns are deadly and enduring, but these are the words used by the director general of the British security service, Manningham-Buller, [1] to categorize the global Jihadi threat, at a time when the MI5 perceived Britain to be Al Qaeda's prime target [2].

The purpose of this article is to describe methods for modeling this source of terrorism risk, and to identify research directions, especially in analysis on a global scale. In the latter regard, aviation and maritime risks are given prominence, because of their significance in border protection. Skeptics of terrorism risk modeling may perceive terrorism to be simply a Manichaean struggle between good and evil, or imagine that terrorists are stupid and crazy. On the contrary, in reality, capable terrorists are both rational and intelligent. Terrorists have to be intelligent in order to make an impact in asymmetric warfare. Atwan [3] has warned the West not to underestimate the intellectual prowess of the Al Qaeda leadership. Osama bin Laden honored Khalid Sheikh Mohammed, the 9/11 mastermind, with the title "mukhtar", meaning "the brain" [4]. Indeed, it may be argued that the most powerful biological weapon in the terrorist's arsenal is not any deadly virus but the human brain itself.

But is it rational for a Jihadi to undertake a suicide mission? Yes, according to the seventeenth century French philosopher, Blaise Pascal. Given the promise of eternal paradise after a martyr's death, and a nonzero likelihood of this promise being actually realized, it is perfectly rational for a Jihadi to accept Pascal's wager, and bet on this outcome of a martyrdom mission. It is known that some terrorists have followed this line of philosophical thought. In the words of one Palestinian, "If you want to compare it to

the life of Paradise, you will find that all of this life is like a small moment. You know, in mathematics, any number compared with infinity is zero" [5].

Building on the understanding that Islamist militants are rational and intelligent, an overview of the principles of terrorism risk modeling that govern the frequency and severity of Jihadi terrorist attacks, the choice of weaponry, and the selection of targets is presented.

### 1.1 Terrorist Targeting

A cornerstone of terrorist targeting is target substitution [6]: if a designated target is too hard, an alternative softer target may be substituted. If, however, there is no available alternative of a similar status, efforts at striking the original target may be redoubled. Target substitution operates on all spatial scales, and is a phenomenon very familiar to criminologists (Yezer, [7]). At the street level, the Bali cafés bombed on October 1, 2005, had been chosen for their inferior security. At the town level, the British embassy in Istanbul was bombed on November 20, 2003, in preference to the fortress-like US embassy [4]. At the national level, the IRA switched a truck bomb attack from London to Manchester, when the border security around the city of London was tightened. At an international level, Jemaah Islamiyah switched an embassy attack from Manila to Singapore because of the difficulty in the Philippine targets [8].

The malice underlying terrorism suggests applying game theory, as Sandler and coworkers did long before 9/11 [9], and others have done since. Game theory models with just a few variables can be analyzed in elaborate mathematical detail. For example, Kardes [10] has provided solutions to some illustrative stochastic game problems with a small number of states. A basic model of a territory with a handful of terrorist targets or weapon systems, may be mathematically tractable, but the US homeland is dense with terrorist targets. As with models of a few targets, insights into what to protect may be gained from considering a simple model with numerous targets, where all, or almost all, of the targets are equally valuable to the defender (Bier [11]).

To develop a full-scale practical model for the entire US homeland, some simplifying assumptions are clearly necessary. These may be coarse, but they can be substantiated from knowledge of the terrorist modus operandi, and validated against information on planned attacks. Al Qaeda operatives are trained to be meticulous over target surveillance [12], and are very sensitive to changes in security. One may reasonably assume that through diligent surveillance, they effectively immunize the attack loss potential against changes in security (Major [13]), in the mathematical sense that, to first order, the expected loss from an attack is invariant against such changes.

For various terrorist organizations such as the IRA, killing large numbers of civilians has very low utility for the terrorists, since such attacks would severely erode their popular support base. Therefore, a target such as a packed sports stadium, had a much lower utility for the IRA than for the defenders. However, for Islamist militants, enraged by many thousands of civilian Muslim deaths in conflict zones, mass fatalities are perceived as a legitimate attack objective. In his statements [14], Osama bin Laden has indeed encouraged such attacks: "It is the duty of Muslims to prepare as much force as possible to attack the enemies of God".

The chief Al Qaeda strategist, Dr Ayman Al Zawahiri, has explained the influence of the Umma, (the global community of Muslims), in their targeting strategy: "Al Qaeda wins over the Umma when we choose a target that it favors" [15]. Opinion poll surveys

show that a significant proportion of Muslims around the world condone terrorist attacks against Western targets as a reprisal for Western indifference to the loss of Muslim lives. The Leeds clique of British–Pakistanis who bombed London on 7/7 had held a celebration party, immediately after 9/11 [16]. Cities with international recognition are collectively favored by the Umma, as is affirmed by the list of postcard cities attacked since 9/11: Bali, Mombasa, Casablanca, Riyadh, Amman, Madrid, and London. In contrast, towns are not favored by the Umma if they are unknown to most Americans, let alone on the Arab street.

The Jihadi preparedness to use maximum force, and the Umma's perception of Crusaders' pain as Islam's gain, suggests that, as a first approximation, target utility valuations based on economic and symbolic value, and casualty potential, are broadly similar for Jihadi attackers and Western defenders. If only Jihadis were motivated to attack a Western target that had low defender utility. A cartoon in Punch magazine once depicted London's Royal Albert Memorial as being an ideal honey-pot IRA target. To the regret of architectural aesthetes, this undefended monument to Victorian garishness was never targeted by the IRA. The Statue of Liberty is a prime example of an iconic terrorist target that is well protected, even though its economic value and casualty potential are comparatively modest. Unlike the undefended Albert Memorial, it is known that the defended Statue of Liberty is a Jihadi target.

If it is posited, as with the Statue of Liberty, that defensive resources commensurate with their utility are applied to protect targets, a parsimonious targeting model is then derived (Woo [17, 18]). This is a phenomenological model: the few parameters are estimated through elicitation of the judgment of international terrorism experts. Cities are grouped into discrete tiers by the experts, for example, New York and Washington D.C. comprise the first tier. A similar style of discrete target tiering is developed for types of targets, for example, hotels, government offices, airports and so on.

The model automatically yields targeting likelihoods akin to a Pareto 80/20 rule, in that it forecasts that the great majority of attacks will be against a minority of potential targets. This focusing of attacks against a small proportion of targets is consistent with the historical experience of major prolonged foreign terrorist campaigns, such as the IRA bombing campaign in England, which concentrated terror in its leading cities: London, Manchester, and Birmingham.

This baseline model can be updated with site-specific information on whether security is relatively better or worse than the norm for a potential target of a particular ranking. The essential characteristics of terrorist targeting are captured by the model:

- Terrorists may substitute one target with another, according to the relative security of the targets.
- Local security enhancement transfers threat elsewhere: excessive site protection may be undesirable on a societal level. For example, some government buildings may be protected against vehicle bombs well beyond terrorist capability, whereas there may be insufficient expenditure on protecting private offices, or public infrastructure.
- There is safety in numbers: increasing the number of targets of a specific type dilutes the individual risk. By contrast, where there are few targets of a specific type, for example, tourist hotels in a city, then the risk is increased, as with the Amman, Jordan, bombings on November 9, 2005.
- Terrorist attacks are geographically focused, with attack likelihood decreasing logarithmically for descending target tiers. This is exemplified by the IRA's choice of

the English city to attack: the first tier being London; the second tier comprising Manchester and Birmingham, and so on.

### 1.2 Weapon Attack Modes

Rationality pervades the operational modus operandi of terrorists. The handbook of all guerrilla movements is Sun Tzu's "The Art of War", which identifies optimal modes of combat: "Now an army may be likened to water, for just as water avoids heights, and hastens to the lowlands, so an army avoids strength and strikes weakness". This dictum echoes the principle of following the path of least resistance that governs the dynamics of the universe, including terrorist activity [19]. This elegant principle was first enunciated by Pierre de Maupertuis: "The great principle is that, in producing its effects, Nature acts always according to the simplest paths".

In hydrology, the principle of minimum energy expenditure governs the pattern of river drainage networks. Similar to the flow of water, the flow of terrorist activity is towards weapon modes and targets, against which the technical, logistical, and security barriers to mission success are least. Since 9/11, the counterterrorism environment for the development of new weapons and planning complex strategic operations has become oppressive for Al Qaeda. Accordingly, it inclines towards off-the-shelf, ready-to-use weapons, (such as man-portable air-defense systems (MANPADS), mortars, hijacked aircraft, and propane tankers), or improvised conventional explosive devices, which do not involve intricate and potentially failure-prone technological development. Al Qaeda is known to be highly adaptive in learning from past terrorist successes and failures from all terrorist organizations around the world [4]. Neural network simulation models can represent the social learning process [20].

The logistical burden of alternative weapon systems can be evaluated in terms of the terrorist demands on finances, equipment, material, trained personnel, and sleeper cell support. Calibration against actual experience is possible for conventional attack modes, but not for exotic attack modes, such as chemical, biological, radiological, and nuclear (CBRN). Event-tree methods have been devised to elaborate the alternative foreign and domestic pathways by which such unconventional weapons can be manufactured or procured.

### 1.3 Frequency of Successful Macro-Terror Attacks

Macro-terror attacks are acts of terrorism, such as the one perpetrated on 9/11, that aim to cause substantial loss, and require significant logistical resources and considerable time for planning and preparation. Al Qaeda is renowned for meticulous detail over its centrally organized attack planning that involves diligent reconnaissance, surveillance, and rehearsal. Most notably, Al Qaeda has developed a long-term strategy, and is extremely patient in planning its military campaign over decades. Indeed, patience is half of the Islamic concept of faith, that covers action, (for which gratitude is due to Allah), and abstinence from action, (for which patience is demanded). Dr Ayman Al Zawahiri [15] has explained the Al Qaeda goal: "We must inflict the maximum casualties against the opponent, for this is the language understood by the West, no matter how much time and effort such operations take".

It turns out that the number of operatives involved in planning and preparing attacks has a tipping point with respect to the ease with which the dots might be joined by

counterterrorism forces. The opportunity for surveillance experts to spot a community of terrorists, and gather sufficient evidence for courtroom convictions, increases nonlinearly with the number of operatives—above a critical number, the opportunity improves dramatically. This nonlinearity emerges from analytical studies of networks, using modern graph theory methods (Derenyi et al. [21]). Below the tipping point, the pattern of terrorist links may not necessarily betray much of a signature to the counterterrorism services. However, above the tipping point, a far more obvious signature may become apparent in the guise of a large connected network cluster of dots, which reveals the presence of a form of community. The most ambitious terrorist plans, involving numerous operatives, are thus liable to be thwarted. As exemplified by the audacious attempted replay in 2006 of the Bojinka spectacular, too many terrorists spoil the plot (Woo, [22]).

Intelligence surveillance and eavesdropping on terrorist networks thus constrain the pipeline of planned attacks that logistically might otherwise seem almost boundless. Indeed, such is the capability of the Western forces of counterterrorism, that most planned attacks, as many as 80–90%, are interdicted. For example, in the three years before the 7/7 London attack, eight plots were interdicted. Yet, any noninterdicted planned attack is construed as a significant intelligence failure. The public expectation of flawless security is termed the *90-10 paradox*. Even if 90% of plots are foiled, it is by the 10% which succeed that the security services are ultimately remembered.

Thanks to the diligence of the security services, which deter the planning of large numbers of attacks, and interdict most of those that are planned, the frequency of successful terrorist attacks is kept low. Only a small proportion of attacks succeed, and these attacks tend to be those involving fewer active operatives. Through this control process, which comes at the cost of some personal civil liberty, the uncertainty in the frequency of successful terrorist attacks is constrained. As happened after 9/11 and 7/7, after each major terrorist attack, democracies will respond by rebalancing the desire for liberty with the need for security.

## 2 RESEARCH ON TERRORISM RISK

Terrorism is a global phenomenon. Where activists cannot effect political change through peaceful means, they coerce through political violence. Terrorism research has a wide international agenda: the structure of terrorist organizations, weaponry, targeting, vulnerability and security, counterterrorism and so on. Terrorism risk assessment forms part of the research agenda, and is shaped and directed by the practical needs of the public and private sectors.

The insurance industry operates worldwide. Accordingly, global models of terrorism risk have been developed to assist risk managers of insurance companies and captive insurers. These models vary in resolution from one country to another, depending on the degree of commercial interest. Insurance risk management requires control of aggregate loss potential. Accordingly, models cover all terrorist groups and all plausible attack modes. Although their adoption is discretionary, risk models are used quite widely by insurers, in recognition of which the insurance industry has funded a considerable amount of research on terrorism risk. Notable is the research carried out by the RAND Center for Terrorism Risk Management Policy, which is a joint project of the RAND Institute for Civil Justice, RAND Public Safety and Justice, and Risk Management Solutions (RMS).

Besides the insurance industry, the US government has a direct stake in assessing terrorism risk on a national scale, with purposes to improve counterterrorism resource allocation among others. Any implementation of a risk-based allocation procedure must address concerns over uncertainty about terrorist targeting. A detailed RAND study (Willis et al. [23]), based on the RMS terrorism risk model, has developed an approach for making allocation decisions, robust against uncertainty in model parameterization.

A considerable volume of academic terrorism risk research has been undertaken to support national public policy, notably at the University of Southern California's Center for Risk and Economic Analysis of Terrorism Events (CREATE), a DHS University Center of Excellence. At spatial scales below the national level, terrorism risk assessment is potentially useful for state and local public officials, for managers of transport infrastructure, utilities, critical facilities, as well as major buildings. Absent prescriptive terrorism mitigation standards, a risk-based approach to decision-making on security improvement is relevant. For major transportation systems, cost–benefit analyses for project prioritization and resource allocation have been conducted (e.g. King and Isenberg [24]).

The challenge of terrorism risk assessment varies according to scale. On one hand, the more restricted the geographical scope, the narrower is the spectrum of possible targets. On the other hand, the dynamical coupling of terrorism risk across regional boundaries and between diverse targets is lost. The same applies to research focusing on specific weapon systems: the more restricted the military scope, the harder it is to address the coupling and switching between alternative choices of weaponry. An analogy with weather forecasting is apposite, since meteorological conditions are dynamically coupled across regions. Local weather forecasting is possible, but only if a large-scale model of the atmosphere is used to define regional boundary conditions.

The problem of scale manifests itself particularly acutely in frequency estimation. An absolute measure of frequency cannot be generated internally from within the confines of a research project that has a limited scope. However, setting aside discussion of the absolute probability of an attack against a specific target, risk assessments can usefully focus on the conditional probability of an attack.

## 2.1 Aviation and Maritime Risk Assessment

Just as the fighter jet is symbolic of militarism, so is the passenger jet of terrorism. Civil aviation is a vulnerable link in the global economy. The continuous adaptation of attack modes to evade security enhancements is a conundrum of aviation risk assessment. A wide range of airport security measures have been analyzed by Martonosi [25] from an operational research perspective. The cost-effectiveness of MANPAD countermeasures has been investigated by von Winterfeldt and O'Sullivan [26], using decision analysis techniques. Their analyses show that measures to deflect SAM missiles might be cost-effective if the probability of an attack exceeds 0.5 in 10 years; the losses are large ($100 billion); and the countermeasures are relatively inexpensive (<$15 billion). It turns out that the RMS estimate of the 10-year MANPAD attack probability for shooting down a plane in the United States falls around the threshold criterion. Also, given that the scale of economic losses and the cost of countermeasures might also straddle the criterion levels, any decision on implementing countermeasures remains awkward, bearing in mind the inevitable prospect of the terrorist threat shifting to another alternative aircraft attack mode. Since 9/11, there has been an intermittent series of

foiled plots against civil aviation, several of which have involved the smuggling of explosives.

Like aircraft, ships can be attacked or converted into floating bombs. Apart from these maritime dangers, US ports face a considerable challenge in preventing illicit terrorist cargo or personnel from entering the United States, while allowing the free flow of maritime commerce. Security standards are tightening at foreign ports, but the possibility exists that an inbound vessel might have terrorist connections. It is impractical for the coast guard to search more than a small percentage of inbound vessels, so an intelligence-led risk-based procedure is needed to improve the search selection.

With access to a global database of all commercial vessel movements, (such as maintained by the Lloyds Marine Intelligence Unit), a threat-ranking system can be devised, based on public information on ownership, flag of registration, crew nationality, last ports of call, and so on. Like any profiling system, it can be subverted by an adaptive terrorist intent on surprise, except that intelligence leads may give reason to revise this threat-ranking. A risk-based methodology for incorporating available intelligence leads, and treating surprising data of dubious reliability, has been devised by Woo [27] using the conceptual framework of Bayesian epistemology.

## 3 CRITICAL NEEDS ANALYSIS

Of the various measures that may be taken to protect the US homeland against terrorism, securing national borders is a priority. The particular contribution made by specific border security measures, such as the US VISIT program, which involves the gathering of personal identity information about people in transit to the United States, or at US border posts, is somewhat indeterminate. A strict regime of personal identity checking casts a virtual security net around the entire United States that takes advantage of the small-world phenomenon of social networks: terrorists may be separated by thousands of miles, but connected instantaneously by a computer database of suspected or known terrorist links.

The potential to unravel a terrorist network may have very substantial deterrent value. A sizeable community of Jihadis involved in planning a large-scale technically complex operation, for example, a CBRN attack, would come under heavy counterterrorism pressure. Given that a major US operation carries a significant risk of network unraveling, there should be a strong impetus for terrorists either to lower the attack scale to reduce their detectability footprint, or to switch the attack to a softer country within the Western alliance. Through its unwavering support for US foreign policy, Britain is seen by Islamists as forming an axis of evil with the United States and Israel. The United Kingdom is an obvious substitute target: the United Kingdom is politically almost exactly aligned with the United States on the war on terrorism, has a far more radicalized Muslim community, and yet is far behind on biometric border security. Already, the terrorist threat to London is comparable with that to New York or Washington. Because Al Qaeda has a global franchise, and terrorist target substitution operates on a transnational scale, there is a critical need for risk assessment which is conducted on a global basis [28].

### 3.1 Global Scale of Terrorism Risk Modeling

Global terrorism models are needed to comprehend the terrorist threat to the US homeland from Islamist militancy. This is obvious for international aviation and maritime

transportation attacks, and it is true for all threat modes, since foreign policy is a prime driver of Muslim discontent and Jihadi recruitment. Further research on global terrorism risk modeling will benefit efforts on focusing counterterrorism action. Terrorist social networks, weapon procurement and transport, and the security of US assets abroad are important concerns that merit analysis from an international perspective.

The Umma has been galvanized collectively by Al Qaeda to seek redress for the plight of Muslim brothers and sisters in conflict zones. The global social networks of Muslims provide a support framework for radicalism, extremism, and terrorism. A crucial role in facilitating terrorism in the Western democracies is played by Muslim diaspora communities: Pakistanis in United Kingdom, Algerians in France, Moroccans in Spain, Somalis in Italy, and so on.

Improved models need to be developed for the evolution of terrorist support. Transcending the boundary between sociology, social psychology, and physics, is the modern discipline of sociophysics. This offers a scientific methodology for incorporating the social dynamics of diaspora communities into terrorism risk assessment. Basic rules of social interaction, akin to the dynamics of physical systems, are capable of enhancing understanding of complex social behavior. The formation of ghettos is a classic paradigm of sociophysics; one which is relevant to terrorism risk. "Jihad" and "Osama bin Laden" are the favorite Google keywords in some British Muslim ghettos. It is no surprise that as many as 100,000 British Muslims considered the 7/7 London bombings to be justified [1].

With the same objective, large-scale agent-based computer simulations of the collective behavior of Islamist militants have been developed (e.g. MacKerrow [29]), but there is much room for advancement in the understanding of Islamist militancy. The discourse on this subject is beset at the highest level by political autism—the inability to think what others are thinking. Mathematical psychologists like Vladimir Lefebvre have found mathematical ways of encoding the recursive sequence of thinking what others think. Terrorism risk assessment will be distorted if its political components misrepresent the underlying root causes of terrorism (Richardson [30]).

## 4 RESEARCH DIRECTIONS

Terrorism risk analysis is no longer a fledgling discipline. The core principles that govern terrorist actions are subject to observation and empirical validation, and, with the passage of time, the database of planned attacks is becoming more amenable to quantitative analysis. What is already clear is that, in the asymmetric warfare waged by the Western democracies against militant Islam, the forces of counterterrorism are achieving considerable success in controlling terrorism. The record is not perfect, as illustrated by the rail bombings of Madrid in March 2004 and London in July 2005. As the authorities remind their citizens: itis not a question of if, but when the next attack will occur. But at least, the question is thankfully not: how many major attacks will there be?

Research into global counterterrorism is needed to elucidate important aspects of the dynamics of the terrorism control process. The close cooperation between security services in the G8 countries contributes significantly to the successful interdiction of the great majority of planned terrorist attacks against these countries by Islamist militants, and to restricting their international operations. The dynamics of terrorism control depend on the global political environment, which is easily destabilized, and subject to the law of unintended consequences, even if politicians would hope otherwise. In order

to be meaningful for homeland security decision-making, cost–benefit analysis should be broadened in scope from having a restricted internal domestic frame of reference to having global coverage of US interests and actions. As terrorist threat is integrated across the globe, terrorism risk research must also be directed globally.

## REFERENCES


1. Manningham-Buller, E. (2006). *The International Terrorist Threat to the UK*, Speech at Queen Mary College, London.
2. Rusbridger, A. (2006). The Guardian newspaper. Manchester, October 19.
3. Atwan, A. B. (2006). *The Secret History of Al Qaida*, Saqi books, London, pp. 256.
4. Gunaratna, R. (2005). *Terrorism Risk Briefing*, Washington, DC.
5. Oliver, A. M., and Steinberg, P. (2005). *The Road to Martyr's Square*, Oxford University Press, Oxford, pp. 214.
6. Drake, C. J. M. (1998). *Terrorists' Target Selection*. Macmillan Press, London, pp. 272.
7. Yezer, A. (2006). Terrorist attacks and their consequences. Presentation at the CREATE workshop on benefit methodologies for Homeland Security Analysis, June 8–9, Washington, D.C.
8. Bell, S. (2005). *The Martyr's Oath*. John Wiley & Sons, Ontario, pp. 254.
9. Sandler, T., and Lapan, H. (1988). An analysis of terrorists' choice of targets. *Synthèse* **76**, 245–261.
10. Kardes, E. (2005). *Robust stochastic games and applications to counter-terrorism strategies*. CREATE report, 64.
11. Bier, V. (2005). *Choosing what to protect*. CREATE report, 27.
12. Gunaratna, R. (2002). *Inside Al Qaeda*. Hurst & Co., London, pp. 282.
13. Major, J. A. (2002). Advanced techniques for modeling terrorism risk. *Journal of Risk Finance* **4**, 15–24.
14. Lawrence, B., Ed. (2003). *Message to the World: The Statements of Osama bin Laden*, Verso, London, pp. 224.
15. Zawahiri A. *Knights under the prophet's banner*, London, 2002.
16. Rusbridger, A. (2006). The Guardian newspaper. Manchester, June 24.
17. Woo, G. (2002). Quantitative terrorism risk assessment. *Journal of Risk Finance* **4**, 7–14.
18. Woo, G. (2003). Insuring against Al Qaeda. *NBER Insurance Workshop Presentation*, Cambridge, Mass.
19. Ranstorp, M. (2006). *In the service of Al Qaeda*. In preparation.
20. Carley, K. (2003). *Destabilizing terrorist networks*, CASOS Working Paper.
21. Derenyi, I., Palla, G., and Vicsek, T. (2005). Clique percolation in random networks. *Phys. Rev. Lett.* **94**, 160202.
22. Woo, G. (2006). *Small World Constraints on Terrorism Attack planning*, Vol. 5. RUSI/Jane's Homeland Security & Resilience Monitor, London.
23. Willis, H. H., Morral, A. R., Kelly, T. K., and Medby, J. J. (2005). *Estimating terrorism risk*, RAND Corporation, Report from Center for Terrorism Risk Management Policy, Santa Monica, pp. 66.
24. King, S., and Isenberg, J. (2005). *Assessment of Urban Transportation Infrastructure for Terrorism Risk Management*. ICOSSAR, Millpress, Netherlands, pp. 2773–2780.
25. Martonosi, S. E. (2005). An operations research approach to aviation security. PhD thesis, M.I.T, 163.

26. von Winterfeldt, D., and O'Sullivan, T. M. (2005). *A decision analysis to evaluate the effectiveness of MANPAD counter-measures*. CREATE report No. 05–30, 24.
27. Woo, G. (2005). Institutionalizing imagination to prevent surprise. Invited talk at the *IDSS National Security Conference*, Singapore.
28. Woo, G. (2006). The terrorist threat to the US from abroad. Presentation at the CREATE workshop on benefit methodologies for Homeland Security Analysis. June 8–9, Washington D.C.
29. MacKerrow, E. (2003). Understanding why-dissecting radical Islamist terrorism with agent-based simulation. *Los Alamos science*, **28**: 184–191.
30. Richardson, L. (2006). *What terrorists want*. John Murray, London, pp. 288.

## FURTHER READING

Wiktorowicz, Q. (2005). *Radical Islam rising: Muslim extremism in the West*. Rowman & Littlefield, New York, pp. 288.

# TERRORIST THREAT ANALYSIS

JACK F. WILLIAMS
*Georgia State University, Atlanta, Georgia*

## 1 INTRODUCTION

Threat analysis is the art of wasting information, that is, the art of peeling away layers of irrelevant information, incorrect information, and disinformation, in order to expose a state or states of relevant and credible information related to a question of interest to the client. Analysts rarely have too little information to form an opinion. Rather, the analyst is often inundated with information culled from classified sources, unclassified but private or sensitive sources, or open sources [1]. After all, there are two ways in which to hide a needle: in a haystack or in a stack of needles. Threat assessment more closely resembles the latter task. Threat analysis is a nuanced and complex inquiry. Central to its understanding is that the most relevant threat information is usually in the hands of the adversary [2]. Thus, we are constantly guessing about threat, and our adversary is constantly guessing about how we are guessing about threat. In order to understand

threat, conventional wisdom segregated threat into two components: (i) capability and (ii) intent [3]. Thus, an analyst could study an adversary's prior attack events, training activity, and the like to ascertain the capability to undertake and carry out an attack. Additionally, an analyst could study an adversary's expressed or implied intent regarding specific targets and operational modes. Synthesizing the two components, an analyst could describe past and present threat profile and develop future threat profiles given a known adversary. Yet, these traditional threat profiles were lacking in a key ingredient: authority. Particularly with religiously motivated adversaries (but certainly not limited to such), moral and theological authority is a necessary condition to make the transition from attack planning to execution [4, 5]. Furthermore, the concept of authority has a direct effect on target selection and tactics, and lends legitimacy to the group among nonviolent, but sympathetic, populations [4–6].

## 2 TRADITIONAL THREAT ASSESSMENT

Conventional wisdom holds that threat must be mapped to a given adversary and consist of that adversary's capability to carry out an event and that adversary's intent to conduct such operations [3, 7]. Thus, traditionally, threat (T) is a product of capability (C) and intent (I) of a *specific nation-state*:

$$T = f(C \times I) \tag{1}$$

The role of the analyst was to develop a threat profile centered on these two attributes. Under the Soviet intelligence paradigm, the adversary was generally self-evident: The Soviet Union, Eastern Bloc Countries, or Soviet Union Surrogate Countries (Vietnam, Syria, etc.). Sources of information to flesh out threat included classified, unclassified, and open-source material. Among analysts, it was well accepted and well understood that the golden source was classified material followed far behind by unclassified material [1, 8]. Open source was rarely considered and, in fact, regularly dismissed out-of-hand by analysts [1, 8]. Notwithstanding a heated division among US intelligence analysts, open source has gained currency, aligning US intelligence with allies such as the United Kingdom, Canada, Australia, Europe, Israel, Morocco, and Jordan, to name a few [8–11].

### 2.1 An Adversary's Capability

An analyst uses several tools to assess an adversary's capability. Initially, analysts subdivided capability into three components: operational, technical, and logistical [12]. An assessment of operational capability focuses on the question whether an adversary had sufficient leadership, command and control, intelligence function, financing, experience, and expertise in carrying out a specific terrorist event. A traditional inquiry would consider an adversary's past events (both operational successes and failures), training centers, centers of gravity, access to various weapons platforms, expertise, indicators and warnings, sources of financing, and alliances with other organizations. An assessment of technological capability would focus on whether an adversary had either internal or external access to the required technology to carry out an event. An analyst would consider an adversary's prior events, research and development programs, and alliances. Careful attention would be paid to indicators of in-house technological development and

attempts to secure such technology from outside sources. After considering the relevant information, an analyst may develop operational grids that identify indicators and precursors of operational and technological mastery and advancement, creating a composite profile of an adversary's capability. An assessment of logistical capability would focus on the ability of a given adversary to sustain a threat on a regional or global level, differentiating terrorism threat from criminal attempt. An analyst would consider an adversary's leadership structure, recruitment, training, educational, social outreach, communications, propaganda, political, and financial footprints.

Conceptually, all three subcomponents of threat capability could be mapped to the foundation stones of global terror, those attributes of a terrorist organization necessary for the organization to sustain itself as a continuing regional or global threat. These attributes include territory, infrastructure, and finance [13]. Territory and infrastructure operate together to provide sanctuary for a terror group, an essential attribute in order to pose a sustainable regional or global threat. Moreover, the closer to the theater of operations a terrorist group can establish sanctuary, the more effective the terrorist activity becomes. This is in part why insurgencies are so effective; the sanctuary and theater of operations are one and the same.

In prior writings, I have argued that, in addition to territory, infrastructure, and finance, for a terrorist group to pose a strategic threat, that group must operate within recognized authority [4, 5]. Authority serves two distinct but closely related purposes. First, *internal authority* is absolutely necessary to conduct operations, recruit, and replenish [4, 5]. For example, within al-Qaeda, authority in the form of the issuance of a *fatwa* or a series of *fatawa* elevates what may appear to be murder and suicide, which are acts strictly forbidden by the Quran, Hadith, Sharia and other Islamic religious sources, into a sacramental duty by embracing principles of *jihad* and martyrdom [4, 5, 14]. Without a carefully reasoned *fatwa* by a recognized religious authority providing religious cover, a suicide bomber is stripped of the patina of religious authority behind his act and exposed as an *irhabi* (wanton criminal or terrorist) or *mufsidoon* (an evildoer) engaged in *fitna* (the sowing of societal chaos) whose proper end is eternity in hellfire [15]. Secondly, external authority is necessary in order for the audience to which religious terrorists speak to acquiesce, accept, or better yet embrace the terrorist group's tactics and goals. External authority is better understood as conferred legitimacy. For terrorist organizations like al-Qaeda, the intended audience is the *umma* (greater Muslim community) and not the West. Jihadist groups like al-Qaeda, who base their operational philosophy on a loose, cobbled collection of *Salafia* authorities [16], *Qutbist* writings [17], and contemporary Jihadist jurists and theologians, engage in what they perceive to be *dawa* (the "call") or the teaching and invitation to non-Muslims and non-devout Muslims to the Muslim faith [16]. Without a solid perception of external legitimacy among the *umma*, the *dawa* fails to resonate; once the *dawa* fails, the educational function of a movement like al-Qaeda dries up; once the educational function dries up, the organization cannibalizes itself and will cease to exist [18, 19]. A terror group's burn rate is exceptionally fast.

### 2.2 An Adversary's Intent

An adversary's intent may be subdivided into (i) general intent to commit certain acts directed at general target categories and (ii) specific intent to commit specific acts directed at specific targets [20]. Each subdivision may be further divided into strategic, operational,

and tactical elements. An analyst employs several techniques to ascertain an adversary's intent. Primarily, the analyst peruses vast amounts of information, carefully teasing out an adversary's beliefs, motives, and intents, by exploring historical interest, past attacks (both successes and failures), current adversarial interest in a site or asset, current surveillance, documented or authenticated threat, desired level of consequence, ideology, religious beliefs, historical authenticity of attack, and ease of attack [21]. Absent a declared intent by an adversary, such as Iranian President Ahmadinejad's intent toward Israel, this usually requires a mastery of the tradecraft and mind-set of an adversary. Analysts draw on cultural, religious, philosophical, ideological, legal, historical, geographical, and linguistic sources to portray the adversary's thought-process and inclinations. The analyst then patiently and deliberately moves from an adversary's general intent to harm, to specific intent to engage in potential acts toward specific targets. That migration is not always graceful, reliable, or accurate.

Often, an analyst may discover that an adversary's intent does not match that adversary's capability. Such a preliminary conclusion could mean a number of things. First, it could mean that present intent telegraphs future capability. An analyst then considers intelligence (or requests intelligence) that might suggest increased research and development by an adversary in a given expertise or the quest by an adversary to find someone or some group that would presently possess that expertise and join ventures with the subject adversary. This often can be accomplished, for example, through training the members of one terrorist group by subject-matter and technical experts from another terrorist group, often for remuneration [22]. Second, it could mean that the manifestation of intent that we discovered or captured is part of a denial and deception ("D & D") campaign. Analysts have developed several heuristics and tools in hedging against being misled by deception, including a technique known as the analysis of competing hypotheses (ACH) [23–29]. Historically, most counterdeception techniques did not work well when confronted by a sophisticated deception program, where, among other things, the deceivers did not even know that they were part of a deception. Stech and Elsaesser have done excellent work in developing robust counterdeception techniques, including an ACH model building on cognitive task analysis (CTA) of the deception detector, courses of action (COA), and Bayesian Belief Networks, which have advanced D & D detection and counterdeception strategies [29, 30].

### 2.3 Synthesizing Capability and Intent

An analyst would think of threat as the product of capability times intent. That way, if either variable is zero, there is zero threat. During the Cold War, for example, the United States worried a lot about Soviet submarines off our coasts loaded with nuclear missiles; however, the United States harbored no concern about British submarines similarly loaded. Although capability was the same, the British intent against us was zero. The goal of synthesizing capability and intent is to develop an adversary's threat profile mapped to a specific target and operational means [8]. Traditionally, this requires the analyst to think of capability and intent as two vectors ranging, for example, from no capability to conduct an event, to complete confidence that our adversary could do so. An analyst then gauges capability and intent somewhere along the relevant vectors. In synthesizing capability and intent, an analyst may employ classification, description, and prediction techniques [8].

## 3 CULTURAL THREAT SPACE AND THE NON-STATE ACTOR

September 11, 2001, is a hinge date in the history of intelligence analysis. The terrorist attacks on the World Trade Center in New York City, the Pentagon in Arlington, Virginia, and a field outside Shanksville, Pennsylvania, thrust the analyst into a more visible light. Although many of us had assessed threat from non-state actors well prior to 9/11, the dramatic paradigm shift from a state-centric focus to a non-state one was undeniable. With that focus came a new and honest assessment of how analysts assessed threat [9, 11]. In this article, I unpack a new frame of reference in assessing threat by a non-state actor. In particular, I assert that threat cannot be understood without a cultural awareness and assessment of the adversary [31–33]. Although many good analysts employ informal cultural assessments in their threat analyses, we can all gain from a more explicit assessment and more robust understanding of how culture affects threat. Furthermore, I assert that the present threat formula must be expanded to include another variable, authority, in order to capture a more robust and accurate profile of threat.

### 3.1 Cultural Space

One cannot understand threat without a sophisticated assessment of the culture within which an adversary operates [31, 33]. Failure to comprehend this basic step in a threat assessment leads well-meaning and highly intelligent analysts to run afoul of the Napoleonic caution to avoid "making pictures of the enemy." For a terrorist movement similar to al-Qaeda, this requires an assessment of both, the sociopolitical and religious attributes of the movement, and the universe within which it operates and seeks to influence [34–36]. Figure 1 offers a basic depiction of the sociopolitical universe of operation and influence. Note that the smaller the circle within the nesting, the tighter the bond and the greater sense of belonging. These nesting circles include Tribe or Village; Other Tribes or Villages (such other tribes historically posed a threat to the tribe); Western-Influenced Nation-States which has not completely displaced tribal influence as the United States has learned in Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF); Arab Nations; and Muslim Nations (which forms the periphery marking the transition from the so-called "Arab World" to the "Rest of the World"); and the Rest of World [37–39]. Groups like al-Qaeda engage the West through this lens, as an inherent adversary, an outsider, a continuing threat [40].

Figure 2, adapted from the Combating Terrorism Center's Militant Ideology Atlas [16], depicts, again through the use of nesting circles, a Jihadist organization's religious world view. In this world view, at its periphery are non-Muslims. Groups like al-Qaeda have essentially rejected the distinction, well documented in the Quran, Hadith, and so on, between "Pagans" (idol worshippers or those who reject monotheism) and the "People of the Book" (Jews and Christians who are in spiritual if not historical possession of prior revelations). Jihadist religious authorities have collapsed in an unprincipled manner the religious distinction between these two groups and have rejected the relatively favored treatment of "People of the Book." Moving toward the center, the next circle encompasses all Muslims. This circle would include the full range of Muslim attitudes toward religion as part of politics. Thus, this circle includes secularists, progressives, reformists, and fundamentalists [41]. These members would generally self-identify as Muslims, even with no religious institutional affinity. At their core, those that would consider themselves

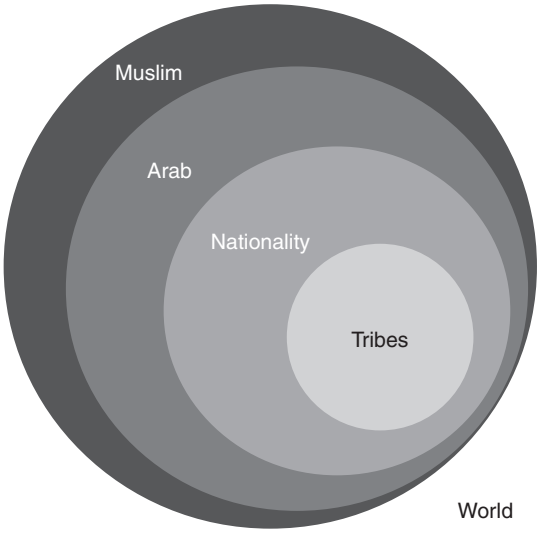



**FIGURE 1** Sociopolitical world view.

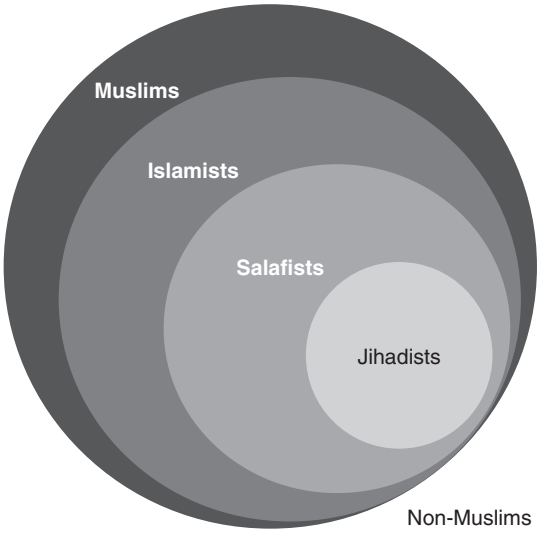



**FIGURE 2** Religious-political world view.

observant of religious practices (for Islam is an orthoproxic religious movement), recognize the five pillars of Islam. The five pillars include the *shahadah* (confession of faith that there is no G-d but G-d and that Mohammed is His Prophet (the final seal of the prophets); *salat* (prayer five times a day at designated times); *zakat* (the giving of charity as a percentage of one's wealth and not simply income); *sawm* (fasting in the month of *Ramadan*); and *hajj* (the pilgrimage to Mecca in one's life time if one can afford it) [42]. These Muslims are the followers of G-d and effectuate His will by following the words

of the Quran (a collection of chapters increasing in length) of the revelations of G-d to Mohammed over a number of years through the Angel *Jibril* (Gabriel) and the examples of the Prophet Mohammed collected in the Hadith [43, 44]. Within this circle one would find the *Sunni*, *Shia*, and other movements within Islam.

The next circle includes Islamists. This is better understood as a political movement within Islam. This is not to suggest that religious sources, doctrine, traditions, and practices do not influence Islamist, they all do, but that political ambition and goals are elevated over the role of traditional religion. Islamists are people who want Islamic law to be the primary source of law and cultural identity within a Muslim state. We often think of Islamists as fundamentalists, a term actually coined in reference to Christian theology and of little analytical use in understanding this Islamic political phenomenon. They are not. In fact, one may document case after case where Islamists (and Jihadists) regularly stray from the well-established teachings of Islam reflected in Holy Sources as a matter of political expediency. The Muslim Brotherhood is probably the most well-known Islamist organization [45].

The next circle includes Salafists. These people are *Sunni* Muslims who want to establish and govern Islamic states based solely on a revivalist interpretation of the Quran and Hadith as understood by the first generation of Muhammad's followers [16]. The most influential Salafists are Saudi religious authorities [16].

The tightest circle is the target audience to which al-Qaeda's teaching resonates. This final circle includes Jihadists. This is the militant core led by a cluster of Salafist thinkers, including al-Maqdisi of Jordan, al-Tartusi and Abu Qatada of England, Ab'd al Azziz of Egypt, and several Saudi religious authorities, who maintain that the only religiously legitimate way for Islam to engage the West is through a violent manifestation of *jihad* until the West submits to the superiority of Islam and either converts or pays the *jizah* (tax) and, according to some authorities, subjects itself to political capitulation and humiliation [16]. This is the culture within which our present adversary operates. Assessing capability, intent, or authority without an awareness of an adversary's cultural space leads to analytical drift, subconscious projection, and superficial threat assessment.

Scholars have not reached a consensus on the terms to be used to describe the Muslims that have engaged in acts of terrorism in the name of Islam. Some scholars have used the terms "Jihadists," "Militant Jihadists," "Salafists," "Islamists," "Muslim Extremists," "Salafi-Jihadists," and "Militant Muslims," or some variation thereof. Others have referred to movements like al-Qaeda as "Militant Islam," "Extremist Islam," "Radical Islam," "Fundamentalist Islam," "Neo-Fundamentalist Islam," "Neo-Wahhabist," "Jihadist Islam," and "Islamist." What makes this endeavor doubly difficult is that some scholars will employ one label for a particular movement, while another scholar will employ that same label for another movement. Moreover, the US government has not applied a consistent terminology. Its use of certain terms to classify movements within Islam in the 9/11 Commission Report was not illuminating. In an excellent essay entitled *"What's in a Name?" The Use of Terminology When Dealing with Islam and Muslims*, collected in First Impressions: American Muslim Perspectives on the 9/11 Commission Report (October, 2004), Maliha Balala made this point clear. For example, the lack of consultation on choice of terms with American Muslims and experts of Islam led to the use of words, such as "Islamist," to qualify the militant groups that constitute a serious threat to America, without distinguishing between nonviolent "Islamists" (a word that could apply easily to all Muslims and sounds to the public like "Islamic") and militant groups. The use of such terms runs the danger of including as a threat

to America those Islamists who seek to foster sociopolitical changes in their societies through peaceful means. In this article, I will use the terms *radical*, *fundamentalist*, or *militant* movements within Islam, where appropriate, to mean distinct but potentially overlapping movements. *Radical* is used to refer to movements within Islam that seek major political or ideological change, particularly major changes in the form of government. These changes in form of government may be through nonviolent or violent means, depending on the methods of any given radical movement. *Fundamentalist* is used to refer either to a political movement within Islam or to an approach to religious sources. As a political movement, fundamentalists may be radical (when they seek the *nonviolent* change of governmental structure) or nonradical (when they attempt to work within a given governmental structure). As far as an approach to religious sources goes, fundamentalists believe in a return to the fundamentals of Islam and a strict interpretation of the sources. *Militant* or *Jihadist* is used to refer to those Muslims and movements within Islam that seek radical change through *violence*, often directed at the West and mainstream Muslims.

### 3.2 Authority and Legitimacy

As previously discussed, the traditional threat model is deficient. In addition to an assessment of an adversary's capability and intent, an analyst must consider authority or legitimacy. Thus, the threat equation should be expanded to include authority ($A$) and cultural influences ($Z$) and may be expressed as follows:

$$T = [(C \times I \times A) + Z] \tag{2}$$

Empirical research suggests that moral and theological authority is a necessary condition for religiously motivated terrorists to make the transition from attack planning and development to execution [4, 5, 14, 15]. As previously discussed, authority serves two distinct but related purposes: internal authority for operational and recruiting purposes and external legitimacy for recruiting, financial, and other support purposes. Furthermore, this concept of authority has a direct effect on target selection and tactics, and lends legitimacy to the group among nonviolent, but sympathetic, populations [4, 5]. The typical and traditional manner by which this authority is communicated is through the issuance of *fatawa*, or religious verdicts by religious authorities sympathetic to Jihadist causes [14, 15, 41]. A *fatwa* is a legal judgment or learned interpretation that a qualified jurist (*mufti*) may give on issues pertaining to Sharia (Islamic law) [46].

Originally, only a jurist possessing a number of qualifications and carefully trained in the Holy Sources and, among other things, the techniques of *ijtihad* (personal reasoning), was allowed to issue a legal opinion or interpretation of an established law. Ijtihad is a potential source of Islamic law after the Quran, the Sira or the Prophet Muhammad's life, the Hadith or his collected words and deeds, the Sunna (custom), and Ijma (consensus). Later, all trained jurists were permitted to issue *fatawa* [46]. More recently, even those who self-profess to be knowledgeable or those with little training (either formal or informal since both methods are historically permissible) have taken to issuing *fatawa* [46]. Furthermore, the great universities of *fiqh* (jurisprudence) and *sharia*, such as Jami'at al-Qarawiyyin in Fez, Morocco, and al-Azhar in Egypt, have lost stature, respect, and influence, and no longer serve the role of containing and isolating poorly reasoned *fatawa*.

A *fatwa* is generally nonbinding, and a Muslim may seek another opinion. Many *fatawa* of famous jurists are collected in books and may be used as precedents. Since 1991, at Georgia State University, we have been engaged in a project to collect and analyze *fatawa* related to Jihadist activity. These *fatawa* may include justifications for attacks against the West, those targets by category or type that are *hallal* (permissible) or forbidden (*haram*), those attack means that are *hallal* or *haram*, the permissibility of collateral damage, the general prohibition and exceptions to the spilling of sacrosanct (Muslim) blood, the destruction of natural resources both outside and within Muslim lands, the justification of prior attacks, etc.

For Jihadist organizations, the *fatawa* are rules of engagement that must be followed in order to perform a legitimate act of *jihad*. We have identified four types of *fatawa* relevant for threat purposes. These four types include the following:

1. *By fiat.* Authority bound within the issuer itself;
2. *By narrative.* Authority is housed in accuracy of the narrative through assessment of transmitters;
3. *By analogy.* Authority rests on strength of classifications, a classical approach to Sharia;
4. *By logic.* Authority rests on soundness of premise and power of logic employed, an approach recently influenced by Western intellectual thought.

Virtually all *fatawa* of interest to an analyst would fall within Types 2, 3 or 4. Absent a centralized *Sunni* Islamic authority structure, multiple persons in many locations issue *fatawa* [46]. These issuances and Muslims' reactions to them reflect the author's relative position within the collection of Islamic scholars and spectrum of Islamic doctrine. Therefore, *fatawa* carry differing degrees of validity and influence, and must be assessed individually [46]. After identifying the type of *fatwa*, we then assess the *fatwa* according to the following protocol:

1. The *fatwa's* author
2. The author's teacher
3. The author's religious, political, and intellectual alliances
4. The author's students
5. The subject matter of the *fatwa*
   - Legitimacy
   - Necessity
   - Proportionality
6. The response to the *fatwa*
   - Internal among religious thinkers
   - External among potential followers
7. *Fatwa* issuer's connection to terror groups and terror acts

Each *fatwa* is then scored as unpersuasive, persuasive, or compelling, depending on both the objective application and subjective evaluation of the protocols.

In addition to the influence of a *fatawa*, this threat methodology incorporates the influence of other religious symbols, statements, songs (*nasheed* or *anasheed*), and propaganda to describe terrorist target sets and operational parameters more completely.

Thus, the analyst should pay closer attention to religious decrees and cultural signs and symbols for clues about potential targets and attack means.

### 3.3 Synthesis

After one populates the threat model by assigning information to bins of capability, intent, and authority, one can then assess and evaluate the data and the information's credibility, reliability, relevance, inferential force, and adversary purpose. Credibility is a measure of belief and authenticity [8]. That measure may be either quantitative (for example, a source has an acceptable track record) or qualitative (subjective indicators suggest believability) or both. Reliability is a measure of replicability [8]. That measure focuses on consistency and coherence. Relevance is a measure of fit. That measure seeks a determination of whether the information proves or disproves a fact of interest to the analyst and the ultimate client. Inferential force is a measure of weight [8]. Not all information is of equal value in developing and supporting a conclusion [1]. Clark identifies seven pitfalls in measuring inferential force [8]. These include what he calls (i) vividness weighting (information experienced directly is given too much weight); (ii) weighing based on the source (for example, the snobbery of downplaying open-source information versus classified information, the belief that the information from spies is more valuable than refugees or defectors, or the belief that intercepted communications are the gold standard); (iii) favoring the most recent evidence (even though an informational signal tends to degrade over time); (iv) favoring or disfavoring the unknown (absence of evidence problem); (v) trusting hearsay (information from a third-party source) about what someone else said or did though the source may be biased; (vi) trusting expert opinions (too much deference, little attempt to gauge objectivity, etc.); and (vii) premature closure and philosophical predisposition (forming an opinion early in the process and then looking only for evidence that supports that opinion). Adversary purpose is a measure of informational intent. Recall that most threat information is initially in the hands of an adversary [2, 8]. Thus, an analyst must consider whether the information, in fact, may be disinformation playing a part in a D & D program [29, 30]. This D & D assessment is as such difficult to make, and is made even more difficult where the adversary's own actors are unaware that they are playing out a D & D program. Important hedges against D & D programs include consideration of alternative hypotheses; perspective shifts; a focus on collection content and not quantity; infusion of randomness into information collection; and development of an efficient feedback loop among all constituent parties to the intelligence process [8, 29, 30]. Another important hedge is something called "Red Teaming," that is, the use of an independent team, made of subject-matter experts, whose job is to try to debunk an analysis, invalidate assumptions, disprove hypotheses, etc. A good Red Team should be a hedge against complacency and "group think" that often send analyses down a wrong path.

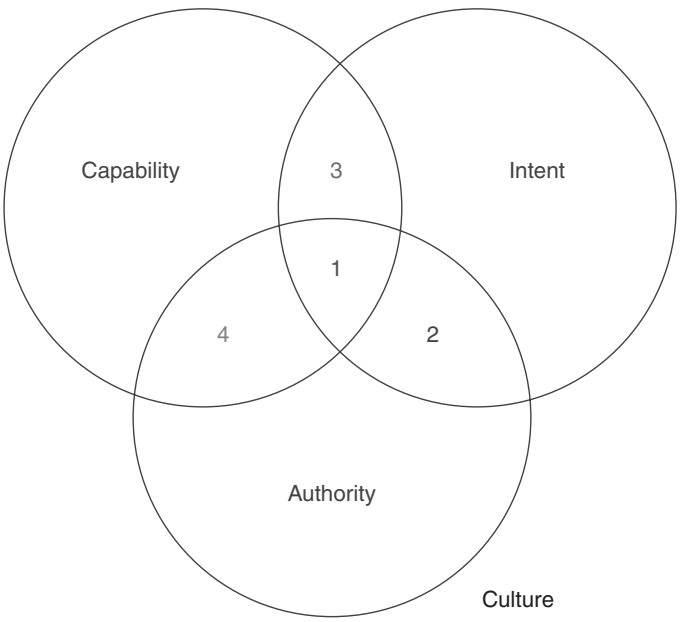
The next step in the threat process is to identify information as either divergent or convergent. Clark suggests that multiple items of information are divergent if they favor different conclusions [8]. Clark further subdivides divergent information into two subclasses of note: (i) divergent information where multiple strands are true but support different conclusion and (ii) divergent information that is contradictory because these

strands suggest logically opposing conclusions [8]. Clark then suggests that multiple items of information are convergent if they suggest or favor the same conclusion. He notes that convergent evidence may be redundant. As Clark observes, "redundancy is one way to improve the chances of getting it right" [8]. Redundant information may be further subdivided into (i) corroborative redundancy and (ii) cumulative redundancy. Both forms of redundancy are measures of the increased weight and credibility of the information.

The next step in the process of synthesizing threat information is to combine information across the threat variables. The following diagram illustrates this step and suggests that the highest threat would come from the intersection of capability, intent, and authority in the intersection space labeled "1" (Fig. 3).

### 3.4 Analysis

After synthesizing the information, the penultimate step in the threat assessment process is to analyze the information in order to make an informed estimate of what may happen in the future. Threat assessments are always predictive. As Clark cogently remarks, "Describing a past event is not intelligence analysis, it is history [8]." Here, an analyst




1. Capability AND Intent AND Authority = Represents High Threat
2. Intent AND Authority BUT NOT Capability = Warrant Close Monitoring of Proliferation for Capability Attainment
3. Capability AND Intent BUT NOT Authority = Warrant Close Monitoring of Fatawa for Authority Attainment
4. Capability AND Authority BUT NOT Intent = May be Perpetrating a Threat Deception to Enhance Negotiation or Increase Influence

**FIGURE 3** Culture-centric threat model.

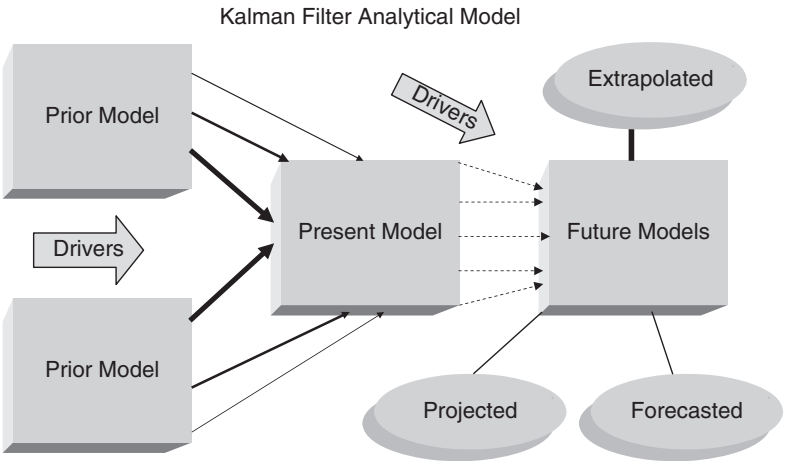



**FIGURE 4** Kalman Filter analytical model.

might begin with a relevant Venn diagram that depicts, in a conceptual frame, what we know, what we do not know, what has happened in the past, and what is the current state.

Threat is a string of conditional probabilities. The Venn diagram above sums up the idea of conditional probabilities, but we may be able to go further in the analysis. Intelligence analysts have used several analytical techniques in order to combine vast amounts of information in complex systems. Among these is the Kalman Filter, developed by Rudolf Kalman [47]. Used by engineers and adapted by financial and restructuring advisors in financially distressed business situations, the Kalman Filter estimates the state of a dynamic system from a series of incomplete or "noisy" measurements (Fig. 4).

The method begins with a thorough description of a past and present threat model [8]. That description may be quantitative, qualitative, or both. After past and present threat models are constructed, the next step is to identify and analyze the drivers (or forces) that acted on the past model to drive it to its present state. Drivers may be strong or weak, direct or indirect, reliable or unreliable, certain or uncertain. Through the use of extrapolation, projection, and forecasting, the analyst may then develop a set of scenarios in order to construct future threat models [8]. Extrapolation holds the drivers constant among past, present, and future stages of the threat model; projection accounts for dynamic drivers among the threat models; and forecasting accounts not only for dynamic drivers but also for new drivers that may emerge and former drivers, may become irrelevant. During each step of the process, the analyst must assess information credibility, determine convergent or divergent information, and render an opinion as to the analyst's confidence in the models, drivers, and predictions.

Analysts use scenarios to identify relatively large drivers. According to Clark, analysts use four types of scenarios [8]: (i) demonstration scenarios (imagine an end state and then describe a plausible path to achievement); (ii) driving-force scenarios (identify and manipulate forces at work on the process, typically holding them constant or at some predetermined rate of change, to derive multiple futures); (iii) system-change scenarios (a cross-impact analysis that accounts for changing forces in a probabilistic manner and emerging synergies and degradations to derive multiple futures); and (iv) slice-of-time

scenarios (an analysis that jumps to a future state without an explanation of how that state was derived).

The Kalman Filter technique, through the use of driving-force or system-change scenario modeling, leads us back to the beginning of this article, to the original drivers of threat that exist within a cultural space: (i) capability, (ii) intent, and (iii) authority (external/internal). These general drivers are then further subdivided into more specific ones.

**Threat Drivers**

- *Capability*
  - Operational
  - Technological
  - Logistical
- *Intent*
  - General
- Strategic
- Operational
- Tactical
  - Specific
- Strategic
- Operational
- Tactical
- *Authority*
  - Existence of *fatwa*
  - Acceptance of *fatwa*
  - Contra-*fatawa* (a fatwa that counters, refutes, or distinguishes the fatwa of interest)
  - Other sources of authenticity, authority, resonance
- Treatises
- Symbols
- Signs
- Song
- *Cultural*
  - Social dynamics
  - Demographic trends
  - Economic trends
  - Political (internal/external)
  - Communications
  - Education
  - Religion
  - Song
  - Story
  - Myth

For example, based on this analysis, we have determined that al-Qaeda has never conducted an operation that had not been previously sanctioned by a *fatwa*. Thus, a *fatwa* is a strong, direct, and reliable indicator of threat. In fact, we have also learned that al-Qaeda has called off at least one operation where no *fatwa* permitted the operation and that lack of a *fatwa* played an indirect role in terminating an al-Qaeda operative where he had regularly exceeded his authority.

These observations lead us to the final step in the threat assessment process, that is, monitoring. Analysts must be active participants in the intelligence loop. For example, the use of the culture-centric threat model identified above where we have identified the existence of a *fatwa* as a strong, direct, and reliable driver has led us to the development of various weapons of mass destruction (WMD) scenarios. The planned attack by an al Qaeda cell that was called off involved a chemical attack in a subway system in the United States. Such an unprecedented attack mode (at least for Jihadists) with the potential for heavy collateral damage to non-Muslims who are noncombatants and Muslims who may use the subway led Ayman al-Zawahiri to request the opinion of a Saudi religious authority. Shortly after that request, Nasser bin Hamed al-Fahd, a prominent Saudi *Salafi* scholar, in an Islamic ruling published in May 2003, approved the use of WMDs against America [48]. He based his indictment on the principle of retaliation, and argued that Muslims have the right to kill 10 million Americans in response to the crimes of their government against the Muslim nation [48]. Al-Fahd elaborated the circumstances under which it is religiously permitted to kill noncombatant Americans: during a military operation when it is hard to distinguish between soldiers and civilians and according to military needs or considerations [48]. Ascribing great importance to the military considerations, he asserted that the military leaders who are responsible for the execution of *jihad* have the authority to make the decisions concerning what types of weapons to use against the infidels. If they decided to use WMDs based on military need, it would be an obligation under Islamic law to use them [48]. Although a thorough analysis of this *fatwa* is beyond the scope of this article, it is important to note that the attack means permitted the use of WMDs particularly chemical agents (and except, possibly the use of biologics), in targeting mass transportation in the United States. This is what we label a dangling *fatwa*, one that exists without a corresponding terrorist event as of yet. Based on our analysis, the intelligence analyst may want to monitor closely any technological developments in the processing or dispersing of chemical agents, access to WMD technology, and the emergence of alliances between al-Qaeda and various right-wing groups located in the Continental United States and Europe with chemical manufacturing and dispersion expertise.

## 4 OBSERVATIONS

Intelligence analysis may be divided into three separate but interdependent stages: (i) collection, (ii) management, and (iii) understanding. Robust threat assessments call on the skills necessary to discharge the three steps in the analytical process at a high level of sophistication. As we migrate from a threat space where we envision threat from a nation-state to threat from a non-state actor, we must refocus our efforts on a more robust threat model that accounts not only for the traditional drivers of capability and intent, but also incorporates authority and cultural drivers in our efforts to build meaningful scenarios that may help us in constructing a predictive model of threat. Yesterday's threat

is history; tomorrow is where we confront threat head-on. Throughout this process, we must remain cognizant of one sobering condition that permeates threat assessments and humbles analysts and academics alike. Many of us were taught deep in our youth that "the truth shall set you free." For an analyst, that translates into a quest for the truth so that we may meaningfully inform our intelligence client. The humbling fact is that there is someone just as committed to obfuscate or hide the truth from us. The attainment of truth involves a constant struggle in an ever-changing environment with a cunning adversary who is fighting back. As intelligence analysts, we will never know the truth until it is too late. We may only approximate it. However, truth is not our ultimate goal, it is not an end in itself; it is our means toward victory.

## REFERENCES


1. Shulsky, A. N., and Schmitt, G. J. (2002). Silent warfare. *Understanding the World of Intelligence 1–30*, 3rd ed. Brassey's, Inc., Washington, DC.
2. Khalsa, S. (2004). *Forecasting Terrorism 1–59*. Scarecrow Press, Inc., Lanham, MD.
3. Department of Homeland Security (2006). *National Infrastructure Protection Plan 39*, USA.
4. Williams, J. F. (2007) al-Qaeda strategic threats to the international energy infrastructure: authority as an integral component of threat assessment. *Proceedings of Carlton University–Ottawa Center for Infrastructure Protection*.
5. Williams, J. F. (2007) The nature of the terrorist threat. *Proceedings of Conference Board of Canada–Targeting the World's Transportation Systems*.
6. Weinberg, D. M., Coplon, G. H., and Williams, J. F. (2008). Understanding terrorism risk and its possible impacts. *Oil Gas J.*
7. Pattakos, A. N. (Pat) (1998). Threat analysis: defining the adversary. *Competitive Intelligence Review*, Vol. 9(2). John Wiley & Sons.
8. Clark, R. M. (2004). *Intelligence Analysis: A Target-Centric Approach*. CQ Press, Washington, DC, pp. 99, 105, 108–110, 113, 137–138, 166–173, 200–201, 204–205, 214–215, 262–263.
9. *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction; Report to the President of the United States 378–379 (2005)*, USA.
10. Director of National Security (effective July 11, 2006). *Intelligence Community Directive Number 301*. National Open Source Enterprise.
11. National Commission on Terrorist Attacks Upon the United States (9-11 Commission) (2004). *Final Report of the National Commission on Terrorist Attacks Upon the United States*, 413.
12. Cragin, K., and Daly, S. D. (2004). *The Dynamic Terrorist Threat: An Assessment of Group Motivations and Capabilities in a Changing World*. RAND Project Air Force.
13. Lesser, I. O., Hoffman, B., Arquilla, J., Ronfeldt, D., Zanini, M. (1999). *Countering the New Terrorism*. RAND, Santa Monica, CA.
14. Hoffman, B. (1999). Terrorism trends and prospects 19–20 and n.33. In *Countering the New Terrorism*, I. O. Lesser, et al., Ed. RAND, Santa Monica, CA.
15. Bar, S. (2006). *Warrant for Terror: The Fatwas of Radical Islam, and the Duty of Jihad*. Rowman & Littlefield, Stanford, CA.
16. McCants, W., Ed. (2006). *Combating Terrorism Center, U.S. Military Academy; Militant Ideology Atlas*. Combating Terrorism Center, West Point, NY.
17. E.g., Qutb, S. (1964). *Ma'alim fi al-Tariq ("Signposts on the Road" or "Milestones")*.
18. Hoffman, B. (1998). *Inside Terrorism 162*. Columbia University Press, New York.
19. Kepel, G. (2003). *The Trial of Political Islam*. Belknap Press.

20. Santos, E.Jr., and Negri, A. (2004). Constructing adversarial models for threat/enemy intent prediction and inferencing. *5423 Enabling Technologies for Simulation Sciences VIII: Int'l Society for Optical Engineering*.
21. Bringer, B. E., et al. (2007). *Security Risk Assessment and Management 11*. John Wiley & Sons.
22. Hunter, T. (1997). *Bomb School International Training Camps*. *Janes Intelligence Review*.
23. Heuer, R. J. (1999). *Psychology of Intelligence Analysis*. Central Intelligence Agency Center for the Study of Intelligence.
24. Heuer, R. J. (1981). Strategic deception and counterdeception: a cognitive approach. *Int. Stud. Q.*, **25**(2), 294–327.
25. Jones, R. V. (1995). Enduring principles: some lessons in intelligence. *CIA Stud. Intell.*, **38**(5), 37–42.
26. Jones, R. V. (1989). *Reflections on Intelligence*. Mandarin, London.
27. Whaley, B., and Busby, J. (2002). Detecting deception: practice, practitioners, and theory. In *Strategic Denial and Deception: The Twenty-First Century Challenge*, R. Godson, and J. J. Wirtz, Eds.
28. Johnson, P. E., et al. (2001). Detecting deception: adversarial problem solving in a low base-rate world. *Cogn. Sci. Multidisciplinary J.* **25**(3), 355–392.
29. Stech, F. J., and Elsaesser, C. (2005). *Deception of Detection by Analysis of Competing Hypotheses*. The MITRE Corporation.
30. Stech, F. J., and Elsaesser, C. (2004). *Midway Revisited: Detecting Deception by Analysis of Competing Hypotheses*. The MITRE Corporation.
31. McFate, M., and Jackson, A. (2005). An organizational solution for DoD's cultural knowledge needs. *Mil. Rev.*
32. United States Marine Corps (USMC) (1940). *United States Marine Corps Small Wars Manual*. Sunflower University Press, Manhattan, KS.
33. Kipp, L., et al. (2006). The human terrain system: a CORDS for the 21st century. *Mil. Rev.*
34. Lewis, B. (2003). *The Crisis of Islam: Holy War and Unholy Terror*. Random House, New York. (A concise treatment of the role religion may play in militant movements within Islam with an elegant treatment of Islamic history in context).
35. Esposito, J. L. (2002). *Unholy War: Terror in the Name of Islam*. Oxford University Press, New York. (Another important treatment of the role or, to be more precise, the abuse of religion by militant movements within Islam, but from a different, but equally persuasive, perspective than that of Professor Lewis).
36. Kepel, G. (2004). *The War for Muslim Minds*. Harvard University Press, Cambridge, MA. (Among one of the most gifted scholars of political Islam or Islamism, the book presents an insightful treatment of militant Islam from a cultural perspective with an excellent critique of the post 9-11 al-Qaeda leadership and organizational structure).
37. Patai, R. (2002). *The Arab Mind*, Rev. ed. Hatherley Press, New York. (Dismissed by some as outdated or insensitive; to others, a treasure trove of information through its comprehensive treatment of the subject, especially its careful selection of Arab authors addressing several sensitive cultural subjects; you may disagree with Dr. Patai, but any serious treatment of Arabic culture must confront his work head on).
38. Pryce-Jones, D. (2002). *The Closed Circle: An Interpretation of the Arabs*. (Thoughtful treatment of how tribal, religious, and cultural traditions drive the Arabs in their dealings with each other and with the West).
39. Nydell, M. K. (2006). *Understanding Arabs: A Guide for Modern Times*, 4th ed. Intercultural Press, Yarmouth, ME. (From the perspective of a linguist, this book does a good job of covering the cultural waterfront of Arabs in the Middle East; although she takes issue with Dr. Patai

on a number of points, her observations, with several notable exceptions, are quite consistent with Dr. Patai's own observations).

40. Ruthven, M., and Nanji, A. (2004). *Historical Atlas of Islam*. Harvard University Press, Cambridge. (One of the best short introductions to Islamic history with engaging but concise text, a beautiful use of maps, and splendid pictures).
41. Williams, J. F. (2005). *The Battle Within Islam: Militant Movements in Islam and the Threat They Pose to the West and to Mainstream Muslims*. The MITRE Corporation.
42. Ruthven, M. (2000). *Islam: A Short Introduction*. (one of the best short introductions to Islam as religion, culture, and politics).
43. Algar, H. (2000). *The Sunna: Its Obligatory and Exemplary Aspects*. Islamic Publications International, New York.
44. Ali, M. M. (2001). *A Manual of Hadith*.
45. Mitchell, R. P. (1993). *The Society of the Muslim Brothers*. Oxford University Press, New York.
46. Masud, M. K., Messick, B., and Powers, D. S., Eds. (1996). *Islamic Legal Interpretation: Muftis and Their Fatwas*. Harvard University Press, Cambridge, MA.
47. Kalman, R. E. (1960). A new approach to linear filtering and prediction problems. *Trans. ASME J. Basic Eng.* **82**, 35–45.
48. Hamd Al-Fahd, N. B. (2003). *A Treatise on the Legal Status of Using Weapons of Mass Destruction Against Infidels (May 2003 [Rabi' I 1424])*.

## FURTHER READING

*Al-Qaeda Training Manual*.

CIA. (2007). *The World Fact Book*.

*Proceedings of the Kuala Lumpur International Forum on Islam*. (2002).

The Holy Qur'an.

The Koran. (N. J. Dawood trans. 1956 and updated 1999).

The Noble Qur'an.

Time Almanac (2008).

United Nations Arab Human Development Report (2002).

## BOOKS

1. Ajami, F. (1998). *Dream Palace of the Arabs: A Generation's Odyssey*.
2. Algar, H. (2000). *The Sunna: Its Obligatory and Exemplary Aspects*.
3. Algar, H. (2002). *Wahhabism: A Critical Essay*.
4. Algar, H. (1997). *Surat Al-Fatiha: Foundation of the Qur'an*.
5. Ali, M. M. (2001). *A Manual of Hadith*.
6. Anonymous. (2002). *Through our Enemies' Eyes: Osama bin Laden, Radical Islam, and the Future of America*.
7. Anonymous. (2004). *Imperial Hubris: Why the West is Losing the War on Terror*.
8. Armstrong, K. (2000). *The Battle for God: A History of Fundamentalism*.
9. Armstrong, K. (2000). *Islam: A Short History*.
10. Armstrong, K. (2001). Was it inevitable? In *How Did This Happen? Terrorism and the New War*, J. F. Hoge, and G. Rose, Eds.

11. Bakhtiar, L. (1996). *Encyclopedia of Islamic Law: A Compendium of the Major Schools*.
12. Beckett, I. F. W. (2001). *Modern Insurgencies and Counter-Insurgencies*.
13. Benjamin, D., and Simon, S. (2002). *The Age of Sacred Terror*. Random House, New York.
14. Bergen, P. L. (2001). *Holy War, Inc.*
15. Carr, C. (2002). *The Lessons of Terror*.
16. Cohen, M. (1994). *Under the Crescent and the Cross: The Jews in the Middle Ages*
17. Doi, A. R. I. (1984). *Shariah: The Islamic Law*.
18. El Fadl, K. A. (2001). *Rebellion and Violence in Islamic Law*.
19. El Fadl, K. A. (2001). *Speaking in God's Name: Islamic Law, Authority and Women*.
20. El Fadl, K. A., (with Ali, T., Viorst, M., and Esposito, J., et al. (2002). *The Palace of Tolerance in Islam*.
21. Esposito, J. (2000). *The Oxford History of Islam*.
22. Esposito, J. (1999). *The Islamic Threat: Myth or Reality?* 3rd ed.
23. Esposito, J. (2004). *Islam: The Straight Path*.
24. Esposito, J. L. (2002). *Unholy War: Terror in the Name of Islam*.
25. Fuller, G. (2003). *The Future of Political Islam*.
26. Habeck, M. (2006). *Knowing the Enemy: Jihadist Ideology and the War on Terror*.
27. Hitti, P. (1967). *History of the Arabs from Earliest Times to the Present*, 9th ed., (emphasis on Islamic culture, arts, and sciences).
28. Huband, M. (1999). *Warrior of the Prophet: The Struggle for Islam*.
29. Huntington, S. (1996). *The Clash of Civilizations and the Remaking of World Order*.
30. Jones, R. V. (1978). *Most Secret War*.
31. Juergensmeyer, M., Ed. (1992). *Violence and the Sacred in the Modern World*.
32. Juergensmeyer, M. (1993). *The New Cold War?*
33. Juergensmeyer, M. (2000). *Terrorism in the Mind of God*.
34. Kent, S. (1966). *Strategic Intelligence for American World Policy*.
35. Kepel, G. (2004). *The War for Muslim Minds*.
36. Kramer, M. (1987). *The Moral Logic of Hizbullah*.
37. Laqueur, W. (1977). *Terrorism*.
38. Laqueur, W. (1979). *The Terrorism Reader*.
39. Laqueur, W. (1999). *The New Terrorism: Fanaticism and the Arms of Mass Destruction*.
40. Ledeen, M. A. (2003). *The War Against the Terror Masters*.
41. Lewis, B. (2003). *The Crisis of Islam: Holy War and Unholy Terror*.
42. Lewis, B. (2002). *What Went Wrong? Impact and Middle Eastern Response*.
43. Lewis, B. (1960). *The Arabs in History*.
44. Lewis, B. (1968). *The Assassins: A Radical Sect in Islam*.
45. Lewis, B. (1991). *The Political Language of Islam*.
46. Lewis, B. (1995). *The Middle East: A Brief History of the Last 2000 Years*.
47. Lewis, B. (2001). *Music of a Distant Drum: Classical Arabic, Persian, Turkish and Hebrew Poems*.
48. Lewis, B. (2001). *Islam in History: Ideas, People, and Events in the Middle East*.
49. Lewis, B. (2004). *From Babel to Dragomans: Interpreting the Middle East*.
50. Marty, M. E., and Appleby, S. R. (1995). *Fundamentalism Comprehended*.
51. O'Neill, B. E. (1990). *Insurgency & Terrorism: Inside Modern Revolutionary Warfare*.
52. Pipes, D. (1996). *The Hidden Hand: Middle East Fears of Conspiracy*.

53. Pipes, D. (2002). *Militant Islam Reaches America*.
54. Qutb, S. (Hamid Algar trans. 2000). *Social Justice in Islam*.
55. Ramadan, T. (1999). *To Be a European Muslim*.
56. Roolvink, R. (1958). *Historical Atlas of the Muslim People*, (Best collection of maps of Muslim world at important times in history).
57. Roy, O., and Volk, C. (1998). *The Failure of Political Islam*.
58. Sageman, M. (2004). *Understanding Terror Networks*.
59. Schanzer, J. (2005). *Al-Qaeda's Armies: Middle East Affiliate Groups and the Next Generation of Terror*.
60. Schacht, J. (1982). *An Introduction to Islamic Law*.
61. Shanor, C. A., and Hogue, L. L. (2003). *National Security and Military Law*.
62. Sprinzak, E. (1999). *Brother Against Brother*.
63. Thompson. L. (2002). *The Counter Insurgency Manual*.
64. Tibi, B. (1998). *The Challenge of Fundamentalism: Political Islam and the New World Disorder*.
65. Townshend, C. (2002). *Terrorism: A Very Short Introduction*.
66. Treverton, G. (2003). *Reshaping National Intelligence for an Age of Information*.
67. Trimble, P. R. (2002). *International Law: United States Foreign Relations Law*.
68. Von Grunebaum, G. E. (K. Watson trans. 1970). *Classical Islam*.
69. Ye'or, B. (2002). *Islam and Dhimmitude: Where Civilizations Collide*.

## ARTICLES AND ESSAYS

1. Vlahos, M. (2002). *Terror's Mask: Insurgency Within Islam*. Johns Hopkins University Applied Physics Laboratory, Laurel, MD.
2. Aboul-Enein, Y. H., and Zuhur, S. (2004). *Islamic Rulings on Warfare*. Strategic Studies Institute, Carlisle, PA.
3. Anspach, M. (1991). Violence against violence: Islam in historical context. *Terrorism and Political Violence 3, 3*.
4. Brei, W. S. (1996). *Getting Intelligence Right: The Power of Logical Procedure*. Joint Military Intelligence College, Washington, DC.
5. Cordesman, A. H. (2004). *The Intelligence Lessons of the Iraq War(s)*. Center for Strategic Studies.
6. Halliday, F. (2000). Terrorisms in historical perspective. *Nation and Religion in the Middle East*. Lynne Rienner Publishers, Boulder, CO.
7. Merari, A. (1990). The readiness to kill and die: suicidal terrorism in the middle east. In *Origins of Terrorism: Psychologies, Ideologies, States of Mind*, W. Reich, Ed.
8. Rapoport, D. (1984). Fear and trembling: terrorism in three religious traditions. *Am. Polit. Sci. Rev.* **78**(3), 658–677.
9. Schwartz, S. (2004). *Rewriting the Koran. The Weekly Standard 19 Sep 27 2004*.

## OPEN-SOURCE INTERNET SITES

1. http://www.odl.state.ok.us/usinfo/terrorism/911.htm (Collections of annotated bibliographies by Oklahoma Department of Libraries)

2. http://www.nyazee.com/islaw/Islamic%20Law%20Infobase.html (Islamic Law Infobase)
3. http://www.odci.gov/cia/publications/factbook/ (*CIA World Factbook* 2007)
4. http://www.bartleby.com/65/ (*Columbia Encyclopedia*)
5. http://www.arches.uga.edu/%7Egodlas/maps.html (populations, maps, and countries of Muslim world)
6. http://www.lib.utexas.edu/maps (maps)
7. http://www.umr.edu/∼msaumr/topics/ (English translation and interactive topical index to Quran)
8. http://www.acs.ucalgary.ca/∼elsegal/I_Transp/IO6_Shia.html (sectarian discussion of Sunni/Shia)
9. http://www.fordham.edu/halsall/islam/islamsbook.html (Islamic history)
10. http://www.acs.ucalgary.ca/∼elsegal/I_Transp/Ilist.html (class notes on Islam)
11. http://www.quran.org/ (authenticated English translations [and other languages] of the Quran)
12. http://www.carm.org/islam/faith_imam.htm (Introduction to Islam from nonMuslim source with chart comparison to Christianity)
13. http://al-islam1.org/laws/ (Islamic law)
14. http://www.mb-soft.com/believe/txo/wahhabis.htm (Wahhabism)
15. http://www.wsu.edu/∼dee/ISLAM/UMAY.HTM (Islamic history)
16. http://www.eppc.org/ (Contains transcripts of conversations by leading scholars on Political Islam, Iraq, and Terrorism)
17. www.arabia.com
18. www.islamfortoday.com
19. www.memri.org (Middle East Media Research Institute)
20. www.saudiinstitute.org (Saudi reformers)

# RISK ANALYSIS METHODS FOR CYBER SECURITY

MICHEL CUKIER AND SUSMIT PANJWANI
*University of Maryland, College Park, Maryland*

## 1 INTRODUCTION

Executive Order 13010 defines the nation's critical infrastructure as "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire,

and rescue), and continuity of government" [1]. Traditionally, the nation's critical infrastructure assets were considered independently from the information assets. However, the development of an information-based economy and the wide proliferation of the Internet have changed the way these critical infrastructure assets are accessed, maintained, and used. The critical infrastructures are now exposed to a different threat profile raised by the interdependence of information assets and critical infrastructure assets.

This is clearly illustrated in the Clinton Administration's Policy on Critical Infrastructure Protection (CIP). Presidential Decision Directives (PDD) 62 and 63, released on May 22, 1998 by President Clinton address the new and nontraditional "cyber-security" threats against critical infrastructure [2, 3]. PDD 63 is the key directive focusing on CIP from both the physical and cyber security perspective [3, 4].

On October 16, 2001, President Bush announced Executive Order 13231, entitled "Critical Infrastructure Protection in the Information Age" [5]. In this executive order, President Bush explicitly stated that "the information technology revolution has changed the way business is transacted, government operates, and national defense is conducted" [6, 7]. Executive Order 13231 established the President's Critical Infrastructure Protection Board [5].

## 2 SECURITY RISK ASSESSMENT

The aforementioned directives emphasize the gravity of the new and evolving risk associated with cyber-security. A security risk assessment framework is needed to quantify this risk. Research has been conducted to define guidelines and frameworks. These frameworks should be leveraged to drive the investment decisions regarding critical infrastructure assets.

The Office of Management and Budget (OMB) Circular A-130, "Security of Federal Automated Information Resources", mandated that the federal agencies must "consider risk when deciding" which security countermeasures to implement [8, 9]. According to the circular, a "risk-based approach" should be adopted to determine the adequate level of security [8, 9]. This circular encourages agencies to consider "major risk factors, such as the value of the system or application, threats, vulnerabilities, and the effectiveness of safeguards" [8, 9]. The OMB Director further emphasized this risk-based approach to security when he issued Memorandum 99-20, "Security of Federal Automated Information Resources", explicitly stating the importance of "continually assessing the risk" associated with information assets to maintain adequate levels of security [9, 10].

Recognizing the gravity of the cyber-security threat, the National Institute of Standards and Technology (NIST) also released guidelines on security risk assessment, contained in "An Introduction to Computer Security: The NIST Handbook" [11] and "Generally Accepted Principles and Practices for Securing Information Technology Systems" [12].

The need for implementing cost-effective, risk-based information security programs was further emphasized by The Federal Information Security Management Act of 2002 [13]. The act was meant to strengthen computer security within the federal government and affiliated parties (such as government contractors) by mandating yearly audits.

## 3 A QUANTITATIVE APPROACH TO CYBER-SECURITY RISK ASSESSMENT

The main aspect of making a risk-based decision is the significance of the data used to make the decision. Often this data is collected in the form of expert opinion or the attack trend observed on the Internet. Because of the continuous evolution of the Internet, the attack trend changes rapidly, and it is important to quantify this evolving attack threat to develop appropriate countermeasures. Moreover, the attack trend observed by an organization may differ from the attack trend observed on the Internet. Indeed, the complexity and technology used by organizations to build their information infrastructure may differ significantly from the networks seen on the Internet. Hence, it is crucial that organizations measure the attack trend at the organization level to make more accurate decisions.

In this article, we present a quantitative approach to security risk assessment that can be used to make risk-based decisions using data representative of the organization's infrastructure. The core of the quantitative risk assessment is the ability to form and evaluate critical hypotheses based on attack data and to perform attack trend analysis. In this article, we describe how quantitative data can be leveraged for (i) hypothesis evaluation and (ii) attack trend analysis. The research test-bed that was used to collect the data and two empirical experiments are also described.

## 4 DATA COLLECTION AND ANALYSIS

The experimental test-bed used in this research consisted of two target computers used just for the purpose of being attacked. Other computers were used to closely monitor the target computers, however, attackers were unaware that they were observed. This architecture is similar to the one developed by the Honeynet project [14]. Differences between the two architectures and details on the deployed architecture are presented in Ref. 15.

The selected subnet for the target computers is unmonitored; IP addresses are assigned to users dynamically. Both target computers ran Windows 2000 and had the same services (i.e. IIS, FTP, Telnet, and NetTime [16]) and the same vulnerabilities maintained throughout the data collection period. Twenty-five vulnerabilities, shown in Table 1, were selected to cover a broad range of discovery dates (from 2000 to 2004), various services (i.e. RPC, LSA, IIS, FTP, HTTP, and Telnet), and different levels of criticality (i.e. Critical, Important, Moderate, and Low). Note that most UDP traffic was filtered at the gateway level, which is why the analysis focused on ICMP and TCP traffic. The outbound traffic was limited to 10 TCP connections per hour, 15 ICMP connections per hour, and 15 other connections per hour.

The traffic was filtered at multiple stages before being analyzed. The data consisted of (i) malicious traffic from the Internet and (ii) management traffic like spanning tree protocol (STP) traffic generated by the bridge, DNS resolutions, and NTP queries. The data were parsed into a format that could be stored in a database. The data were then parsed based on a protocol to filter out the remaining management traffic. Traffic not directed toward either target computer was also filtered.

**TABLE 1 List of Vulnerabilities Remaining on the Target Computers**

| Year | Bulletin Number | Service | Criticality | Vulnerability Description |
|---|---|---|---|---|
| 2004 | MS04-012 | RPC/DCOM | Critical | Race condition |
| 2004 | MS04-012 | RPC/DCOM | Important | Input vulnerability |
| 2004 | MS04-012 | RPC/DCOM | Low | Buffer overflow |
| 2004 | MS04-012 | RPC/DCOM | Low | Input vulnerability |
| 2004 | MS04-011 | LSA | Critical | Buffer overflow |
| 2004 | MS04-011 | LSA | Moderate | Buffer overflow |
| 2003 | MS03-010 | RPC endpoint mapper | Important | Vulnerability not clearly specified |
| 2003 | MS03-018 | IIS | Important | Memory vulnerability |
| 2003 | MS03-026 | RPC interface | Critical | Buffer overflow |
| 2003 | MS03-049 | Workstation service | Critical | Buffer overflow |
| 2003 | MS03-039 | RPC | Critical | Buffer overflow |
| 2002 | MS02-062 | IIS | Moderate | Memory vulnerability |
| 2002 | MS02-018 | FTP | Critical | Vulnerability not clearly specified |
| 2002 | MS02-018 | HTTP | Critical | Buffer overflow |
| 2002 | MS02-004 | Telnet | Moderate | Buffer overflow |
| 2001 | MS01-041 | RPC | Not rated | Input vulnerability |
| 2001 | MS01-044 | IIS | Not rated | Input vulnerability |
| 2001 | MS01-026 | IIS | Not rated | Vulnerability not clearly specified |
| 2001 | MS01-026 | FTP | Not rated | Memory vulnerability |
| 2001 | MS01-026 | FTP | Not rated | Vulnerability not clearly specified |
| 2001 | MS01-016 | IIS WebDAV | Not rated | Input vulnerability |
| 2001 | MS01-014 | IIS exchange | Not rated | Input vulnerability |
| 2000 | MS00-086 | IIS | Not rated | Vulnerability not clearly specified |
| 2000 | MS00-078 | IIS | Not rated | Input vulnerability |
| 2000 | MS00-057 | IIS | Not rated | Input vulnerability |

## 5 HYPOTHESIS EVALUATION: ARE PORT SCANS PRECURSORS TO AN ATTACK?

In this section, we show how quantitative data can be utilized to evaluate security related hypotheses. The security community continues to debate if port scans are considered to be precursors to an attack. The case study described in this section (i.e. a short version of experiment described in Ref. 15) shows how the data collection architecture previously described to quantify such an assumption can be leveraged.

### 5.1 Data Filtering

In order to determine the link between scans and attacks, we filtered the malicious traffic collected into four categories: ICMP scans, port scans, vulnerability scans, and attacks. ICMP scans can be easily recognized by their protocol. Regarding port scans, as reported by Ref. 17, three packets are sufficient to finish a TCP handshake and establish a connection. Information on open ports and services can be gathered by using as few as two packets. We showed empirically using Nmap [18] in Ref. 15 that in 99.8% of the cases, port scans were defined as connections with four or fewer packets. Regarding vulnerability scans, we ran NeWT 2.1 [19] and showed empirically that 99.9% of the

vulnerability scans consisted of connections having between 6 and 12 packets. Based on these results:

- port scans were characterized as connections with less than five packets;
- vulnerability scans were characterized as having connections between 5 and 12 packets; and
- attacks were characterized as connections with more than 12 packets.

### 5.2 Data Analysis

The goal of the experiment was to analyze the link between scans and attacks. Therefore, we only kept unique scans and attacks. For example, if multiple port scans were launched from one specific source IP address toward one of the target computers, we recorded that this source IP address had launched at least one port scan without recording the actual number of port scans. Similarly, if one source IP address launched several attacks (of the same type or of different types) against one of the target computers, we recorded that at least one attack had been launched from that source IP address against the target computer. The link between the 22,710 connections of malicious activity (collected over a period of 48 days) and unique ICMP scans, port scans, vulnerability scans, and attacks is shown in Table 2.

For each of the 760 attacks from different source IP addresses, we checked if a scan or combination of scans was linked to the attack (from the same source IP address toward the same target computer). The number and percentage of direct attacks (i.e. attacks not linked to a scan) and attacks linked to different scans and combinations of scans are provided in Table 3. We observed that more than 50% of the attacks were not linked to a scan. However, over 38% of the attacks were linked to a vulnerability scan. Port scans and combinations of port and vulnerability scans were linked to 3–6% of the attacks.

### 5.3 Interpretation of Results

These experimental results indicated that the majority of the attacks were not linked to a scan. When scans were linked to attacks, the most frequent ones were (i) a vulnerability scan, (ii) a combination of port and vulnerability scans, and (iii) a port scan.

One explanation for these observations might be the large number of automated attacks captured by the honeypot-based test-bed. These attacks were developed in a manner to fingerprint the vulnerability rather than the machine they were trying to compromise.

**TABLE 2 Distribution of Malicious Activity: Nonunique and Unique Records**

| Malicious Activity | No. of Records | No. of Unique Records |
|---|---|---|
| ICMP scans | | 3007 |
| Port scans | 8432 | 779 |
| Vulnerability scans | 2583 | 1657 |
| Attacks | 2035 | 760 |
| Total | 22,710 | 6203 |

**TABLE 3 Distribution of Scans Linked to an Attack**

| Type of Scan | No. Attacks Linked to a Scan | Percentage of Attacks |
|---|---|---|
| Port | 28 | 3.68 |
| ICMP | 1 | 0.13 |
| Vulnerability | 296 | 38.95 |
| Port & ICMP | 0 | 0 |
| Port & vulnerability | 42 | 5.53 |
| ICMP & vulnerability | 5 | 0.66 |
| Port & ICMP & vulnerability | 7 | 0.92 |
| None | 381 | 50.13 |

This section illustrated how the data collection architecture could be used to address issues associated with the cyber-security threat, like the potential link between scans and attacks.

## 6 ATTACK TREND ANALYSIS: COMPARISON BETWEEN INTERNAL AND EXTERNAL MALICIOUS TRAFFIC

Often, organizations make security decisions based on the malicious activity observed and recorded on the Internet. Using this method, malicious traffic originating inside of the organization is overlooked. We conducted two studies to compare malicious traffic originating inside of the organization (called *internal traffic*) to malicious traffic originating from outside of the organization (called *external traffic*). We analyzed the correlation between internal and external malicious traffic at two different levels. First, we conducted an analysis at a higher level, correlating the internal and external malicious traffic solely on the basis of the number of connections. We then refined the analysis by considering the number of connections targeted toward specific ports.

The data used for this analysis was collected over a period of 15 weeks from October 4, 2004 to January 16, 2005. The data were subdivided into weeks (week 1–52) with week 1 corresponding to the period October 4–10, 2004. In week 7, data were collected from 6 (out of 7) days and in weeks 5 and 8, data were collected from 5 days. From the malicious traffic on both target computers, we filtered out: (i) ICMP scans that were identified through the protocol and (ii) port scans that were identified based on the number of packets per connections (i.e. connections with a maximum of four packets).

Correlation coefficients were calculated based on the 15 data points obtained during the 15-week long data collection period to form the basis of one aspect of the comparison. We applied Guilford's [20] interpretation of the correlation coefficient (i.e. no correlation = "N", low correlation = "L", moderate correlation = "M", high correlation = "H", and very high correlation = "VH"):

- correlation coefficients lower than 0.2: no correlation (N),
- correlation coefficients between 0.2 and 0.4: low correlation (L),
- correlation coefficients between 0.4 and 0.7: moderate correlation (M),
- correlation coefficients between 0.7 and 0.9: high correlation (H), and
- correlation coefficients higher than 0.9: very high correlation (VH).

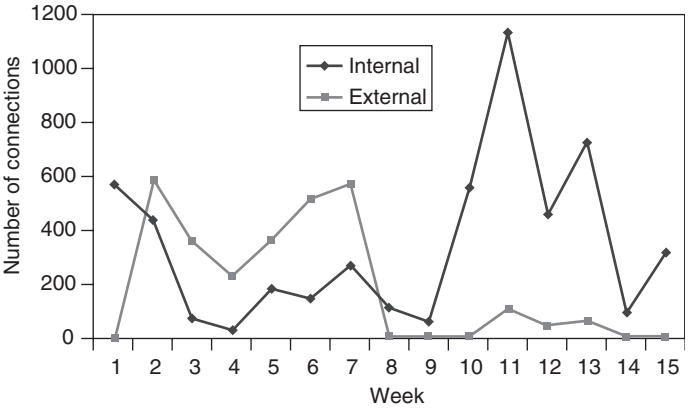



**FIGURE 1** Number of internal/external connections per week.

### 6.1 Correlation 1: Number of Connections

In this section we compare internal and external malicious traffic based on the number of malicious connections. Over the 15-week data collection period, the two target computers received a total of 8029 malicious connections. 5,174 of the connection (64.4%) originated from within the organization and 2855 (35.6%) originated from outside of the organization. Figure 1 shows the number of internal and external connections received each week. No clear relationship existed between internal and external malicious traffic as shown in Figure 1. This is further confirmed by calculating the correlation coefficient, −0.21, which indicated a low correlation between internal and external traffic. The average amount of internal malicious traffic was much higher than the external traffic (345 connections versus 191). As expected, just considering the number of connections was not sufficient for providing a detailed comparison between internal and external malicious traffic.

### 6.2 Number of Connections per Port

Since the type of malicious activity is linked to the port that is targeted, we focused on the ports targeted most frequently to compare internal and external malicious traffic. The set of ports consists of 21 (ftp), 22 (ssh), 23 (telnet), 80 (www-http), 135 (epmap), 139 (netbios-ssn), and 445 (microsoft-ds). This set of ports was targeted on an average by 87.2% of the internal traffic and 61.4% of the external traffic. Table 4 presents the number of connections associated with internal and external malicious traffic. For most ports, the number of internal connections differed from the number of external ones. To better compare internal and external traffic, the percentage of the number of connections targeting the selected set of ports is also shown in Table 4. For each port, the percentages between internal and external connections varied significantly. These observations are further confirmed when calculating the correlation coefficients between the number of connections per port. The correlation between internal and external malicious traffic was low for ports 21 and 445, and no correlation was observed for ports 22, 23, 80, 135, and 139. Port 445, which was targeted 29% (internal) and 55% (external) of the time, had a correlation coefficient of −0.2. Port 135, targeted 12% (internal) and 25% (external)

**TABLE 4 Total Number and Average of the Percentage of Connections per Port and Correlation Coefficients of the Number of Connections per Port**

| Port | 21 | 22 | 23 | 80 | 135 | 139 | 445 |
|---|---|---|---|---|---|---|---|
| Internal | 46 (0.6%) | 47 (0.6%) | 14 (0.2%) | 201 (3.2%) | 618 (11.7%) | 371 (6.3%) | 2716 (54.6%) |
| External | 33 (0.4%) | 20 (0.3%) | 36 (0.8%) | 130 (1.9%) | 256 (24.7%) | 178 (4.0%) | 810 (29.3%) |
| Correlation coefficient | −0.32 | −0.11 | −0.09 | −0.11 | −0.14 | 0.07 | −0.2 |

of the time, had an even lower correlation coefficient of −0.14. These results confirm that internal and external malicious traffic are weakly correlated (i.e. since no correlation coefficient exceeded 0.4, the malicious traffic has a low or no correlation).

### 6.3 Correlation 3: Correlation Across Ports

To further analyze the malicious traffic per port, we calculated the correlation coefficients between the various ports for the total, internal, and external malicious traffic. Tables 5, 6, and 7, respectively, provide the correlation coefficients for the total, internal, and external malicious traffic.

Table 5 contains the correlation coefficients for the total malicious traffic. These coefficients might lead to some inaccurate conclusions. Indeed, the correlation coefficient between ports 21 and 135 was low for the total traffic but was moderate for the internal and external traffic. Moreover, for ports 21 and 445, the total malicious traffic indicated a moderate correlation, but internal traffic indicated a high correlation and external traffic led to no correlation. These examples show that the total malicious traffic is not sufficient for comparing in detail the correlation across ports and that the origin of the malicious traffic should also be considered.

Based on Tables 6 and 7, we observed that the value of the correlation coefficient between two port numbers often differ between internal and external malicious traffic. The most significant differences between the correlation coefficient values were as follows:

- ports 21 and 445: high correlation (internal) and no correlation (external);
- ports 22 and 445: moderate correlation (internal) and no correlation (external);

**TABLE 5 Correlation Coefficients for Total Malicious Traffic**

| Port | 21 | 22 | 23 | 80 | 135 | 139 | 445 |
|---|---|---|---|---|---|---|---|
| **21** | 1 | | | | | | |
| **22** | 0.71 (H) | 1 | | | | | |
| **23** | 0.65 (M) | 0.47 (M) | 1 | | | | |
| **80** | 0.83 (H) | 0.88 (H) | 0.66 (M) | 1 | | | |
| **135** | 0.24 (L) | 0.38 (L) | 0.03 (N) | 0.39 (L) | 1 | | |
| **139** | −0.03 (N) | −0.31 (L) | 0.03 (N) | −0.05 (N) | 0.3 (L) | 1 | |
| **445** | 0.41 (M) | 0.58 (M) | −0.2 (L) | 0.52 (M) | 0.59 (M) | −0.11 (N) | 1 |

**TABLE 6 Correlation Coefficients for Internal Malicious Traffic**

| Port | 21 | 22 | 23 | 80 | 135 | 139 | 445 |
|---|---|---|---|---|---|---|---|
| **21** | 1 | | | | | | |
| **22** | 0.74 (H) | 1 | | | | | |
| **23** | 0.42 (M) | 0.27 (L) | 1 | | | | |
| **80** | 0.83 (H) | 0.92 (VH) | 0.4 (M) | 1 | | | |
| **135** | 0.4 (M) | 0.28 (L) | 0.04 (N) | 0.38 (L) | 1 | | |
| **139** | −0.03 (N) | −0.13(N) | 0.22 (L) | −0.11 (N) | 0.51 (M) | 1 | |
| **445** | 0.74 (H) | 0.7 (M) | 0.08 (N) | 0.81 (H) | 0.59 (M) | −0.07 (N) | 1 |

**TABLE 7 Correlation Coefficients for External Malicious Traffic**

| Port | 21 | 22 | 23 | 80 | 135 | 139 | 445 |
|---|---|---|---|---|---|---|---|
| **21** | 1 | | | | | | |
| **22** | 0.85 (H) | 1 | | | | | |
| **23** | 0.85 (H) | 0.89 (H) | 1 | | | | |
| **80** | 0.91 (VH) | 0.87 (H) | 0.9 (VH) | 1 | | | |
| **135** | 0.41 (M) | 0.48 (M) | 0.61 (M) | 0.59 (M) | 1 | | |
| **139** | 0.12 (N) | −0.14 (N) | 0.24 (L) | 0.28 (L) | 0.37 (L) | 1 | |
| **445** | 0.15 (N) | −0.08 (N) | −0.12 (N) | 0.27 (L) | 0.06 (N) | 0.29 (L) | 1 |

- ports 23 and 80: moderate correlation (internal) and very high correlation (external);
- ports 23 and 135: no correlation (internal) and moderate correlation (external);
- ports 80 and 445: high correlation (internal) and low correlation (external);
- port 135 and 445: moderate correlation (internal) and no correlation (external).

Attacks are linked to ports in different ways. Different attacks can target the same port (i.e. a DoS as well as a race condition attack may be launched against the same FTP server listening on port 21). Moreover, attacks may target more than one port during the attack (i.e. the Sasser worm targets ports 139 and 445). The relationship between attacks and ports show that attacks can be discriminated at a high level using the ports they target. When comparing internal and external malicious traffic, similar correlation coefficient values between ports indicated that internal and external malicious traffic were similar. Based on Tables 6 and 7, we observed that most of the time the correlation coefficients differ between internal and external traffic. This indicates that, even though some attacks might be similar for internal and external malicious activity, the majority differed. In sum, we found that the amount of malicious traffic differs between internal and external malicious activity and that the type of malicious traffic also differs.

## 7 APPLICATION OF QUANTITATIVE SECURITY ASSESSMENT

This article shows how security quantification helps to characterize the evolution of the attack threat. We briefly mentioned two applications of quantitative security assessment.

### 7.1 Critical Infrastructure Protection (CIP)

We mentioned the importance of cyber-security attacks against the critical infrastructure in the introduction. The first step in evaluating this attack threat was to determine the threat profile of the critical information infrastructure. The case study described in this article can be replicated to quantify the attack trend and profiles.

### 7.2 Intrusion Tolerance

Another solution to deal with evolving attack trends is the application of intrusion tolerance. Verissimo and colleagues [21] define intrusion tolerance as the ability of the system to "address the system faults and attacks in a seamless manner through a common approach to security and dependability". The main premise behind this concept is that because of the pervasiveness of the some form of vulnerability and attacks in the system, it might be beneficial to design the system to withstand attacks as opposed to trying to eliminate all vulnerabilities in the system. Refs. 21 and 22 are two examples where intrusion tolerance is provided at the middleware level.

## 8 DISCUSSION

Since the threat against critical infrastructure has evolved from a pure physical threat to a fusion of physical and cyber-security threat, particular attention needs to be focused on the cyber-security threat. Risk-based approaches are recommended for measuring and alleviating the cyber-security threat. The core of a risk-based approach lies in the ability to form and evaluate security assumptions. This article illustrates how empirical data can be utilized to quantify such assumptions. In particular, we assessed the assumption that port scans were precursors of an attack. We showed, based on malicious traffic, that the majority of the attacks were not linked to a scan. Another study focused on the assumption that internal and external malicious traffic are similar. We showed that using the number of connections is not sufficient for making a detailed comparison between internal and external malicious traffic. However, when refining the analysis of malicious traffic per port targeted, we showed that through the calculation of the correlation coefficients, internal and external malicious traffic often differs significantly.

Since the cyber-security threat varies greatly over time and external malicious traffic differs from internal traffic, a bias in the risk assessment could come from the use of: (i) expert opinions or (ii) malicious traffic collected on the Internet. This article makes the case for collecting continuous in-house data to accurately assess the cyber-security threat to avoid biasing the overall risk assessment study.

## REFERENCES

1. *President Clinton (1996). Executive Order EO 13010 Critical Infrastructure Protection*, http://www.fas.org/irp/offdocs/eo13010.htm.
2. Department of Justice (1998). *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63* , http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.

3. Department of Justice (1998). *Critical Infrastructure Protection*, http://www.cybercrime.gov/critinfr.htm.
4. Department of Justice (1998). Computer Crime and Intellectual Property Section (CCIPS). Presidential Decision Directive 63-protecting the nation's critical infrastructure. *Critical Infrastructure Protection*, Department of Justice, http://www.usdoj.gov/criminal/cybercrime/critinfr.htm#Vb.
5. U.S. General Accounts Office (2003). GAO report number GAO-03-173, Critical Infrastructure Protection, http://www.gao.gov/htext/d03173.html.
6. *President Bush. Executive Order Amendment of Executive Orders, and Other Actions, in Connection with the Transfer of Certain Functions to the Secretary of Homeland Security*. (2003). The White House President George W. Bush, http://www.whitehouse.gov/news/releases/2003/02/print/20030228-8.html.
7. The White House. *Using 21st Century Technology to Defend the Homeland* http://www.whitehouse.gov/homeland/21st-technology.html.
8. Office of Management and Budget. *Circular No. A-130 Revised. Office of Management and Budget*. http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html.
9. U.S. General Accounts Office (1999). GAO/AIMD-00 http://www.gao.gov/special.pubs/ai00033.pdf.
10. *Lew, J. J. (1999). Memorandum For The Heads Of Departments And Agencies* http://www.whitehouse.gov/omb/memoranda/m99-20.html.
11. Bowen, P., Hash, J., and Wilson, M., (2006). *NIST Special Publication 800-100. Information Security Handbook: A Guide for Managers. INFORMATION SECURITY.* csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.
12. *National Institute of Standards and Technology (NIST). Special Pub 800-12 –An Introduction to Computer Security: The NIST Handbook*. http://csrc.nist.gov/publications/nistpubs/800-12/.
13. *Federal Information Security Management Act of 2002 (Title III of E-Gov)* (2002). http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
14. The Honeynet Project (2002). *Know Your Enemy*, Addison-Wesley.
15. Panjwani, S., Tan, S., Jarrin, K., and Cukier, M. (2005). An experimental evaluation to determine if port scans are precursors to an attack. *Proceedings of International Conference on Dependable Systems and Networks (DSN-2005)* Yokohama, Japan. 602–611.
16. http://sourceforge.net/projects/nettime.
17. Socolofsky, T. and Kale, C. A (1991). *TCP/IP Tutorial, RFC 1180*, http://www.ietf.org/rfc/rfc1180.txt.
18. http://www.insecure.org/nmap/.
19. http://www.tenablesecurity.com/products/newt.shtml.
20. Guilford, J. P. (1965). *Fundamental Statistics in Psychology and Education*, 4th ed., McGraw-Hill, New York.
21. Verissimo, P., Neves, N. F., Cachin, C., Poritz, J., Powell, D., Deswarte, Y., Stroud, R., and Welch, I. (2006). Intrusion-tolerant middleware: The road to automatic security. *IEEE Secur. Priv*. **4**(4), 54–62.Jul./Aug.
22. Courtney, T., Lyons, J., Ramasamy, H. V., Sanders, W. H., Seri, M., Atighetchi, M., Rubel, P., Jones, C., Webber, F., Pal, P., Watro, R., Cukier, M. and Gossett J. (2002). Providing Intrusion Tolerance with ITUA, *Supplemental Volume of the 2002, International Conference on Dependable Systems & Networks (DSN-2002)*, Washington, DC, June 23–26, 2002, pp. C-5-1–C-5-3.

# DEFEATING SURPRISE THROUGH THREAT ANTICIPATION AND POSSIBILITY MANAGEMENT

WILLIAM L. MCGILL

*College of Information Sciences and Technology, Pennsylvania State University, University Park, Pennsylvania*

BILAL M. AYYUB

*Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland*

## 1 RISK ANALYSIS IN AN OPEN WORLD

Expectation is imagination constrained by bounded uncertainty [1]. Rational decisions are based on expectations, and expectations are largely influenced by the bounds a decision maker's imagination places on possible outcomes. When these bounds on expectation are prescribed incorrectly, such as through the illusion of knowledge manifesting from overconfidence, blind sightedness, or faulty reasoning, a failure of imagination could result, which in some contexts could prove harmful to the decision maker. For any decision problem, it is thus important to clearly articulate what is known, what is thought to be known, what is not known, and acknowledge the possibility of unknown unknowns. This last type of uncertainty has been referred to as *ontological uncertainty* [2].

Risk analysis is a tool that informs the decision making process by providing answers to the following three questions for a given future situation (a.k.a. the risk triplet) [3]:

1. What can go wrong?
2. What are the consequences of concern?
3. What is the likeliness of these consequences, all things considered?

In the context of critical infrastructure protection, the first question identifies a set of *plausible initiating events* and *attack profiles*, where a threat scenario an initiating event is the pairing of a threat type with a specific target and an attack profile describes the manner in which the event will occur (e.g. combination of delivery system and intrusion path) [4]. As is mentioned later, failure to identify and consider single plausible initiating event or attack profile increases a defender's vulnerability to surprise. Answers to the latter two questions attempt to make statements about likeliness of each initiating event and the ensuing consequences. Collectively, the triplet of initiating event, consequence dimensions of concern, and likeliness of consequences (to include both likeliness of event and likeliness of consequences given event) define risk [5]. That is, risk is a *multi-dimensional concept*. In practice, probabilistic risk analysis is used to make quantitative statements about risk though quantification is not always necessary to understand risk.

In all decision problems, one must accept either closed-world or open-world assumptions [6]. In the context of risk analysis, *closed-world* thinking assumes a complete set of clearly defined failure events, where any evidence that supports the likeliness of one necessarily supports the unlikeliness of others [7]. For example, if information suggests that an event "*A*" will occur with a probability $p$, then closed-world thinking insists that "not *A*" will occur with a probability $1-p$. Moreover, the closed-world assumption requires that all events contained within the set "not *A*" possess a clear definition: everything that can possibly happen must be articulated. The *open-world assumption* eases this exhaustiveness requirement, and permits reasoning about the future while accepting the possibility of unanticipated events. However, under open-world thinking, knowledge that supports "*A*" cannot offer any support to "not *A*" since not all elements in this set possess a clear definition. That is, the existence of unknown or residual events within a set of possibilities renders statements about likeliness doubtful. To deal with this problem, researchers have proposed maintaining an open mind while entertaining beliefs, and assuming a closed world only for the purposes of decision making by conditioning the set to include only those events that can be articulated [8].

Although the basic risk analysis philosophy is valid for all types of decision making, the mathematical tools available for calculating risk are largely tuned to problems where the probabilities of alternative scenarios and their outcomes can, in principle, be obtained. Notwithstanding the inherent difficulties in assessing these probabilities, extending probabilistic tools to risk analysis when the full spectrum of possibilities is unknown has been met more often with frustration than success. Key examples of this can be found in the domain of security [9], safety [10], international politics [11], high technology [12], project management [13], wastewater treatment [14], civil engineering [15], reliability engineering [16], and just about any other situation where human action plays a key role [1]. Under open-world assumptions, one accepts the possibility of unknown events, which by their very nature lack definition [17]. Without a clear definition of what the residual event is, it is not possible to assign a probability either to the residual event or to a defined event since information cannot offer any weight, directly or indirectly, to an event that lacks definition.

At this point, the distinction must be made between *probable events* and *possible events*. *Probability* is a quantitative measure of likeliness of occurrence of a future event relative to all other events in the same set of possibilities. *Possibility* indicates the degree of membership or belongingness of an event to the set of alternatives, and as a measure provides an upper limit of the actual probability. The connection between probability and possibility is as follows: perfectly possible events can have a probability as high as one, whereas impossible events necessarily have a probability of zero. This notion of possibility is markedly different than probability in that it bounds the potential probability of an event, yet provides no indication of the actual event probability; all it says is that the event is possible. Thus, whereas it is meaningless to assign a probability to events under open-world assumptions, it is perfectly acceptable to construct a possibility distribution over these events.

## 2 SURPRISE EXPLOITS IGNORANCE

A particularly menacing problem that exploits closed-world thinking is that of surprise. Surprise manifests itself in the unknown, unrecognized, and unrealized, and is a direct

by-product of a failure of imagination. According to Grabo [18], surprise occurs when a defender is either unaware of potential hazards or unprepared to defend or respond to unexpected consequences from known, but ignored hazards (i.e., the *counterexpected* event). Each aspect of the prototypical security risk formula (i.e. *risk = threat × vulnerability × consequence* [19]) has elements that contribute to surprise, such as is shown in Figure 1. An event may be unexpected, the probability of its occurrence may be understated, or the resulting consequences may be unanticipated. In general, *surprise exploits defender ignorance*. Figure 2 shows the various types of ignorance, all of which contribute to a defender's vulnerability to surprise. Defeating surprise rests in a decision maker's awareness of possible scenarios and their outcomes, as well as in his preparedness to mitigate a full range of consequences following such events.

Examples of surprise can be found in many areas related to homeland security. In the counterterrorism context, adversaries seek to leverage defender ignorance about adversary intent and capabilities to achieve an asymmetric advantage over their targets. For instance,

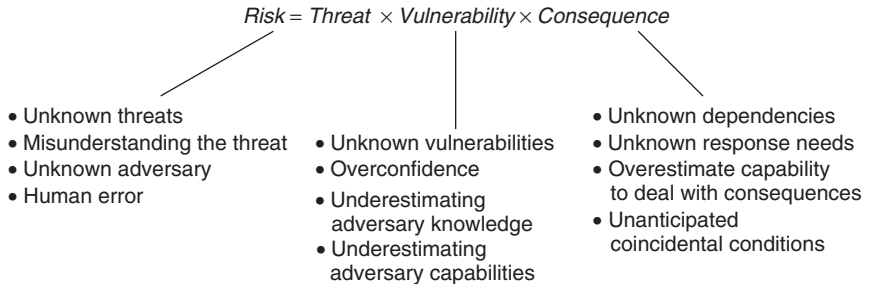



**FIGURE 1** Some sources of surprise in risk analysis for critical infrastructure protection.

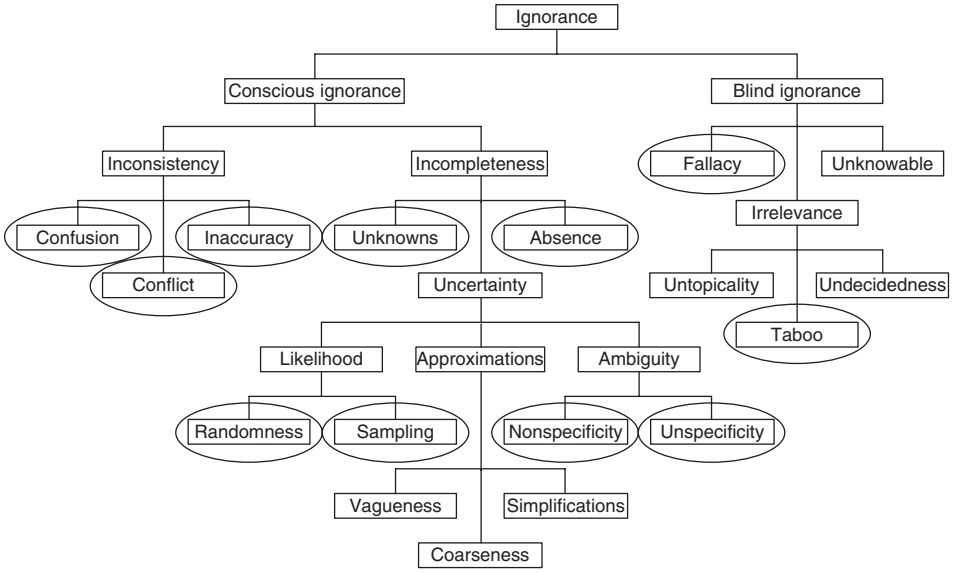



**FIGURE 2** Hierarchy of ignorance types highlighting those types that are particularly susceptible to surprise.

the use of airplanes to attack the World Trade Center and Pentagon on 9/11 was arguably a surprise given that a majority of defenders were unaware that such vehicles would be used as projectiles to attack buildings. Manunta [9, 20] highlights the propensity of adversaries to seek opportunities for achieving surprise, and argues that this behavior renders the security problem incompatible with Bayesian probabilities. In the international affairs arena, Cadell [21] notes that potential adversaries engage in deception to deliberately mislead or confuse their opponents to prevent them from learning the deceiver's true intentions or activities. In this sense, deception thrives by manipulating uncertainty to affect a target, and surprise occurs when the actions of the deceived leads to them experiencing unintended and potentially undesirable events and outcomes. For natural-occurring events, Woo [22] notes that "there are many arcane geological hazard phenomena which are beyond the testimony of the living, which would be met with incredulity and awe were they to recur in our own time". Such "black swans" are highly consequential scenarios that are either unknown or have a perceived probability so low as to be considered negligible, yet would result in significant surprise were they to occur [23]. In highly complex technical systems, Johnson [24] suggests that surprise occurs due to unexpected emergent behaviors stemming from the interaction between system components and their environment. Critical infrastructure is among such highly complex technical systems, where unknown interdependencies between infrastructure services may lead to unpredictable cascading consequences [25].

## 3 IGNORANCE CONTRIBUTES TO VULNERABILITY

Surprise is felt when an event our outcome occurs that was not expected, and can vary in degree according to how far out the realm of possible it was perceived prior to its occurrence [1]. Each possible outcome for a given situation carries with it a degree of *potential surprise* that describes the intensity of this feeling: those outcomes that are deemed possible carry a zero degree of potential surprise, whereas outcomes deemed impossible maximize this measure. Surprise in this sense is experienced by a decision maker whose imagination should ideally reflect the constraints imposed by collective knowledge of his organization. Several authors link these ideas to that of possibility theory [26–28]. Coincidentally, many opponents of probabilistic risk analysis for security suggest that possibility theory provides the mathematical tools needed to support risk and decision analysis, and have made attempts to apply possibilistic techniques to risk analysis problems. Recent work by Karimi and Hüllermeier [29] and Baudrit et al. [30] suggests that progress is being made to propagate both probabilistic and possibilistic information within a quantitative risk analysis framework.

A surprising event is one that is outside the realm of our expectations, and often arises from an inaccurate or insufficient handling of uncertainty. When a situation or decision problem is novel or unique, the challenge is to use the knowledge one has available to set bounds on the scope of imagined future outcomes [31]; more knowledge reduces epistemic uncertainty, whereas lack of knowledge must entertain a wider range of possibilities. According to this point of view, scenarios describing what can happen are considered regardless of their perceived likeliness. Furthermore, the focus is on the outcomes of a scenario, and the goal is to mitigate or constrain the range of possibilities. One example applying this line of thinking has been described in [4] when comparing asset-driven and threat-driven approaches to terrorism risk analysis; the authors asserted that a complete set

of threat scenarios that span a complete spectrum of possibilities can be identified based on the physical characteristics of the potential target and without consideration of adversary intent or probability of attack. Thus, only events that are not physically possible are initially ruled out. Unless supported by disconfirming evidence that judge them impossible or consequentially insignificant, all scenarios are considered throughout the analysis [32].

## 4 DEFEATING SURPRISE THROUGH AWARENESS AND PREPAREDNESS

*The key to defeating surprise is awareness and preparedness*. Awareness is achieved by acknowledging the possibility of alternative threatening events and preparedness is achieved by taking steps to mitigate the range and scope of potential outcomes that can be realized independent of threat type. That is, awareness decreases a decision maker's vulnerability to surprise from an unexpected event, and preparedness decreases vulnerability to surprise from unanticipated outcomes. This section discusses two approaches for defeating surprise—threat anticipation aimed at increasing awareness of plausible threat scenarios and possibility management aimed at increasing preparedness of unanticipated outcomes following an adverse event.

### 4.1 Threat Anticipation: Increasing Awareness

The most challenging part of the risk assessment process is identifying an exhaustive set of initiating events. This is especially true in the homeland security context, where adversaries choose from among myriad threat types, targets, and attack profiles to inflict damage, harm, and fear on their targets. To facilitate the scenario identification process, Kaplan et al. [33] developed the theory of scenario structuring (TSS). Beginning with a *success scenario* or *as-planned scenario* that corresponds to nominal performance of a system, TSS seeks to define an exhaustive set of scenarios that negatively deviates from the success state. Initially, this set consists of a single scenario defined generically as the *failure event*. Collectively, the union of the successful scenario with the failure scenario defines a closed universe of possibilities. However, this extreme level of nonspecificity does not facilitate a defensible assessment of event likeliness, but rather only defines the nature of events. As more information is obtained about what can go wrong, the failure event is partitioned into more specific, distinct subsets, where both a clearly defined event (e.g. "*A*") and its complement (e.g. "not *A*") coexist so as to preserve exhaustiveness of the set. The challenge is to partition the set of plausible scenarios in such a way that each partition has a clear definition that facilitates meaningful assessment of probability and consequence, and provides sufficient resolution to support decision making without imposing too much of a cost burden for doing the analysis.

The process of *threat anticipation* seeks to increase awareness by constructing an exhaustive set of plausible initiating events based on the inherent susceptibilities of target elements to a wide range of threat types, independent of demonstrated adversary capabilities and intent. The process for threat anticipation is illustrated in Figure 3 for a notional asset. Moreover, for each identified threat scenario, an exhaustive set of representative attack profiles is constructed based on the compatibility of alternative intrusion paths (i.e. path leading to a target element) with various attack modes, such as a ground vehicle for explosive threats. The outcome of this procedure is a complete list of initiating events and associated attack profiles that provides the basis for follow-on vulnerability

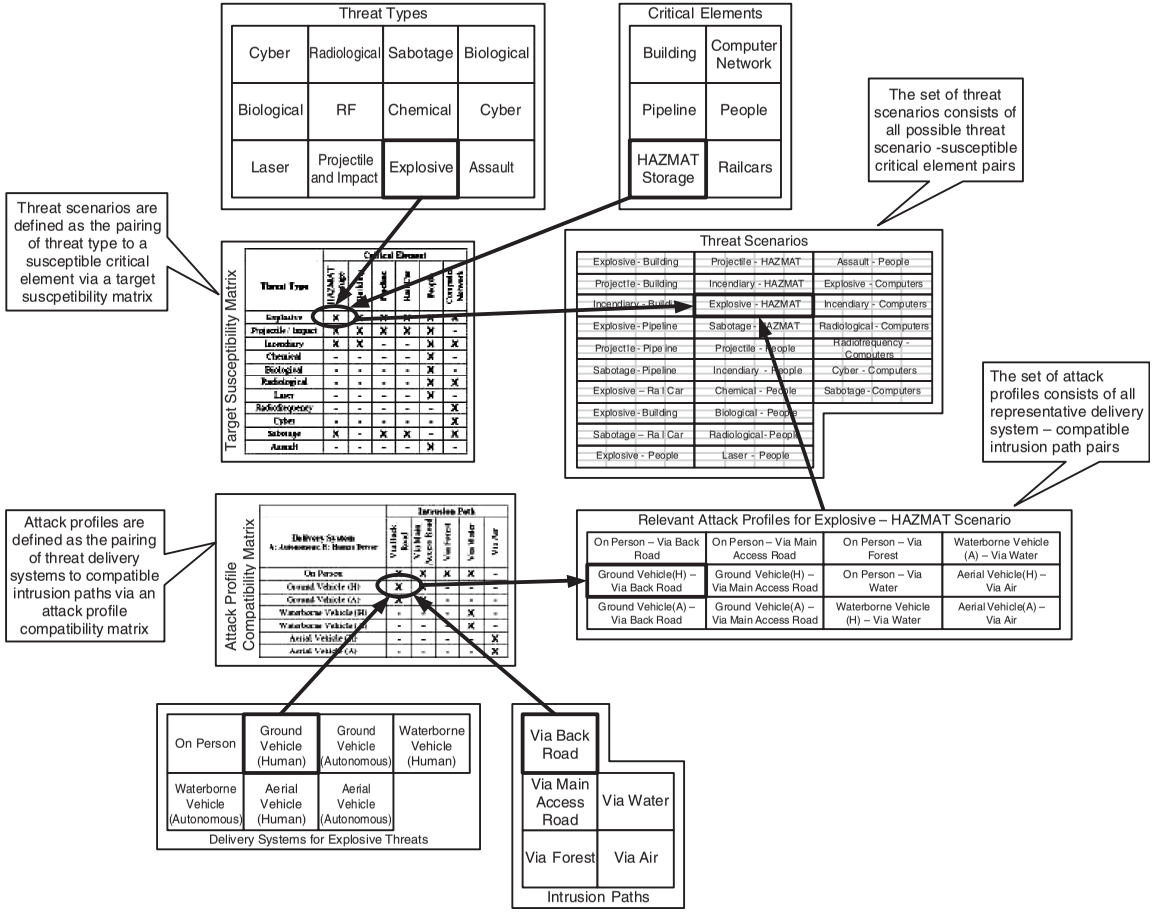



**FIGURE 3** Structured approach for threat anticipation.

analysis and risk assessment. More importantly, the mere acknowledgment of possible scenarios, however unlikely they are perceived to be, lessens vulnerability to surprise by bringing them to the decision maker's attention.

### 4.2 Possibility Management: Improving Preparedness

It is important to note that while an event might come as a surprise, the outcomes following such an event may be manageable. If the capability of an asset or system to deal with the outcomes of a surprising event already exists, then that asset or system has an inherent resilience to surprise due to its ability to recover from known events with similar outcomes. For example, facilities within the oil and gas industry are prepared to deal with explosions due to accidents or system failures, and thus are inherently prepared to mitigate the effects of a malicious explosives attack of similar scale. In contrast, known events may lead to unanticipated outcomes, such as through cascading effects following the collapse of a tree branch on a critical electric power distribution line. In practice, whether an event comes as a surprise is less important than the magnitude of the outcomes following its occurrence, particularly since the range of potential outcomes are what really guide investments in mitigation strategies and preventive measures. In order to defeat surprise, attention should be placed on outcomes that can potentially occur regardless of the initiating event, followed by steps to enhance response and recovery capabilities in light of the possibilities.

This section presents a simple methodology for *possibility management* that seeks to limit the ability of an adversary to achieve surprise through increased knowledge about possible outcomes and improved countermeasures that limit the range of possibilities. A diagram illustrating the steps of the methodology is given in Figure 4. The focus of this methodology is on assessing the possibility of *outcomes* as opposed to the possibility of *events*. Through this approach, a *possibility distribution* over a specified impact measure

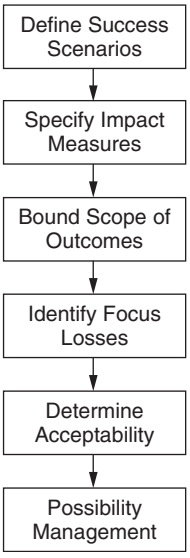



**FIGURE 4** Methodology for possibility management.

such as economic loss or recuperation time is constructed by leveraging knowledge of what *cannot* happen so as to constrain the scope of imagined outcomes. Within this range of possibilities, a focus loss can be identified for the purposes of determining whether such a loss can be tolerated. If the focus loss is too great, a precautionary approach [34] can be taken that seeks to decrease or eliminate its possibility. This methodology is broadly applicable to all levels of critical infrastructure and key resource protection, from protection of a single asset to an entire geographical region or infrastructure sector, and can be looked at from an all-hazards perspective.

*Step 1: Define success scenarios.* This step defines the success scenarios of an asset or system, where the word "success" indicates that the asset or system is functioning as intended [33]. For example, a success scenario of a nuclear power plant might be to provide a specific amount of energy to the energy grid, and a success scenario of the finance and banking infrastructure might be to facilitate the reliable execution of financial transactions between two or more parties. As a suggested rule of thumb, success scenarios for assets are mission focused, and success scenarios for systems are capability focused.

*Step 2: Specify impact measures.* This step identifies suitable impact measures that quantify the effects of a deviation from each success scenario following the occurrence of a disruptive event. For example, disrupted energy production at a nuclear power plant might be measured in terms of lost revenue or recuperation time. Similarly, the impact of a core damaging event at the same plant might be measured in terms of cost to repair or number of persons exposed to harmful radiation. The appropriate measures and bounds of the ensuing impacts are chosen according to the needs of each individual decision maker.

*Step 3: Bound the scope of possible outcomes.* This step bounds the scope of possible outcomes by using available knowledge and information to rule out impossible outcomes or discount otherwise perfectly possible outcomes. In particular, this step identifies three points for each impact measure as shown in Figure 5. The first point defines the *best-case scenario* (*BCS*), which by default corresponds to zero consequence or impact. The second point defines the limiting *perfectly possible*

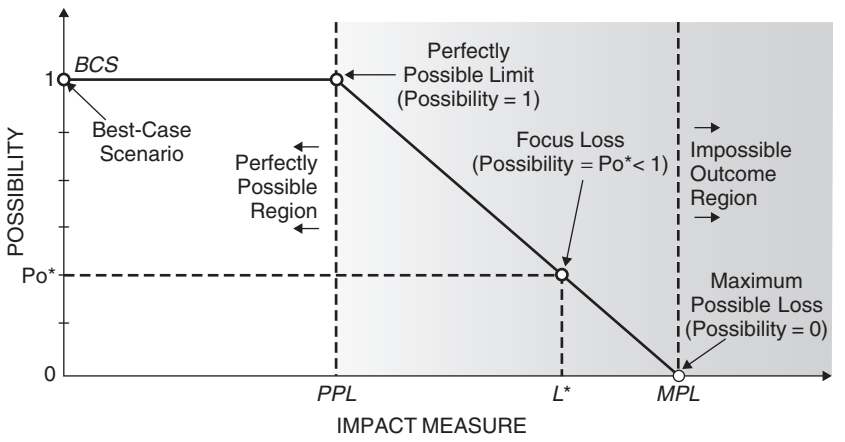



**FIGURE 5** Possibility distribution for the outcomes following a disruptive event.

*loss* (*PPL*) or the point along the impact axis that bounds the set of outcomes that are perfectly possible. The third point defines the *impossibility limit* or *maximum possible loss* (*MPL*) or the point along the impact axis that separates the possible from the impossible. By convention, outcomes deemed perfectly possible carry a possibility of one, whereas outcomes deemed impossible carry a possibility of zero. The possibility of an outcome is a nonincreasing function of impact; thus, the magnitude of *PPL* is always less than or equal to the *MPL*. Under total ignorance, *MPL* and *PPL* coincide, and remain so until knowledge becomes available to judge various outcomes as less than perfectly possible. Given values for *BCS*, *PPL*, and *MPL*, linear piecewise-continuous possibility distribution can be constructed by drawing two line segments: a horizontal line connecting the *BCS* to the *PPL* and another line of decreasing slope connecting *PPL* to *MPL*. Such a possibility distribution is illustrated in Figure 5.

*Step 4: Identify focus losses.* This step identifies a *focus loss* ($L^*$) for the purposes of determining whether the current state of the asset or system is tolerable to the decision makers and for constructing scenarios for red teaming or disaster response exercises with the potential to yield this degree of loss. $L^*$ is a single-valued point along the impact axis bounded by *PPL* and *MPL*, that is, $PPL < L^* < MPL$ (Figure 5). For scenario development, Ha-Duong [35] suggests choosing a value for $L^*$ that coincides with a possibility level of about 1/3; however, the exact choice of possibility level is at the discretion of the decision makers and emergency response planners.

*Step 5: Determine acceptability of focus loss.* Given the focus loss obtained in Step 4, this step assesses whether such a loss is acceptable, tolerable, or manageable. An asset or system can be considered *resilient* if decision maker is prepared to deal with focus loss in such a way that will quickly resume the success scenario irrespective of the exact nature of the disruptive event.

*Step 6: Possibility management.* This step explores the impact of various proposals to enhance mitigation effectiveness and increase resilience by improving the response and recovery capabilities of the affected asset or system. If the focus loss is unacceptable, precautionary measures such as enhanced response and recovery capabilities may be considered that seek to reduce the focus loss. It is important to note that mathematical possibility theory does not support benefit–cost analysis in a strict sense; however, research has shown that possibility distributions can be transformed into probability distributions [36], and as such statements on the probability of realizing some degree of benefit can be made [5].

In addition, the focus loss can be used to construct scenarios for red team and disaster recovery exercises and emergency response planning [35]. There exist an infinite number of scenarios that could potentially result in the focus loss, and such scenarios can be constructed using methods such as the "lego-block" approach described in [37].

## 5 FUTURE RESEARCH DIRECTIONS

The discussion and proposed approaches for defeating surprise described in this article are aimed at helping homeland security decision makers cope with an open world by increasing awareness of plausible threat scenarios and attack profiles through threat anticipation

and improving preparedness through possibility management. In the technical sense, threat anticipation supports the risk analysis process by developing an exhaustive set of scenarios, and possibility management complements this activity by taking precautionary measures to mitigate loss independent of its cause. Collectively, these techniques serve to decrease a decision maker's overall vulnerability to surprise. Further research along the lines of Pugsley [38] should be pursued to identify a set of factors that contribute to an increased susceptibility to surprise through lack of awareness and preparedness so as to provide guidance to decision makers and organizations on how to improve their defenses against surprise attacks.

## REFERENCES


1. Shackle, G. L. S. (1970). *Decision, Order, and Time in Human Affairs*, 2nd ed., Cambridge University Press, Cambridge.
2. Elms, D. G. (2004). Structural safety—issues and progress. *Prog. Struct. Eng. Mater.* **6**(2), 116–126.
3. Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Anal.* **1**(1), 11–27.
4. McGill, W. L., Ayyub, B. M., and Kaminskiy, M. P. (2007). Risk analysis for critical asset protection. *Risk Anal.* **27**(5), 1265–1281.
5. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*. Chapman & Hall/CRC Press, Boca Raton, FL.
6. Walton, D. N. (1990). What is reasoning? what is argument? *J. Philos.* **87**(8), 399–419.
7. Ayyub, B. M. (2004). From dissecting ignorance to solving algebraic problems. *Reliab. Eng. Syst. Saf.* **85**, 223–238.
8. Smets, P., and Kennes, R. (1994). The transferable belief model. *Artif. Intell.* **66**(2), 191–234.
9. Manunta, G. (1999). Security decisionmaking and PRA methodology: does PRA methodology effectively assist security decisionmakers? *J. Sec. Admin.* **22**(2), 1–9.
10. Reason, J. T. (1998). *Managing the Risks of Organizational Accidents*. Ashgate, Hampshire, England.
11. Handel, M. I. (1990). Surprise and change in international politics. *Int. Secur.* **4**(4), 57–85.
12. Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton, NJ.
13. Pender, S. (2001). Managing incomplete knowledge: why risk management is not sufficient. *Int. J. Proj. Manage.* **19**, 79–87.
14. Demotiér, S., Schön, W., and Denœux, T. (2006). Risk assessment based on weak information using belief functions: a case study using water treatment. *IEEE Trans. Syst. Man Cybern.* **36**(3), 382–396.
15. Beard, A. N. (2004). Risk assessment assumptions. *Civ. Eng. Environ. Syst.* **21**(1), 19–31.
16. Blockley, D. I. (1989). Open world problems in structural reliability. *Proceeding of 5th International Conference on Structural Safety and Reliability*, pp. 1659–1665. San Francisco, CA, August 7–11 1989.
17. Ayyub, B. M., and Klir, G. J. (2006). *Uncertainty Modeling and Analysis in Engineering and the Sciences*. Chapman & Hall/CRC Press, Boca Raton, FL.
18. Grabo, C. M. (2002). *Anticipating Surprise: Analysis for Strategic Warning*. Joint Military Intelligence College, Washington, DC.

19. Broder, J. F. (1984). *Risk Analysis and the Security Survey*, Butterworth Publishers, Boston, MA.
20. Manunta, G. (2002). Risk and security: are they compatible concepts? *Secur. J.* **15**(3), 43–55.
21. Caddell, J. W. (2004). *Deception 101–Primer on Deception*. United States Army War College, Carlisle Barracks, PA.
22. Woo, G. (1999). *The Mathematics of Natural Catastrophes*. Imperial College Press, London.
23. Taleb, N. N. (2007). *The Black Swan: The Impact of the Highly Improbable*. Random House, Allen Lane, UK.
24. Johnson, C. W. (2006). What are emergent properties and how do they affect the engineering of complex systems? *Reliab. Eng. Syst. Saf.* **91**(12), 1475–1481.
25. Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Complex networks: identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst. Mag.* **21**, 11–25.
26. Klir, G. J. (2002). Uncertainty in economics: the heritage of G.L.S. Shackle. *Fuzzy Econ. Rev.* **VII**(2), 3–21.
27. Prade, H., and Yager, R. R. (1994). Estimations of expectedness and potential surprise in possibility theory. *J. Uncertain. Fuzz. Knowl. Based Syst.* **2**(4), 417–428.
28. Fioretti, G. (2001). A mathematical theory of evidence for G.L.S. Shackle. *Mind Soc.* **2**(3), 77–98.
29. Karimi, I., and Hüllermeier, E. (2007). Risk assessment system of natural hazards: a new approach based on Fuzzy probability. *Fuzzy Sets Syst.* **158**(9), 987–999.
30. Baudrit, C., Couso, I., and Dubois, D. (2007). Joint propagation of probability and possibility in risk analysis: towards a formal framework. *Int. J. Approx. Reas.* **45**(1), 82–105.
31. Chapman, A. (2006). Regulating chemicals–from risks to riskiness. *Risk Anal.* **26**(3), 603–616.
32. Heuer, R. J. (1999). *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Washington, DC.
33. Kaplan, S., Visnepolschi, S., Zlotin, B., and Zusman, A. (2005). *New Tools for Failure and Risk Analysis: Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*. Ideation International, Farmington Hills, MI.
34. Cameron, E., and Peloso, G. F. (2005). Risk management and the precautionary principle: a Fuzzy logic model. *Risk Anal.* **25**(4), 901–911.
35. Ha-Duong, M. (2006). *Scenarios, Probability, and Possible Futures*. Working Paper. URL: http://www.centre-cired.fr/perso/haduong/files/HaDuong-2006-ScenariosProbabilityPossible Futures.pdf.
36. Dubois, D., Foulloy, L., Mauris, G., and Prade, H. (2004). Probability-possibility transformations, triangular Fuzzy sets, and probabilistic inequalities. *Rel. Comput.* **10**, 273–297.
37. Wideburg, J. (1989). Operational threat assessments for civil defence planning. *Eur. J. Oper. Res.* **43**, 342–349.
38. Pugsley, A. G. (1973). The prediction of proneness to structural accidents. *Struct. Eng.* **51**(6), 195–196.

## FURTHER READING

Ayyub, B. M., Klir, G. J. (2006). *Uncertainty Modeling and Analysis in Engineering and the Sciences*. Chapman & Hall/CRC, Boca Raton, FL.

Fioretti, G. (2004). Evidence theory: a mathematical framework for unpredictable hypotheses. *Metroeconomica* **55**(4), 345–366.

Kam, E. (2004). *Surprise Attack: The Victim's Perspective*, 2nd ed., Harvard University Press, Boston, MA.

National Commission on Terrorist Attacks. (2004). *The 9/11 Commission Report: The Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized Edition. Norton W. W. & Company, New York, NY.

Shackle, G. L. S. (1979). *Imagination and the Nature of Choice*. Edinburgh University Press, Edinburgh.

# MEMETICS FOR THREAT REDUCTION IN RISK MANAGEMENT

ROBERT FINKELSTEIN

*Robotic Technology Inc., University of Maryland University College, Adelphi, Maryland*

BILAL M. AYYUB

*Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland*

## 1 PREMISE

*Risk*, defined as a function of the probability of an event occurring and the consequences given that the event occurs, can be controlled and managed by either reducing the adverse consequences of an event, given that it occurs, or reducing the probability of the event occurring [1, 2]. Memetics can influence both risk components.

Memetics promises to reduce homeland security risks that are a result of human-caused threats by reducing the number of adversaries and thus the probability of an act; increasing the awareness of the risk to the public at large and those responsible for the targeted infrastructure, thus reducing the probability of a successful attack or mitigating its consequences; and enhancing the training of first responders, thus mitigating the consequences of a terrorist act.

## 2 THE MEME

The word "meme" is a neologism coined by Richard Dawkins [3] in The Selfish Gene (1976), (although it may have had earlier roots) and defined as a self-reproducing and propagating information structure analogous to a gene in biology. Dawkins focused on the

meme as a replicator, analogous to the gene, able to affect human evolution through the evolutionary algorithm of variation, replication, and differential fitness. But for military or homeland security applications, the relevant characteristics of the meme are that it consists of information which persists, propagates, and influences human behavior.

### 2.1 Meme Definitions

There are a plethora of definitions for the meme, with most being variations of Dawkins' original notion of a unit (whatever that means) of cultural transmission, where culture may be defined as the total pattern of behavior (and its products) of a population of agents, embodied in thought, behavior, and artifacts, and dependent upon the capacity for learning and transmitting knowledge to succeeding generations. While none of these definitions is sufficient to allow a meme to be clearly recognized or measured (which is now the focus of research), they do provide an initial grasp of the concept. A few of the many definitions extracted from the literature include [4, 5] the following:

- A self-reproducing and propagating information structure analogous to a gene in biology.
- A unit of cultural transmission (or a unit of imitation) that is a replicator that propagates in the meme pool leaping from brain to brain via (in a broad sense) imitation; examples: "tunes, ideas, catch-phrases, clothes fashions, ways of making pots or of building arches".
- Ideas that program for their own retransmission or propagation.
- Actively contagious ideas or thoughts.
- Shared elements of a culture learned through imitation from others—with culture being defined rather broadly to include ideas, behaviors, and physical objects.
- An element of a culture that may be considered to be passed on by nongenetic means, especially imitation.
- Information patterns infecting human minds.
- While the internal meme is equivalent to the genotype, its expression in behavior (or the way it affects things in its environment) is its phenotype.
- Any information that is copied from person to person or between books, computers, or other storage devices. Most mental contents are not memes because they are not acquired by imitation or copying, including perceptions, visual memories, and emotional feelings. Skills or knowledge acquired by ordinary learning are not memes.
- A (cognitive) information structure able to replicate using human hosts and to influence their behavior to promote replication.
- Cultural information units that are the smallest elements that replicate themselves with reliability and fecundity.
- A rule of behavior, encoded by functional neuronal groups or pathways. (Behavior is action, whether mental or physical. Ideas such as tying shoe-laces or opening a door represent rules of physical action, that is, rules of patterned neural–muscular interaction. Concepts such as apple, seven, or causality, represent rules of mental action, or rules of cognition, that is, rules of patterned neural–neural interaction. Hence, physical movement is governed by memes which represent rules of physical action and thought is governed by memes which represent rules of mental action).

- Any kind, amount, and configuration of information in culture that shows both variation and coherent transmission.
- A pattern of information (a state within a space of possible states).
- A unit of cultural information as it is represented in the brain.
- An observable cultural phenomenon, such as a behavior, artifact, or an objective piece of information, which is copied, imitated, or learned, and thus may replicate within a cultural system. Objective information includes instructions, norms, rules, institutions, and social practices provided they are observable.
- A pattern of information, one that happens to have evolved a form which induces people to repeat that pattern.
- A contagious information pattern that replicates by parasitically infecting human minds and altering their behavior, causing them to propagate the pattern. Individual slogans, catch-phrases, melodies, icons, inventions, and fashions are typical memes. An idea or information pattern is not a meme until it causes someone to replicate it, to repeat it to someone else. All transmitted knowledge is memetic.
- The smallest idea that can copy itself while remaining self-contained and intact—essentially sets of instructions that can be followed to produce behavior.

Our initial effort to provide a pragmatic, functionally useful description of the meme led to the following definition:

> *A meme is information transmitted by any number of sources to at least an order of magnitude more recipients than sources, and propagated during at least twelve hours*.

To distinguish a meme from other sorts of information (e.g. from casual, common daily utterances), we invoke an order of magnitude rule and place an emphasis on the necessity of a threshold for propagation and persistence.

We use Claude Shannon's definition of information as that which reduces uncertainty, as manifested, for example, in the difference between two states of uncertainty before and after a message has been received. In Shannon's formulation, a message carries information inasmuch as it conveys something not already known. Thus, there is a subjective element in that the same message may or may not reduce uncertainty, or can have a different influence or impact, depending on the states of the recipients; a meme, as a subset of information, could have different consequences for different recipients. Memes may be characterized or rated as a function of their ability to propagate (among a few or millions of people) or persist (over days or centuries).

Memes, continuing with Shannon's formulation of information, can also be characterized using entropy as a measure of informational order and disorder, where the entropy of a meme is a function of its size (e.g. number of bits or words). The usefulness of this approach remains to be determined. Additional information on Shannon entropy is provided by Ayyub and Klir (2006) [6].

As a practical approach, we defined metrics and submetrics for evaluating memes, including propagation, persistence, impact, and entropy. The submetrics for the *propagation* metric include the number, type, and dispersion of recipients of the meme. Depending on the problem under consideration, the type of recipients might be characterized or categorized by their economic, social, or educational class; ethnicity or culture; religion; gender; age; tribe; politics; and so on, while the dispersion of recipients might

categorized as local, tribal, familial, regional, national, global, and so on. The submetrics for the *persistence* metric distinguish between the duration of transmission of the meme and the duration of the meme in memory or storage. The submetrics for the *entropy* metric distinguish among small, medium, and large memes, which (using an order of magnitude rule) are characterized as less than or equal to 100-K bits, less than or equal to 100-M bits, and greater than 100-M bits. Submetrics for the *impact* metric distinguish between the impact (or potential impact) of the meme on the individual (individual consequence) and its impact (or potential impact) on society as a whole (societal consequence).

### 2.2 Meme Transmission and Reception

A meme is transmitted after being created in the mind of an individual or retransmitted after being received by an individual from elsewhere. Arriving at a new potential host, the meme is received and decoded. The potential host becomes an actual host if the meme satisfies certain selection and fitness criteria. The new host replicates and transmits the meme (perhaps with a different vector, such as a text message instead of speech). Because the number of memes at any given time exceeds the number of recipients able to absorb them, fitness criteria determine which memes will survive, propagate, persist, and have impact. The selection and fitness criteria include human motivators such as fear (e.g. of going to hell or failing in business) and reward (e.g. of going to heaven or succeeding in business). Alternatively, the meme might be beneficial in a practical way (such as instructions on how to make a hard-boiled egg or an improvised explosive device); entertaining to the recipient, such as a joke ("Why did the terrorist cross the road?") or a song ("Bomb bomb bomb, bomb bomb Iran," as sung by Senator John McCain, as featured on YouTube.com); or consist of a direct appreciative feedback to the recipient (such as providing emotional satisfaction, for example, reinforcement and pride in membership in a nation, tribe, religion, ethnic group, or ideology).

To be readily acceptable to the host, the meme should fit existing constructs or belief systems of the host, or be a paradigm to which the host is receptive. Memes also aggregate and reinforce in complexes (memeplexes) so that a suitable existing framework in the mind of the host is especially susceptible to a new meme which fits the framework (such as a new precept by a religious leader that would be absorbed by a follower of that religion, whereas it would be ignored or escape notice by a nonfollower). Suitable storage capacity, in memory or media, is necessary for the meme to persist, along with enduring vectors (e.g. the meme is literally chiseled in stone or reproduced in many, widely distributed copies of books or electronic media).

New research projects could provide a scientific and quantitative basis for memetics and an exploration of its prospective applicability and value, possibly discovering whether brief memes such as "Death to America" or "Glory to the Martyrs" or "Winston tastes good like a cigarette should" are, in fact, cognitively and functionally different from nonmemes such as "I like your hair," or "Please pass the salt".

### 2.3 Quantitative Bases

Since Dawkins' revelation about memes, the concept has attracted a coterie of proponents, skeptics, and opponents. In 30 years there has been no significant research of the concept to establish a scientific basis for it—but neither has there been a definitive refutation. To progress as a discipline with useful applications, memetics needs a

general theory—a theoretical foundation for the development of a scientific discipline of memetics. It needs a narrowly focused, pragmatically useful definition, and, ultimately, the ability to make testable predictions and falsifiable hypotheses. The discrete meme must be defined, identified, and distinguished in the near-continuum of information, just as the discrete gene can be identified (more or less) in long string of DNA nucleotides (albeit, with current technology a gene may not be clearly identifiable). A quantitative basis for memes must be established, using, for example, tools such as information theory and entropy; genetic, memetic, and evolutionary algorithms; neuroeconomics tools such as functional magnetic resonance imaging (fMRI) and biochemical analyses; and modeling and simulation of social networks and information propagation and impact.

As an example, a transmission probability can be quantified using the following procedure provided herein for illustration purposes using uncertainty measures [6, 7]:

- Assess the information content of memes (or memeplex) using uncertainty measures.
- Assess the internal inconsistency.
- Assess the inconsistency among memes within a host and other memes at potential hosts.
- Assess utilities based on a value structure.
- Assess shaping factors based on meme source, timing, complexity, impact, and so on.
- Aggregate into an overall successful transmission likelihood.

### 2.4 Military Worth

If memetics can be established as a scientific discipline, its potential military worth includes applications involving information operations (IO) to counter adversarial memes and reduce the number of prospective adversaries while reducing antagonism in the adversary's military and civilian culture, that is, it could have the ability to reduce the probability of war or defeat while increasing the probability of peace or victory.

In the context of asymmetric warfare, IO are of increasing importance for achieving victory (or avoiding defeat). IO consist of the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations (PSYOP), military deception (MILDEC), public affairs (PA), and operations security. In concert with specified supporting and related capabilities, IO are deployed to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting one's own. Potentially, memetics can have a major effect on PSYOP, MILDEC, and PA.

PSYOP are intended to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives and to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. PSYOP focuses on the cognitive domain of the battle space and targets the mind of the adversary. It seeks to induce, influence, or reinforce the perceptions, attitudes, reasoning, and behavior of foreign leaders, groups, and organizations in a manner favorable to friendly national and military objectives. It exploits the psychological vulnerabilities of hostile forces to create fear, confusion, and paralysis, thus undermining their morale and fighting spirit.

There are strategic, operational, and tactical PSYOP, as described in Joint Publication 3.53, *Doctrine for Joint Psychological Operations* (5 September 2003) [8].

Strategic PSYOP consists of international activities conducted by US government agencies primarily outside the military arena but which may use Department of Defense (DoD) assets. Operational PSYOP is conducted across the range of military operations, including during peacetime, in a defined operational area to promote the effectiveness of the joint force commander's campaigns and strategies. Tactical PSYOP is conducted in the area assigned to a tactical commander, for a range of military operations, to support the tactical mission.

PSYOP may occur across the spectrum of peace to conflict to war, integral to diplomacy, economic warfare, and military action, ranging from negotiations and humanitarian assistance to counterterrorism. But according to the *Information Operations Roadmap*, DoD (30 October 2003) [9], despite PSYOP being a low-density, high-demand asset which is particularly valued in the war on terrorism, PSYOP capabilities have deteriorated. Well-documented PSYOP limitations include an inability to rapidly generate and immediately disseminate sophisticated, commercial-quality products targeted against diverse audiences, as well as a limited ability to disseminate PSYOP products into denied areas. Remedial action is urgently required—and memetics may be a solution for recent PSYOP difficulties.

MILDEC involves actions executed to deliberately mislead the adversary's military decision makers about friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly force's mission. According to the *Information Operations Roadmap*, DoD (30 October 2003) [9], MILDEC should be one of the five core capabilities of IO and the value of MILDEC is intuitive. Counterpropaganda includes activities to identify and counter adversary propaganda and expose adversary attempts to influence friendly populations' and military forces' situational understanding. It focuses on efforts to negate, neutralize, diminish the effects of, or gain an advantage from foreign PSYOP or propaganda efforts.

PA operations assess the information environment in areas such as public opinion and attempt to recognize political, social, and cultural shifts. PA is a key component of information-based flexible deterrent options, intended to build the commanders' predictive awareness of the international public information environment and the means to use information to take offensive and preemptive defensive actions. PA is considered to be a lead activity and the first line of defense against adversary propaganda and disinformation (with the caveat that it must never be used to mislead the public, national leaders, or the media). According to the Field Manual FM 46-1, *Public Affairs Operations* (HQ, Department of the Army, Washington, DC, 30 May 1997) [10], PA operations are combat multipliers in that they keep soldiers informed, maintain public support for the soldier in the field, and mitigate the impact of misinformation and propaganda.

Memetics also has potential military worth in supporting the military culture by enhancing recruitment and training. Recruitment may be improved with memetics by influencing the motivation of prospective recruits, enhancing the image of the military, increasing service awareness ("branding"), providing a national perspective and global situational context for serving one's country. Likewise, training can be improved by increasing trainee motivation, providing better explanations for the training, easing comprehension of the training components, enhancing retention of what is learned during training, and solidifying military culture for the trainees (traditions, customs, and mores).

## 3 HOMELAND SECURITY

In contrast to natural hazards that are indiscriminate and without malicious intent, a unique challenge with assessing risks due to the deliberate actions of intelligent human adversaries is their ability to innovate and adapt to a changing environment. Although one can rely on historical data to estimate annual occurrence rates for natural hazards affecting a region, given that the timescale of geological and meteorological change is much greater than the planning horizon for most homeland security decisions, assets in the same region are always plausible targets for adversaries despite a lack of past incidents [11, 12].

The uncertainty associated with adversary intentions is largely epistemic, and in principle can be reduced given more knowledge about their intentions, motivations, preferences, and capabilities. In general, the threat component of the security risk problem is most uncertain owing to the fact that defenders are often unaware of the adversary's identity and objectives. Less uncertain is the vulnerability component of the risk equation since countermeasures to defeat adversaries are relatively static in the absence of heightened alert. However, since the effectiveness of a security system depends on the capabilities and objectives of the attacker (which is uncertain), the performance of a security system under stress is more uncertain than the consequences following a successful attack. Thus it seems that to build a security risk profile for an asset, it is prudent to start with those aspects of the risk problem that are most certain (i.e. consequence), proceed with the less certain aspects (i.e. vulnerability then threat) as necessary to support resource allocation decisions, and finally proceed to the threat component. Such an approach, however, should recognize that most effective mitigation strategies can be achieved based on threat reduction, changing, or elimination.

In the spectrum of conflict from peace to war, from persuasion to conquest or defeat, from PSYOP to physical destruction, it is far better to mitigate the threat in the beginning by reducing the prospective pool of terrorists. In that early part of the spectrum, there are many problems requiring solutions outside the purview of memetics, such as poverty and the lack of opportunity. But memetics can, potentially, increase the popular demand for realistic solutions to endemic social problems and focus the blame where it belongs. By neutralizing false and incendiary memes that provoke the emergence of terrorists, countermemes can reduce the number of prototerrorists and the probability of consequent terrorist acts.

In the United States, the color-coded terrorist threat warning system has become nearly meaningless in providing specific guidance to the public on responses to terrorist acts. Also, the national critical infrastructure is at terrorist risk from causes outside the purview of memetics, such as insufficient facility security or response systems. But memetics can, potentially, provide the means for increasing the awareness of the public to the terrorist threat in a way that is meaningful as well as memorable. By employing more easily remembered informational techniques, memetics can educate managers of the critical infrastructure about how best to protect their facilities from threat or mitigate its consequences. First responders could also benefit from easily transmitted and absorbed memes to learn the complex tools and techniques needed for countering explosive as well as chemical, biological, and radiological hazards.

## 4 PROSPECTS

Memetics can ameliorate unfavorable consequences from an adversary's culture and help to deter conflict and reduce animosity through cultural education and generating acceptable solutions to endemic problems. In the case of combat, memetics can enhance tactics, strategy, and doctrine by making an otherwise adversarial situation more acceptable to noncombatants, helping to minimize collateral damage by improving the ability to discern combatants from noncombatants, and encouraging civilians to identify insurgents and terrorists. At the conclusion of combat, memetics can bolster peacekeeping, occupation, and nation-building by making these operations more palatable to civilians and facilitating patience for the "long-haul." During postcombat with continuing insurgence, memetics can help minimize collateral damage by enhancing the ability to discern combatants from civilians and identify insurgents and terrorists.

For homeland security, memetics can reduce the number of prospective adversaries and therefore reduce the probability of an attack. By increasing the awareness of the human-caused risk in the public at large and those who manage the targeted infrastructure, the probability of a successful attack can be reduced, or its consequences mitigated. Likewise, the consequences of an attack can be mitigated by using memes to enhance the training of first responders.

## 5 FUTURE RESEARCH DIRECTIONS

The discussion provided herein addresses countermeasures relating to the threat component of homeland security risks, and is aimed at aiding decision makers to develop effective strategies for threat reduction and potential elimination. Further research is needed to enhance our understanding of the nature of memes and their attributes. We must develop techniques for identifying memes, such as fMRI, as well as developing simulation methods and simulation environments, that is, sandboxes, to allow analysts to explore the creation of memes and determine their effectiveness using quantifiable metrics and submetrics.

## REFERENCES

1. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*, Chapman and Hall/CRC Press, Boca Raton.
2. Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Anal*. **1**(1), 11–27.
3. Dawkins, R. (1976). *The Selfish Gene*, Oxford University Press, Oxford.
4. R. Aunger, Ed., (2000). *Darwinizing Culture: The Status of Memetics as a Science*, Oxford University Press, Oxford.
5. Aunger, R. (2002). *The Electric Meme: A New Theory of How We Think*, The Free Press, New York.
6. Ayyub, B. M. and Klir, G. J. (2006). *Uncertainty Modeling and Analysis in Engineering and the Sciences*, Chapman & Hall/CRC, Boca Raton.
7. Ayyub, B. M. (2004). From dissecting ignorance to solving algebraic problems. *Rel. Eng. Sys. Safety* **85**, 223–238.

8. Joint Chiefs of Staff. Doctrine for Joint Psychological Operations (2003). *Joint Publication 3.53*, Department of Defense, Washington, DC.
9. Department of Defense (2003). *Information Operations Roadmap, 30 Oct. 03*, Washington, DC.
10. Department of the Army (1997). *Public Affairs Operations Army Field Manual FM 46-1, HQ*, Washington, DC.
11. Ayyub, B. M., McGill, W. L., and Kaminskiy, M. (2007). Critical asset and portfolio risk analysis for homeland security: an all-hazards framework. *Risk Anal*. **27**(3), 789–801.
12. McGill, W. L., Ayyub, B. M., and Kaminskiy, M. (2007). A Quantitative Asset-Level Risk Assessment and Management Framework for Critical Asset Protection. *Risk Anal*. **27**(5), 1265–1281.

## FURTHER READING

National Commission on Terrorist Attacks (2004). *The 9/11 Commission Report: The Final Report of the National Commission on Terrorist Attacks Upon the United States*, Authorized ed. Norton W. W. and Company New York, NY.

Department of Homeland Security (2006). *National Infrastructure Protection Plan*. URL: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf. Last accessed 27 November 2006.

Hoffman, B. (1998). *Inside Terrorism*, Columbia University Press, New York.

Martz, H. F., and Johnson, M. E. (1987). Risk analysis of terrorist attacks *Risk Anal*., **7**(1), 35–47.

Haimes, Y. Y. (2006). On the Definition of Vulnerabilities in Measuring Risks to Infrastructures *Risk Anal*., **26**(2), 293–296.

# HIGH CONSEQUENCE THREATS: ELECTROMAGNETIC PULSE

MICHAEL J. FRANKEL
*EMP Commission, Washington, D.C.*

## 1 INTRODUCTION

While the power of a nuclear weapon was seared into the world's psyche during the waning hours of WWII, nuclear scientists and defense specialists have long been aware that the potential for widespread destruction, devastation, and disorder as a consequence of nuclear detonation may exceed even that anticipated by the popular imagination. The locus of such assessment lies in their awareness of the full effects of a nuclear burst,

effects not realized in the immediate and particular circumstances of the Japanese wartime experience.

When a nuclear warhead is detonated, the energy bound up in the rest mass of an atom is released. While a large fraction of this energy is originally in the form of radiation—x rays, $\gamma$ rays, and neutrons—at low burst heights, much of this energy is converted to kinetic and thermal forms, as the atmosphere quickly absorbs the radiated energy, heats up, and launches an extraordinarily powerful blast wave that causes much of the immediate damage to any structures caught in its destructive path. Along with the familiar blast waves comes a veritable witch's brew of destructive insults; a thermal pulse that may ignite fires, along with broken gas lines, overturned stoves, etc., producing secondary fires that can propagate damage beyond the initial blast radius or even coalesce into a highly destructive firestorm, cratering, and ground shocks damaging even well-buried underground structures, an intense but localized ("source region") electromagnetic pulse (EMP), and of course fallout that may extend the effects of the weapon far from the burst site and whose lethal effects may linger long after all other signs of the immediate devastation have disappeared.

But there are also other effects attendant upon a nuclear burst, especially at bursts heights—at relatively high altitude above 30 km or so—which our WWII experience did not adequately presage. These high altitude effects include enhancement of the natural radiation belts that circle the earth (whose existence was unknown during WWII) or the creation of entirely new, albeit temporary, radiation belts that may destroy or degrade artificial satellites in low earth orbits encompassed by their reach [1],[1] ionization effects in the atmosphere, which interfere with communications, direct effects of large X-ray dosages, which can travel unimpeded many thousands of miles through space to affect satellites at great distances from the burst point, and—the subject of this article—by the production of gigantic high altitude EMPs, which may produce unprecedented widespread disruption on the ground [2].[2]

## 2 WHAT IS EMP?

EMP from weapons detonations in space was discovered as a surprise by-product of early nuclear weapons tests; one of which (STARFISH, a 1.4 Mt device exploded in 1962 at an altitude of 400 km above Johnston Island in the Pacific Ocean), delivered an EMP, which turned out the street lights in downtown Honolulu, a distance of about 800 nautical miles away. Earlier testing in the Soviet Union reportedly damaged buried cables and electric power equipment at a remove of 600 km from detonations of a few hundred kilotons yield at burst heights ranging from about 60 to 300 km [3].

[1]The detonation of Starfish in 1962 was the proximate cause of the almost immediate loss of Telstar, the first commercial telecommunications satellite, launched in 1961. Over the next few months, every single commercial satellite in orbit failed, well before its expected lifetime. No information is publicly available on the fate of a number of satellites performing classified intelligence missions at the time.

[2]We are focused here on the high altitude phenomenon often referred to as high electro magnetic pulse (HEMP) in the national security literature. A ground level burst will produce a localized phenomenon known as *source region electro magnetic pulse (SREMP)*, whose strong electric fields will generally be confined to a radius of a scale with the blast damage radius from a weapon. There are also other forms of EMP related to effects on space systems, such as systems generated electro magnetic pulse (SGEMP), which stem from an interaction between bomb X rays and metallic structures. We will not deal with these, or other EMP exotica, here.

The EMP from a nuclear device comes in two components, a fast pulse and a slow pulse, each emerging from a different physical mechanism. The fast pulse is a result of the initial high energy $\gamma$ radiation from the bomb traveling toward the earth and in turn producing a stream of electrons heading in the same direction by encounters with the sensible atoms of the atmosphere in a region 20–40 km high, where the atmosphere has thickened enough to intercept the $\gamma$ rays. The stream of electrons heading toward earth must travel through the magnetic field that surrounds our earth and, as must any charged particle traversing a magnetic field, be forced to "turn", or accelerate, in a direction perpendicular to the field. This near coherent acceleration of the charged electron stream is the source of the fast component, the first radiated EMP field felt on earth. The area coverage of this pulse can be enormous—the phenomenon has been likened to installing a radiating phased ray antenna a thousand miles long up in the sky (Fig. 1)—and its peak electric field may reach tens of kilovolts per meter, a level sufficient to degrade or destroy many commercial electrical components that form the warp and woof of our twenty-first century technology-based society.

The mechanism of the slow pulse is associated with the expansion of the ionized bomb materials in the earth's magnetic field as well as the rise of a bomb heated and ionized patch of atmosphere cutting the earth's geomagnetic field lines. While the fast pulse may last only for nanoseconds and couple unwanted high frequency energy pulses to vulnerable electrical devices, the slow component may last from milliseconds to seconds and couple low frequency, long wavelength pulses to suitable antennae tuned to receive these frequencies. In fact, the US power grid, with conducting runs of wire running from tens to hundreds of kilometers in uninterrupted length, represents such an "antenna" seemingly ideally tuned to the reception and coupling of the frequencies of the slow EMP.

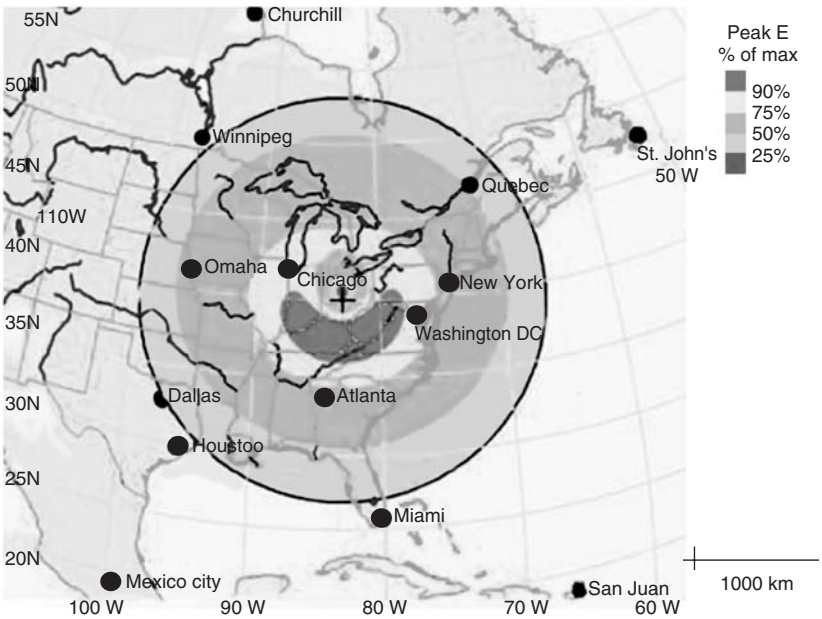



**FIGURE 1** Illustrative EMP coverage—fast pulse. Thirty kiloton nominal yield and 100 km burst height.

## 3 CONSEQUENCES OF AN EMP EVENT ON OUR INFRASTRUCTURES

### 3.1 Direct Effects

So what can an EMP actually do to you? In terms of directly visible destructive impact on physical structures or biological systems, the answer is nothing. Instead, EMPs are expected to couple unwanted energies into the soft underbelly of our technology-dependent society—the ubiquitous electronic systems, controls, gadgets, means of communication, and power sources that undergird and enable the daily functioning of twenty-first century American civilization. The fast EMP may apply fields of many kilovolts per meter either directly—free field coupling—or through the ubiquitous *ad hoc* antennae, short runs of wire or cable, in the local electrical network to which most devices are connected. As has been repeatedly demonstrated in test programs, levels of insult starting at a few kilovolts per meter are generally sufficient to degrade electronic equipment functioning and higher field levels—easily achievable by a high altitude nuclear source—may even cause permanent physical damage in most commercial-off-the-shelf electronic systems (Fig. 2).

The slow EMP produces long wave pulses capable of coupling electrical energy directly with the long cable runs of the power grid transmission system potentially damaging key components such as hard to replace high voltage transformers. While the fast EMP may be simulated in specialized electric pulse machines, the slow pulse has a natural analog in the EMP produced by geomagnetic storms associated with mass ejection events on the sun and correlated roughly with the 11 year sunspot cycle. Figure 3 demonstrates the physical damage that may result from application of this type of slow pulse. The transistor damage shown in the figure occurred at the same time that the 1989 geomagnetic storm brought down the entire Hydro Quebec system leaving 9 million Canadian customers without power for periods of up to 2 weeks.

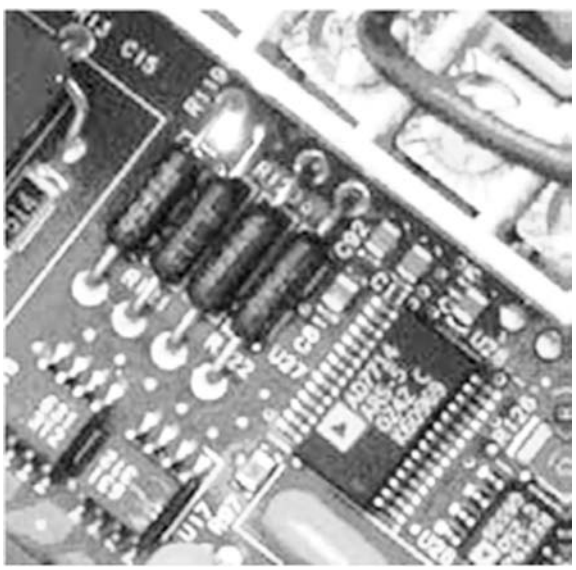


**FIGURE 2** Electrical arcing damage to a circuit board during current injection EMP simulation testing [4]. [Courtesy of W. Radasky, Metatech Corp.].

**FIGURE 3** Permanent damage to high voltage transformer during 1989 geomagnetic storm. [Courtesy of Public Service Electric and Gas Corp.].

High voltage transformers are house-sized, complex, and expensive affairs; no longer manufactured in this country; and require on the order of a year to fill and ship an order. Loss of a significant number of high voltage transformers would undermine any prospect of the power grid to recover in a timely manner and cause almost incalculable economic harm and human misery over a period that might well extend for many months. Figure 4 is a graphical representation of a calculation sponsored by the EMP Commission [4] showing the catastrophic collapse of the power grid in a specific scenario of a high yield detonation over the eastern part of the United States. Red and green circles represent high voltage transformers which are predicted to and have failed, with the colors indicating impressed current directions. The straight lines represent high voltage (>365 kV) distribution lines.

It is not only the slow pulse that couples to the long lines represents a danger to the functioning of the power system but the supervisory control and data systems (SCADAs) and protective relays and breakers—whose earlier electromechanical designs are being increasingly replaced by more versatile but more electrically vulnerable digital electronic systems—are also at risk from the fast pulse. The power grid is an extraordinarily complex network under constant dynamic control, which strives to match generation with the load. It is fair to say that no adequate predictive models exist that fully understand all their potential interactions and—on the order of every decade or so—there is a major power failure, which may stem from one or two precipitating failures which cascaded out of control in some surprising way. Since the coverage of the EMP pulse may extend to a significant fraction of the country, we may envision the result of the failure of potentially hundreds of power grid components over a widely dispersed area, all simultaneously. Worst case estimates anticipate the failure of the power grid over a significant fraction of the country, with many components having suffered permanent physical damage. There is little precedent for any of this, and the time needed to recover from such a state is uncertain. In the worst imaginable, but possible, scenario—the loss of the entire national power system from coast to coast—recovery is particularly uncertain as there is simply no experience available for such a black start condition [5].

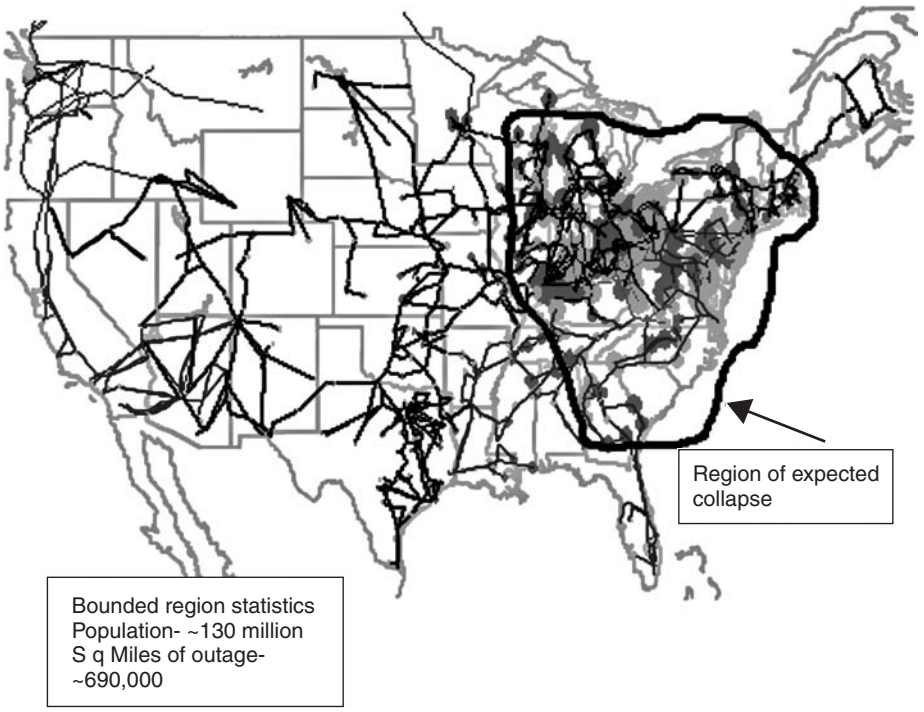



**FIGURE 4** Collapse of portion of power grid representing 70% of domestic power generation in high yield burst scenario [4]. [Courtesy of W. Radasky, Metatech Corp.] (See online version for color).

We have discussed the vulnerability of the power grid, but that is not the only critical infrastructure at risk. Significant elements of the computer-controlled national telecommunications network may also be at risk in an EMP attack. Computers, routers, switches, etc., if unshielded, may be damaged by EMPs. The telecommunications system—and thus the nation's financial system—though possessing short-term backup power systems of its own, is in turn ultimately dependent on the functioning of the power grid. The terrorist attack of September 11, 2001, on the World Trade Center exposed telecommunications and concentration of key facilities as serious weaknesses of the financial services industry. Equity markets closed for four days, until September 15, due to failed telecommunications. The New York Stock Exchange could not reopen because key central offices were destroyed or damaged leaving them unable to support operations. According to a senior government economic official, Fedwire (the electronic funds transfer system operated by the Federal Reserve enabling fund transfers between financial institutions), CHIPS (Clearing House Interbank Payments System is an electronic system for interbank transfer and settlement. CHIPS is the primary clearing system for foreign exchange), and SWIFT (Society for Worldwide Interbank Financial Telecommunications provides stock exchanges, banks, brokers, and other institutions with a secure international payment message system) would cease operation if telecommunications are disrupted. He further observed that ACH (Automated Clearing House is an electronic network that processes credit and debit transactions), ATMs (automated teller machines), credit and debit cards

all depend on telecommunications. Disruption of these systems would force consumers to revert to a "cash economy".

In the recent report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (The EMP Commission) [4], the Commission documented the direct effects of EMP irradiation not only on the power and telecommunications infrastructures but also on the transportation, emergency services, banking, oil and gas, water, food, and space infrastructures. Although SCADAs were previously mentioned in conjunction with the power grid, many of the direct vulnerabilities in the other critical infrastructures of this country stem, in turn, from the widespread infiltration of these automated control and monitoring systems into critical functional nodes of most systems that undergird the smooth functioning of our economy and maintain our well being. If the SCADAs that monitor and control the pump pressures in the oil and gas pipelines malfunction or cease working altogether, then fuel will not be delivered to industries and everybody else who needs it; rail systems that rely on sensors to monitor tracks and controls to set rail switches may not function; emergency responder communications networks may be unusable; if electronically controlled, the various pumps that deliver water from reservoirs and underground sources may not function; and stored foods may spoil if dependent on vulnerable refrigeration system.

### 3.2 Indirect Effects

In an increasingly interdependent world, the power system itself is increasingly dependent on the functioning of the telecommunications system to maintain situational awareness and active remote control. The telecommunications system may maintain itself for a short period by backup, on site power. Uninterruptible power supplies—batteries—may keep operations functioning for a few hours, but generally no longer than a day. Some telecommunications facilities are equipped with backup generators that may keep things going until the fuel runs out. But, these would have to then be replenished by fuel deliveries provided by the transportation system, which in turn require fuels themselves from the oil and gas infrastructures, each of which in turn depends on the availability of power from the grid. Personnel would have to be delivered by the transportation system to repair and maintain the power and they would have to be fed by the food and water infrastructures and paid by the financial system, which in turn depend on telecommunications and power system. A major catastrophe that took down the power system for any extended period of time thus has the potential to produce incalculable misery and ultimately loss of life, with recovery scenarios of uncertain prospects. This mutual interdependence of the critical infrastructures is shown in Figure 5.

Experience demonstrates that such interdependencies and interactions may well be overlooked, until an emergency situation suddenly reveals their existence as they surface to bite us. For example, many of the recovery procedures developed by organizations to deal with emergencies implicitly assume that transportation is available to transport personnel somewhere to go fix something. But, immediately following the precipitating events of 9/11, airplanes (except emergency military transport) were all grounded. In 1991, the accidental severing of a single fiber-optic cable in the New York City region not only blocked 60% of all calls into and out of New York, but it also disabled all air traffic control functions from Washington, DC, to Boston—the busiest flight corridor in the Nation—and crippled the operations of the New York Mercantile Exchange. These key

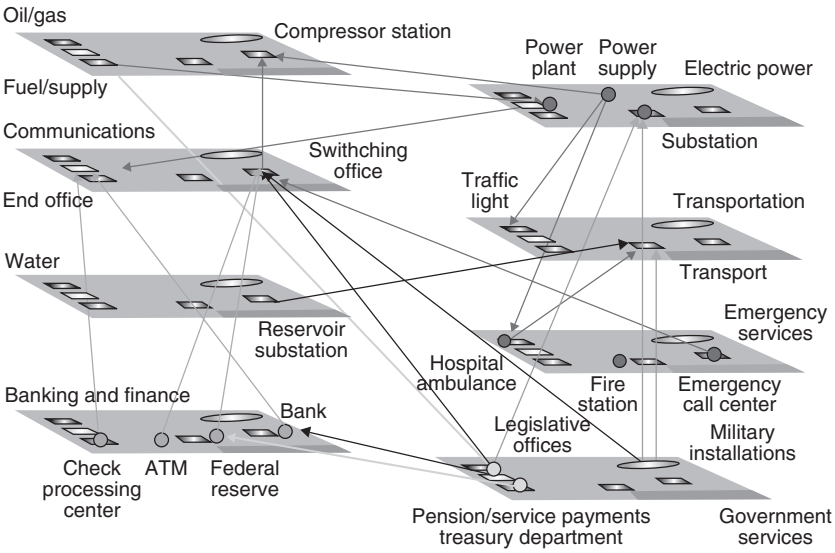



**FIGURE 5** Infrastructure interdependencies (diagram courtesy of Sandia National Laboratory). All interdependencies are not shown.

interdependencies are always there, but they are not recognized as warranting advanced contingency planning [6].[3]

Generally, in situations where an infrastructure experiences failure, such as loss of electric power due to storm or some other localized event—the August 2003 electric blackout of the Northeast was ultimately attributed to a localized failure with subsequent unanticipated cascading effects (due to loss of situational awareness through failure of monitoring systems, which prevented timely load shedding that might have been otherwise averted) [7]—many of these infrastructure interdependencies and interactions can be safely ignored. But, in an EMP attack scenario, the energy of EMP is expected to affect the different infrastructures simultaneously through multiple electronic component disruptions and failures over a very wide geographical area. Understanding these cross-cutting interdependencies and interactions is critical to assessing the capability of the full system of systems to recover. The modeling and simulation needed to explore the response of such a complex situation involve a large but finite number of elements and should be amenable to analysis, at least approximately. Efforts to develop a predictive modeling capability are underway, but much progress still needs to be made.

## 4 THE RISK OF AN EMP ATTACK

Risk is normally accounted as a multiplicative concatenation of threat, vulnerability, and consequences, with each of these factors in turn quantitatively represented as a conditional probability. EMP, however, is also one of a class of very high consequence, low

[3]Nuclear plants require some existing power in a grid and may not be started into a black grid. Coal and gas generating plants also require some existing electricity to run. Presumably, hydroelectric plants might be the first sources brought back on line to nucleate the recovery of other elements. But this would have to be done very carefully and load balancing might be particularly stressing under such circumstances.

probability (or more accurately, unknown) events, which classical risk methodology [8] finds difficult to encompass. EMP is one of a small number of events whose consequences are potentially so large that they hold the possibility of affecting the basic functioning of civil society in our country for an extended period. Although many intuitively believe that the threat may be small, the consequences are so large that risk may not be negligible [9][4] and may result in a finite risk. The EMP Commission, while refusing to assess the likelihood of such an event, nevertheless utilized a capabilities-based threat assessment methodology to conclude that the technical information to accomplish such an attack was widely disseminated amongst potential adversaries. But it is also a truism that vulnerability invites the attention of those who might exploit it, and reducing such vulnerability must inevitably reduce the risk. Given the scale of likely consequences, it is thus remarkable that the Federal government, in its organizational embodiment in the Department of Homeland Security (DHS), has to date given almost no attention at all to this issue. Most critical, and telling, is the lack of any serious study and planning function within DHS, which is the critical first step required to come to grips with the issues reviewed in this article.

It is important to emphasize that such a lack of attention is not uniformly practiced across the Cabinet Departments of this country. The Department of Defense (DOD) has long been aware of the EMP threat to the functioning of a modern military no less dependent on the operation of advanced electronic components than the civilian sector. The DOD has made investments to ensure the continued operation and viability of our fighting forces and military infrastructure in EMP environments. All these are in stark contrast to the present lack of readiness of the civilian infrastructures to withstand, operate through, and recover from any such electromagnetic event.

## 5 MANAGING THE RISK: RECOMMENDATIONS TO HELP PROTECT OURSELVES

While risk was defined as the product of the likelihoods of threat, vulnerability, and consequence, risk management addresses the steps that may be taken to mitigate, contain, or recover from identified risk [10]. The following general recommendations are offered to address the current demonstrated vulnerabilities of our infrastructures.

- As a mechanism for focusing preparation activities at the DHS, planning is presently organized around consideration of 15 canonical disaster scenarios [11]. These scenarios range from essentially localized disturbances such as a terrorist chemical attack or a natural disaster such as a hurricane to very few scenarios with potentially more widespread effects such as a biological attack. It presently includes one nuclear scenario that envisions a detonation of a small yield device at ground level in a city in the United States. A strong recommendation to DHS is to initiate a planning activity for EMP disasters by adding a 16th scenario of a high altitude nuclear burst. EMP disaster analysis and planning should be augmented by inclusion of EMP scenarios in planning exercises that engage the federal government response with first responders in the state and local government.

[4]As do many others, Schneier makes the point, inter alia, that estimates of risk are greatly conditioned by familiarity. Thus, our intuition about EMP risk may not be worth much. Similarly, many intuitively believed the threat of terrorists crashing commercial airliners into skyscrapers was small.

- As far as possible, attention should be paid to the development of dual benefit solutions to EMP threats. Thus, for example, measures that may be taken to implement protection of the critical elements of the power grid to EMP may also confer other protective benefits against the threat of geomagnetic storms. The latter is a regular natural phenomenon that has demonstrably damaged key elements of the grid in the past (Fig. 3). Recent calculations analyzing the response of the power grid to a so-called 100 year storm (EMP Commission, personal communication) point to an existing known vulnerability to an expected natural phenomenon with the prospect of very severe consequences, with no apparent protection. It is hard not to make analogies to Katrina. As well, measures implemented to monitor and enhance the system's ability to recover from EMP may also enhance the overall reliability and quality of the infrastructure, conferring economic benefit.
- Critical components of each infrastructure should be identified and inventories compiled. Plans should consider the economic and logistical feasibility of storing long lead time replacement items in the vicinity of their prospective use.
- The federal government should enhance its investment in the analysis of infrastructure interactions and the development of validated modeling and simulation tools to support realistic planning simulations and the rapid testing of mitigation and recovery strategies. A good start has already been made here but more effort will be required before a reliable tool capable of exploring far from equilibrium situations with potentially hidden-under-normal-circumstances interaction pathways is available to the planning community. Agent-based approaches may hold particular promise and should be explored.

The Commission to Assess the Threat to the United States from Electromagnetic Pulse has published a number of volumes detailing both the threat and the impact of EMP environments on the military and civilian infrastructures of the country. The volume describing civilian infrastructures was unclassified and contained approximately 70 more specific recommendations addressed in the main volume to the DHS, including recommendations for legislative actions aimed at the Congress. Our final recommendation is that those 70 specific actions be reviewed for action and implemented as rapidly as possible.

## REFERENCES

1. Papadopulous, K. D., briefing available at http://www.lightwatcher.com/chemtrails/Papadopoulos-chemtrails.pdf.
2. Defense Threat Reduction Agency, briefing available at www.fas.org/spp/military/program/asset/haleos.pdf.
3. (2004). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*, Vol. 1: Executive Report, p. 4.
4. Radasky, W. *Critical National Infrastructures*, Vol. 3, EMP Commission, calculation, Metatech.
5. Schneider, F. B., Bellovin, S. M., and Inouye, A. S. (1998). Critical infrastructure you can trust: where telecommunications fit, *26th Annual Telecommunications Policy Research Conference*, http://www.tprc.org/abstracts98/schneider.pdf.
6. Report of the Ontario Ministry of Energy. (2003). Following August 2003 blackout. http://www.energy.gov.on.ca/index.cfm?fuseaction=electricity.reports_outage.

7. US-Canada Power System Outage Task Force. (2003). *Interim report: Causes of the August 14 Blackout in the US and Canada*, November, 2003 ftp://www.nerc.com/pub/sys/all_updl/docs/blackout/814BlackoutReport.pdf.
8. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*. Chapman & Hall.
9. Schneier, B. (2003). *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, Springer.
10. Scouras, J., Cummings, M. C., McGarvey, D. C., Newport, R. A., Vinch, P. M., Weitekamp, M. R., Colletti, B. W., Parnell, G. S., Dillon-Merrill, R. L., Liebe, R. M., Smith, G. R., Ayyub, B. M., and Kaminskiy, M. P.. (2005). *Homeland Security Risk Assessment*, *Volume I An Illustrative Framework*. RP04-024-01a. Homeland Security Institute, Arlington, VA, November 11.
11. http://media.washingtonpost.com/ wp-srv/nation/nationalsecurity/earlywarning/National PlanningScenariosApril2005.pdf.

### FURTHER READING

Glasstone, S., and Dolan, P. J. (1977). *The Effects of Nuclear Weapons*. Department of Defense and the Department of Energy.

Longmire, C. L. (1978). On the electromagnetic pulse produced by nuclear explosions. *IEEE Trans. Electromag. Compat.*, **EMC-20**(1), 3–13.

Messenger, G. C., and Ash, M.S. (1986). *The Effects of radiation on Electronic Systems*, Chapter 8, Van Nostrand Reinhold, New York.

# HIGH CONSEQUENCE THREATS: NUCLEAR

CALVIN SHIPBAUGH
*Arlington, Virginia*
MICHAEL J. FRANKEL
*EMP Commission, Washington, D.C.*

## 1 INTRODUCTION

World War II taught the world to measure destructive power by a new metric. Fission weapons, which "split" atoms of uranium or plutonium and release a portion of their binding energy, are measured by their yield in terms of the number of kilotons (kt) of

trinitrotoluene (TNT) equivalent to the total energy released. The first fission weapons that were produced in 1945 had yields in the neighborhood of 15–20 kt [1]. This approximate magnitude may crudely be assumed to represent early design attempts at producing nuclear explosions, although the yield of the first French test was reportedly several times greater [2].[1] Lower yields can cause large scale devastation to an urban area. North Korea is the most recent nation to conduct a nuclear test. The yield was very low, and is reported to be less than 1 kt [3]. This yield stands in contrast to prior historical observations of what might have been expected for a first explosion, and illustrates that surprises regarding conventional wisdom on nuclear issues have appeared in recent times.

Thermonuclear weapons, which release excess binding mass energy when hydrogen atoms "fuse", can have yields much higher than those of the most powerful fission weapons. The largest ever tested had a yield of approximately 50 Mt [4], which is more than three thousand times the yield of the fission bomb dropped on Hiroshima. Few nations have demonstrated the ability to manufacture thermonuclear weapons. But, in a volume focused on the risk to homeland security from the activities of well-funded terrorist groups and rogue nations, it would seem prudent to focus our attention on effects of low yield threats, on the order of 1–20 kt. These threat weapons may be relatively unsophisticated devices—improvised nuclear devices (INDs) constructed from stolen or diverted fissile materials—or more sophisticated devices constructed with the aid of experienced weapons designers, and either bought or stolen from a nuclear weapon state whose custodial safeguards are compromised during a period of internal political instability. It has been widely reported that the Department of Homeland Security (DHS) has followed the same track, defining a 10 kt threat for use by federal, state, and local homeland security disaster planning efforts [5].

## 2 SCOPE OF THE DESTRUCTIVE PHENOMENA

A nuclear explosion in the atmosphere produces a strong blast, much greater than hurricane force winds. This is complicated in urban terrains by combinations of direct and indirect waves that may concentrate the blast flow and enhance intensity. A distinction is made between dynamic pressure, which results from the hammer blow impact of the shock front and its following winds, and overpressure, which uniformly "squeezes" its targets.

A crater will result if a nuclear explosion occurs near a land surface or within the lower levels of a structure, while ground shock will damage some structures beyond the crater. The diameter and depth of the crater depend on the type of material, and varies approximately as the cube root of yield. The apparent crater radius of a 1 kt explosion in dry soil is approximately 20 m [6]. The ground shock effect is enhanced if a nuclear explosive is buried in a few meters of ground [7].[2]

If exploded in or near water, another potential effect is high waves and surge of vapor. The damage caused by waves is, in general, less significant for a low yield explosion than blast or thermal effects, but should be considered for calculating damage to the nearby shore. Vapor clouds that surge outward from the explosion are highly contaminated with radioactive materials.

[1] This test event is known as *Gerboise bleue*. It was said to be 70 kt, and was conducted in 1960.

[2] A 1 kt surface detonation in hard rock generates 100 MPa at a depth of less than 20 m, but a coupled explosion generates the same pressure at approximately 80 m.

The radiant energy of a low yield nuclear explosion can cause severe fire or other thermal damage (e.g. third-degree burns) at distances of several hundred meters to kilometers. The damage depends on transmission through the atmosphere. Factors such as humidity or fog and reflections from the surface affect the intensity as a function of range. The duration of a pulse depends on yield, so the thermal effect on a target depends on the yield as well as on the energy density at the target. The damage threshold increases with the yield.

The most distinctive feature of a nuclear explosion, apart from the sheer magnitude of energy released, is nuclear radiation [8].[3] An acute whole-body dose from the prompt radiation emerging from the explosion in the range of 150–300 cGy [9] induces nausea and fatigue in most victims in the first hours, and can cause fatalities in a few percent of cases within 6 weeks. The $LD_{50/60}$ dose, at which fatalities reach 50% within 60 days, is often reported to be approximately 450 cGy (without medical treatment). A dose of 600–700 cGy is lethal to most people; that is, $LD_{95/60}$ [9]. Table 1 provides a summary of the known physiological response to radiation dose.

Residual radiation results from the radioactive decay of fission products, radioisotopes created by prompt neutrons, and nuclear materials present in the weapon. The vast majority of this material is carried up by the mushroom cloud and falls back downwind. This phenomenon creates a widespread, lingering hazard. Although fallout presents a long-term risk, it should also be noted that 55% of the theoretical total residual radiation dose released will occur in the first hour, and 75% will occur in the first 12 h. A rule-of-thumb is that a sevenfold passage of time reduces the dose rate by a factor of 10 [6].

Although electromagnetic pulse (EMP) is most often discussed in reference to high altitude explosions where effects can be very widespread, a surface explosion can produce a local or "source region" electromagnetic pulse (SREMP). The intensity of the electric field (i.e. up to a few kilovolts per meter) can be immediately destructive to many kinds of electronics within a deposition region of a few kilometers from the blast point. The effects of such local EMP can also be conducted well beyond the immediate environment of the explosion by coupling electromagnetic energy to wires and cables that conduct the effects to more distant, but electrically connected, sites.

## 3 CASE STUDY: CONSEQUENCES IN POPULATION CENTERS

We consider now the likely consequence of detonation of a low yield device at zero height of burst—such as might be associated with weapon delivery by a van—in a symbolically and politically important urban center such as Washington, DC.

[3]One Gray (Gy) is the modern term for dose. It is equivalent to 100 rads (radiation absorbed dose). One centi-Gray (cGy) is therefore equivalent to one rad. One rad is defined as 100 ergs absorbed per gram of target material (such as body tissue). The term sievert (Sv) is used to measure the equivalent dose, which is the dose in Gy multiplied by a radiation weighting factor to account for the difference in biological effects among types of radiation. The typical annual background dose, less than one cGy, is three orders of magnitude less than this acute dose. Strictly speaking, biological effects should not be treated in units of cGy (or rads, as in older documents), but for an acute whole-body exposure from a nuclear explosion the radiation weighting factor for both neutrons and gammas is near unity. The average annual effective dose in the United States was estimated (for 1980) to be 3.6 mSv.

**TABLE 1 Physiological Response to Radiation Dose [10]**

| Dose Range (REM Free Air) | Onset and Duration of Initial Symptoms | Performance (Mid-range Dose) | Medical Care and Disposition |
|---|---|---|---|
| 0–70 | 6–12 h: none to slight transient headache, nausea, and vomiting in 5% at upper end of dose range | Combat effective | No medical care, return to duty |
| 70–150 | 2–20 h: transient mild nausea and vomiting in 5–30% | Combat effective | No medical care, return to duty |
| 150–300 | 2 h to 3 d: transient to moderate nausea and vomiting in 20–70%; mild to moderate fatigability and weakness in 25–60% | DT:PD 4 h until recovery. UT:PD 6–20 h; DT:PD 6 wk until recovery | 3–5 wk: medical care for 10–50%. High end of range death in >10%. Survivors return to duty |
| 300–530 | 2 h to 3 d: transient nausea and vomiting in 50–90%; moderate fatigability in 50–90%. | DT:PD 3 h until death or recovery. UT:PD 4–40 h and 2 wk until death or recovery | 2–5 wk: medical care for 10–80%. Low end of range <10% deaths; high end death >50%. Survivors return to duty |
| 530–830 | 2 h to 2 d: moderate to severe nausea and vomiting in 80–100%. 2 h to 6 wk: moderate to severe fatigability and weakness in 90–100% | DT:PD 2 h to 3 wk; Cl 3 wk until death. UT:PD 2 h to 2 d, 7 d to 4 wk; Cl 4 wk until death. | 10 d to 5 wk: medical care for 50–100%. Low end of range death >50% at 6 wk: High end death for 99% |
| 830–3000 | 30 min to 2 d: severe nausea, vomiting, fatigability, weakness, dizziness, disorientation; moderate to severe fluid imbalance, headache | DT:PD 45 min to 3 h; Cl 3 h until death. UT:PD 1–7 h; Cl 7 h to 1 d, PD 1–4 d; Cl 4 d until death | 1000 REM: 4–6 d medical care for 100%; 100% deaths at 2–3 wk. 3000 REM: 3–4 d medical care for 100%; 100% death at 5–10 d |
| 3000–8000 | 30 min to 5 d: severe nausea, vomiting, fatigability, weakness, dizziness, disorientation, fluid imbalance, and headache | DT:Cl 3–35 min; PD 35–70 min: Cl 70 min until death. UT:Cl 3–20 min; PD 20–80 min; Cl 80 min until death | 4500 REM: 6 h to 1–2 d; medical care for 100%; 100% deaths at 2–3 d |
| Over 8000 | 30 min to 1 d: severe prolonged nausea, vomiting, fatigability, weakness, dizziness, disorientation, fluid imbalance, and headache | DT and UT: Cl 3 min until death | 8000 REM: medical care immediate to 1 d, 100% deaths at 1 d |

### 3.1 Radiation Consequences

The *Hazard Prediction and Assessment Code* (HPAC) [10] calculates likely consequences of such an explosion scenario. Figures 1 and 2 show the resulting dispersion of radioactive materials (fallout) and estimated casualties following an explosion of a 1 and 20 kt device in downtown Washington, DC.

Not unexpectedly, the resulting radioactive footprint and estimated casualties are more significant in the 20 kt scenario than in the 1 kt case. The total casualties may be expected to decrease if more rapid evacuation is achieved, but it is clear that fallout effects are a significant contributor to the overall hazard. The medical consequences of accumulated dose listed in Table 1 are overlayed with the fallout footprint and population statistics from the Oak Ridge National Laboratory population database [11] to produce the HPAC casualty estimates.

Similarly, potential exposure may be estimated for initial radiation effects. A $\gamma$ dose of 300 cGy from a low altitude fission explosion is received at a slant range of approximately 850 m for 1 kt and 1500 m for 20 kt (Fig. 3) [6]. The corresponding range for neutrons is approximately 900–1350 m.

### 3.2 Blast Consequences

The overpressures and dynamic pressures will cause severe blast wave damage within the immediate vicinity of the explosion. Reinforced concrete structures will be damaged at 5 psi peak overpressures and wood frame structures—typical housing construction

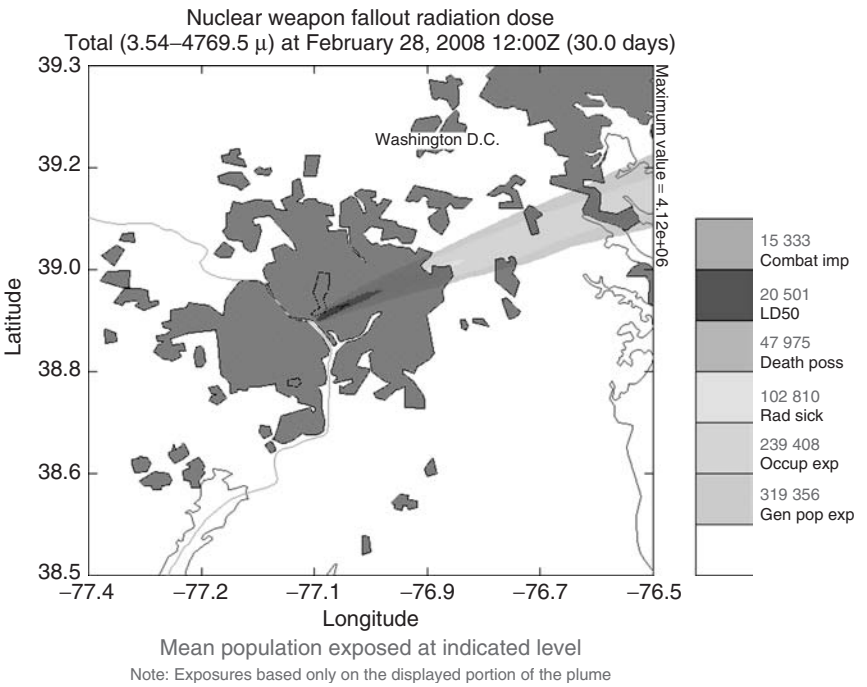



**FIGURE 1** One kiloton burst, zero height of burst. 30.0 days accumulated radiation dose (HPAC calculation, historical weather).

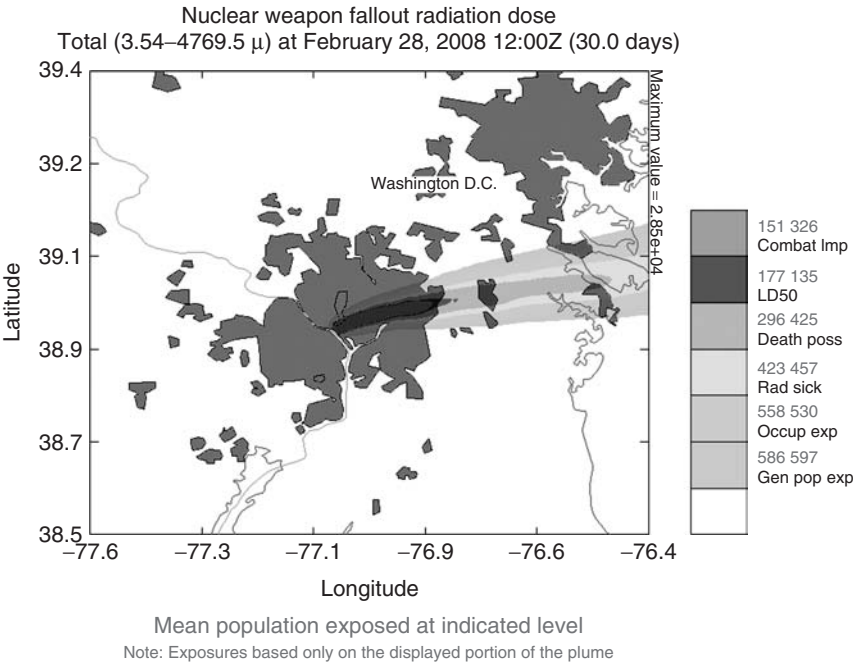



**FIGURE 2** Twenty kiloton burst, zero height of burst. Thirty-hour accumulated radiation dose (HPAC calculation, historical weather).

in the United States—will show heavy damage at 2 psi and severe damage at 5 psi. Structures close enough to experience more than 5 psi dynamic pressures may expect to be demolished. At the lower end of the 2–5 psi damage regime, vehicles are likely to be overturned or damaged but may remain operable. Underground components such as pipes and mains will survive the blast, but above-ground structural damage may cause losses at connections. As shown in Figure 3, for a 20 kt surface explosion, 2–5 psi damage range translates into a distance of 2000–1200 m from the explosion point, respectively.

Since the energy of an explosion, which produces the blast is contained in a spherically expanding volume of hot gas, the force of the blast falls off as the cube of the distance from the explosion point and thus gives rise to the "cube-root scaling" typical of explosive phenomena. Thus, at any distance from the detonation site, a 20 kt event will be felt to be *approximately* three times as intense as would a 1 kt event set off at the same point. This is illustrated in Figures 4 and 5, which show the reach of 5 psi curves where severe damage may be expected for the Washington, DC, scenario [12].

### 3.3 Thermal Consequences

The threshold for a low yield weapon to ignite newspaper is approximately 5 cal/cm$^2$ [6]. The corresponding prompt effect slant range on a clear day for a near surface *air burst* is 700 and 3200 m, respectively, for 1 and 20 kT devices [6]. Persistent ignition of wood by direct thermal irradiation may be difficult, but combustibles contribute to fires.

Once fires are ignited, there is the possibility that they will spread, although this phenomenon is limited by fire breaks and availability of fuel. Both history and insight

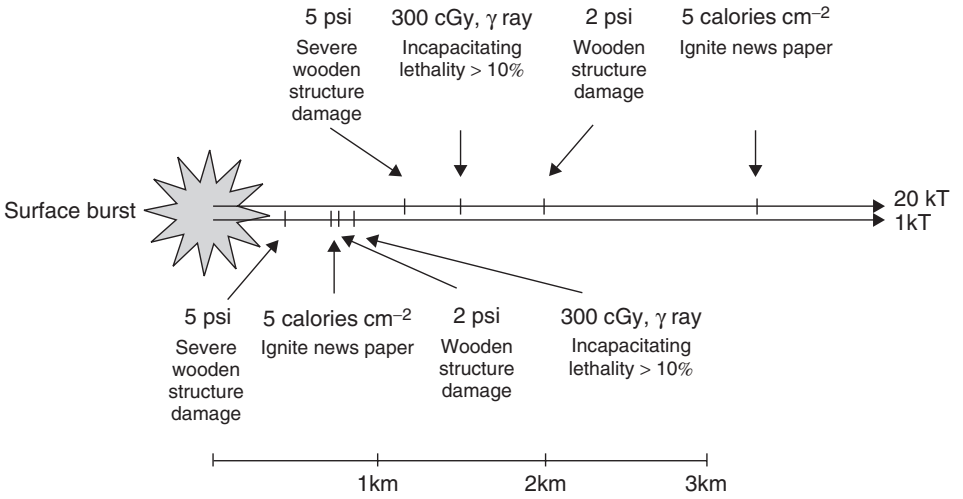



**FIGURE 3** Fission explosions—distance versus threshold.

**FIGURE 4** Two (blue) and five (yellow) pounds per square inch circles for a 1 kt explosion in downtown Washington, DC. (See online version for color).

gleaned from disruptive events such as earthquakes allow a confident prediction of significant fire activity, as additional damage—such as ruptured gas lines—contributes to ignition and fires. If enough fuel is present, ignition effects might possibly coalesce into a firestorm such as that occurred in Hiroshima, Nagasaki, Hamburg, or Dresden. This could cause more total casualties than the prompt blast effects of the bomb itself. In the

**FIGURE 5** Two (blue) and five (yellow) pounds per square inch circles for a 20 kt explosion in downtown Washington, DC. (See online version for color).

two atomic bombings of Japan during World War II, it is impossible to estimate with any confidence the fatalities due to immediate bomb effects and those due to the subsequent firestorms. The likelihood of this extreme fire activity occurring in many modern US population centers may not be high as there is not as much wood as found in Japanese or old European construction.

### 3.4 Widespread Consequences

In the immediate vicinity of the blast, severe consequences discussed in the preceding sections may be expected to overshadow local concerns about electromagnetic phenomena. The consequences of essentially random equipment failures many kilometers from the blast zone are probably not a significant source of concern.

It is, however, possible to consider the potential for other major effects, secondary to the prompt damage, but which depend on the particular location of the explosion. For example, had the van delivering the nuclear device been rolling down New York's Wall Street rather than Washington DC's Pennsylvania Avenue, it is possible that the financial infrastructure of the United States might be severely compromised. The concern is not merely the shut down of trading markets for an undefined period, but the potential to adversely affect the database systems (ACH, SWIFT, Fedwire, CHIPS[4] [13]) that account for and manage the flow of trillions of dollars per day through the economy. Apart from

[4]Fedwire is the electronic funds transfer system operated by the Federal Reserve enabling fund transfers between financial institutions. CHIPS (clearing house interbank payments system) is an electronic system for interbank transfer and settlement. SWIFT (society for worldwide interbank financial telecommunications) provides stock exchanges, banks, brokers, and other institutions with a secure international payment message system ACH (automated clearing house) is an electronic network that processes credit and debit transactions.

great loss to life and property, the impact of this event would be of very high consequence on the financial and banking system impact [14].[5]

### 3.5 Uncertainties

The variation of effects given a yield, along with variations of demographics, geography, urban design, and environmental factors, all contribute to uncertainties in consequences. Studies of the effects of very low yield explosions are very rare and have generally not been performed with any scientific rigor. These represent another uncertainty. Understanding the terrorist threat demands an on-going study. Scenario development coupled to scientific and engineering analysis is useful for depiction of potential events, for gaining insight into complex processes and surprises, and for bounding the predictions.

### 3.6 Risk

A report by the National Commission on Terrorist Attacks Upon the United States finds that "al Qaeda continues to pursue its strategic objective of obtaining a nuclear weapon" [15]. Discussions of the threat presented by nuclear proliferation include recent Congressional concerns regarding networks that were identified years ago as supplying equipment and knowledge that supported the spread of nuclear weapons' potential around the globe [16]. There is a confluence of threats, vulnerabilities, and consequences, and thus a nonzero risk of a high consequence attack.

The quantitative determination of the risk posed by nuclear threats, the evaluation of this risk relative to other high consequence threats, and the prioritized allocation of resources to address such threats are the tasks of the DHS.

## 4 RISK REDUCTION: RECOMMENDATIONS

Leading the national effort to secure the United States is part of the mission of the DHS [17]. Increased attention is being given to preventing nuclear attacks in the US homeland by terrorist or clandestine operators [18, 19].[6,7] A single nuclear explosion would be a high consequence event that strains or overwhelms regional capability to respond and may inflict debilitating economic and social consequences that affect the entire nation. A scenario involving multiple nuclear explosions is traditionally a problem in the realm of military exchanges, but this may not remain the case. Risk management in this area faces the need for recognizing the large uncertainties, and developing strategies that address widely diverging goals.

[5]Under the assumptions of one study, the consequences for a "typical" low yield nuclear explosion result in a lifetime labor value loss of approximately 200 billion dollars. The losses are amplified by a (crudely estimated) comparable reduction in the gross domestic product and a smaller property loss. The total estimate is hundreds of thousands of casualties and a loss of 1.5 trillion dollars.

[6]The DHS Domestic Nuclear Detection Office (DNDO) was established in 2005 to improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop, or transport nuclear or radiological material for use against the Nation, and to further enhance this capability over time.

[7]In 2004, a Task Force of subject-matter experts presented four areas of recommendation to the Department of Defense (DoD). Their findings are as follows: "make immediate operational changes", "improve nuclear intelligence collection capabilities", "start a spiral development program", and "establish joint warfighting requirements and capabilities". These include numerous specific recommendations, such as details regarding spiral development of some types of radiation detection system along with test beds and the S&T base.

The following general recommendations are offered to address potential susceptibilities across a diverse set of conditions.

- As a mechanism for minimizing risk, there is a premium to be gained by emphasizing prevention. During the cold war, this was attained largely due to the skillful use of deterrence. The risk of nuclear terrorism creates a strong need for additional methods, such as intelligence, detection, and interdiction capabilities. The importance of sensing and mitigating attempts to transport weapons and threat materials into the United States has been recognized with the creation of the DHS/DNDO. As was the case with cold war era studies, full systems analyses including political and cultural factors are critical to understanding what is needed to succeed in reducing the likelihood of nuclear explosions throughout the world.
- Given the great uncertainty in the diversity of the nature of the modern nuclear threat, there is compelling reason to examine a range of scenarios to extend existing studies to nontraditional attacks. What are the consequences for attacks against symbolic sites or obscure vulnerable points that may present high leverage for an adversary to inflict extensive damage on civilian infrastructure and key resources? It is advisable to prepare contingencies for strikes that are not well considered in the definitions of what constitutes attractive targets according to conventional wisdom.
- High consequence events are not defined by explosive yield alone. Studies that include a scenario to examine the consequences and response options to subkiloton weapons should be conducted, given the surprisingly low yield of the recent North Korean test. In particular, planning and preparations for responding to the lowest yield events observed in initial testing performed by nations may serve as a set of capabilities to gain experience and develop road maps for further expanding contingencies to better handle more stressing scenarios.
- Further study of the problem of protecting population against radiation effects from a terrorist nuclear attack appears desirable. The issue of remaining shielded indoors (if the structure is sufficiently intact) to await decay of intense radioactivity versus evacuation to minimize exposure time (including inhalation hazards) is important for further analysis under a variety of scenarios.
- This problem is not going to disappear, and the high consequences mean that an investment in analysis will remain an on-going part of our security needs throughout the foreseeable future. Efforts should be supported for identifying, clarifying, and estimating the conditional probabilities that describe the threat. Prioritized investment in response will require further investment in analysis tools to support realistic planning. A single detonation may be a great catastrophe, but it does not end civilization, and the need to continue developing mitigation and recovery strategies in the aftermath remains as a hedge against subsequent events.

The current multipolar nuclear threat environment is widely recognized as more complex and less transparent than the situation faced throughout most part of the cold war. Since 9/11, it has been clear that there are two general categories to address—actions by national actors and terrorist threats which may or may not be completely distinct from state motivations. Mitigation is not just a matter of better technology and traditional strategies. The pursuit of understanding nontechnical factors is very important for risk reduction.

## REFERENCES


1. Malik, J. (1985). *The Yields of the Hiroshima and Nagasaki Nuclear Explosions*, Los Alamos National Laboratory, LA-8819, September 1985.
2. http://www.assemblee-nationale.fr/rap-oecst/essais_nucleaires/i3571.asp.
3. Office of the Director of National Intelligence (2006). Public Affairs Office, Washington, DC, October 16, 2006. This announcement was released at: http://www.dni.gov/announcements/20061016_release.pdf.
4. Ministry of the Russian Federation for Atomic Energy (1996). *USSR Nuclear Weapons Tests and Peaceful Nuclear Explosions: 1949 through 1990*, ISBN 5-85165-062-1, Russian Federal Nuclear Center-VNIIEF, 1996.
5. http://www.globalsecurity.org/security/library/report/2004/hsc-planning-scenarios-jul04.htm.
6. Glasstones, S., and Dolan, P. J. (1977). *The Effects of Nuclear Weapons*, U.S. DoD and ERDA, Washington, DC.
7. Buchan, G. C. et al. (2003). *MR-1231, Future Roles of US Nuclear Forces RAND*, Santa Monica.
8. Hall, E. J., and Giaccia, A. J. (2006). *Radiobiology for the Radiologist*, 6th ed., Lippincott Williams & Wilkins, Philadelphia.
9. (1996). *NATO Handbook on the Medical Aspects of NBC Defensive Operations AMedP-6(B), Part I- Nuclear*, FM 8-9, NAVMED P-5059, AFJMAN 44-151, Departments of the Army, The Navy, and the Air Force, Washington, DC, 1 February 1996.
10. Defense Threat Reduction Agency, http://www.ofcm.gov/atd_dir/pdf/hpac.pdf.
11. http://www.ornl.gov/sci/landscan/.
12. Federation of American Scientists *Nuclear Weapons Effects Calculator*, http://www.fas.org/main/content.jsp?formAction=297&contentId=367.
13. http://www.tax.state.ny.us/evta/glossary.htm.
14. Zycher, B. (2003). *A Preliminary Benefit/Cost Framework for Counterterrorism Public Expenditures*. RAND, MR1693.
15. http://govinfo.library.unt.edu/911/staff_statements/staff_statement_15.pdf.
16. (2007). *A.Q. Khan's nuclear Wal-Mart: out of Business or Under New Management?: Joint Hearing before the Subcommittee on the Middle East and South Asia and the Subcommittee on Terrorism, Nonproliferation, and Trade of the Committee on Foreign Affairs, House of Representatives, One Hundred Tenth Congress*, first session, June 27, 2007. http://foreignaffairs.house.gov/110/36424.pdf.
17. http://www.dhs.gov/xabout/strategicplan/.
18. http://www.dhs.gov/xabout/structure/editorial_0766.shtm.
19. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. (2004). *Report of the Defense Science Board Task Force on Preventing and Defending Against Clandestine Nuclear Attack*, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington DC, June 2004.


## FURTHER READING


Glasstone, S. and Dolan, P. J. (1977). *The Effects of Nuclear Weapons*, Department of Defense and the Department of Energy.

Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*, Chapman and Hall.

# MODELING POPULATION DYNAMICS FOR HOMELAND SECURITY APPLICATIONS

Mark P. Kaminskiy and Bilal M. Ayyub
*Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland*

## 1 INTRODUCTION

Analysis of the risks related to combating terrorism problems is a multidisciplinary subject. It includes practically all the methods of probabilistic risk analysis such as scenario development, event-tree analysis, and precursor analysis. It is worth mentioning that the analysis of real data related to counterterrorist actions is definitely not on this list, which is true for the so-called simulation models [1, 2] as well. The simulation models can add some insights on terrorist population dynamics (TPD), but in contrast to the models considered below, no "quantitative conclusions can be made from the simulation results" [2]. Thus, developing the data analysis methodology related to counterterrorist actions constitutes an important part of the respective methodological tools needed.

International terrorism today is very different compared to what we dealt with in the 1970s and 1980s [3, 4]. The scale of this phenomenon is much larger, so we can apply the notion of *population* to this international community of terrorists to timely investigate its dynamics. The TPD models introduced below are similar (but not identical) to some survival data analysis models, which are, in turn, borrowed from nuclear physics and chemical kinetics theory [5, 6]. One can also find an analogy between the models considered below and the population dynamics models used in Ecology [7, 8], which were introduced independently by Volterra and Lotka in 1920s (the so-called Lotka–Volterra equations). In the suggested population dynamics models, the response function is the number of terrorist cells as a function of time counted from any conveniently chosen origin. It should be noted that *all* the parameters of these nonformal models are physically meaningful, for example, they can include the initial number of the terrorist cells $N_0$, the disabling rate constant $\lambda$ or the cell half-life $t_{1/2}$, and the rate of formation of new cells $P$. The model parameters can be estimated using the data like, say, the annual or monthly numbers of disabled or identified terrorist cells. By estimating these parameters, one can assess other important characteristics, which include, but are not limited to, current number of terrorist cells, the time needed to reduce the number of active cells to a given level, the number of active cells at any given time in the future, and so on. The respective statistical data analysis is reduced to the routine nonlinear least squares estimation (LSE) procedures, which is illustrated by a case study. The article is mainly based on the authors' prior work [9], and also includes some new results on relationship between the Lotka–Volterra model and the suggested TPD model, as well as the above-mentioned case study.

## 2 CLOSED SYSTEM

For the time being, it is assumed that the system is *closed* (sealed). The closed system is defined in the given context, as such a system, is 100% protected from terrorists penetration from outside, as well as it is 100% protected from creating the terrorist cells inside this system.

Owing to all antiterrorist actions (inside and outside the system), it is reasonable to assume that the number of terrorist cells decreases according to the following differential equation:

$$\frac{\mathrm{d}N}{\mathrm{d}t} = -\lambda N \tag{1}$$

where $\lambda$ is a positive rate constant. In nuclear physics, Eq. (1) is known as the radioactive *decay law*, and the constant $\lambda$ is called *decay constant*. For the considered population of terrorist cells, the $1/\lambda$ can be called the *mean time to capture* or *mean lifetime of terrorist cells*. Another convenient parameter related to $\lambda$, which can be borrowed from nuclear physics, is the *half-life* $t_{1/2}$, that is, time needed for disabling of half of the cells, that is, $N(t_{1/2}) = N_0/2$, where $N_0$ is the initial number of the terrorist cells. Using Eq. (1), one obtains:

$$t_{1/2} = \frac{\ln 2}{\lambda} \tag{2}$$

The number of terrorist cells $N(t)$ at a given instant $t$ is easily obtained by the integration of Eq. (1):

$$N(t) = N_0\ \mathrm{e}^{-\lambda t} \tag{3}$$

It should be noted that from the data analysis standpoint, Eq. (3) is not convenient. In reality, one can observe only the cumulative number of *disabled* cells (denoted below by $N_\mathrm{d}$), which is given by

$$N_d(t) = N_0 - N_0\ \mathrm{e}^{-\lambda t}$$

so that

$$N_d(t) = N_0(1 - \mathrm{e}^{-\lambda t}) \tag{4}$$

On the basis of available data, the parameters of Eq. (4), that is, the initial number of the terrorist cells $N_0$ and the rate constant $\lambda$ (or the half-life $t_{1/2}$), can be estimated. Eq. (4) is illustrated in Figure 1.

## 3 SYSTEM WITH FORMATION OF NEW CELLS

A more complicated situation arises, when the system is modeled assuming that it is not 100% protected from terrorist penetration from outside, and it is not 100% protected from formation of the terrorist cells inside the system itself. Similar to the previous case, it is assumed that the terrorist cells are disabled at the rate $\lambda$.

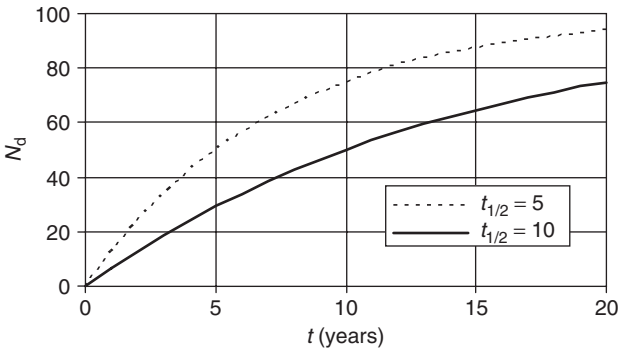



**FIGURE 1** Cumulative number of disabled cells $N_d$ as a function of time, $N_0 = 100$.

In this case, Eq. (1) is replaced by

$$\frac{dN}{dt} = -\lambda N + P \tag{5}$$

where $P$ is the rate, at which the new cells are produced due to the penetration from outside the system and/or due to the formation of cells inside the system.

Qualitatively, Eq. (5) shows that one deals with two conflicting processes—the formation of new cells at rate $P$ and their disabling at rate $\lambda N$. Depending on the sign of the right side of Eq. (5), the number of cells either increases or decreases. The last case is considered below.

The traditional solution of Eq. (5) used in nuclear physics [5] is based on the initial condition $N(0) = N_0 = 0$, which assumes, in the given context, that at the beginning, there are no terrorist cells or their number is negligible compared, say, to the number of cells produced at the rate $P$ during first year. This initial condition does not look realistic for the problems considered, which is why it is not discussed in this paper.

The more realistic initial condition assumes that at the beginning, there is a number of terrorist cells, that is, $N(0) = N_0 > 0$. The solution of Eq. (5) under this initial condition is considered below.

Eq. (5) is a linear differential equation of the first order and of the first degree in $N$ and its derivative. This type of equation may be solved using integrating factors. It can be shown that the solution of Eq. (5) under the initial condition $N(0) = N_0 > 0$ is given by

$$N(t) = \frac{P}{\lambda}\left(1 - e^{-\lambda t}\right) + N_0 e^{-\lambda t} \tag{6}$$

Similar to Eq. (4) from the previous section, Eq. (6) should be rewritten in terms of the observable cumulative number of disabled cells $N_d(t)$ as

$$N_d(t) = \left(1 - e^{-\lambda t}\right)\left(N_0 - \frac{P}{\lambda}\right) \tag{7}$$

where $\frac{P}{\lambda} < N_0$.

On the basis of the available data, the parameters of Eq. (7), that is, the initial number of the terrorist cells $N_0$, the disabling rate constant $\lambda$ (or the cell half-life $t_{1/2}$), and the rate of formation of new cells $P$, can be estimated. Eq. (7) is illustrated in Figure 2.

The figure reveals that the counterterrorist actions (evaluated through the disabling rate constant $\lambda = 0.139$ per year) are less effective when the rate of formation of new cells $P$ is five cells per year compared to the situation when the rate $P$ is only two cells per year. On the basis of Eq. (6), Figure 3 displays the above conclusion in terms of number of active cells.

Using models (6) and (7) one can estimate such important characteristics like the time needed to reduce the number of active cells to a given level, the number of active cells at any given time in the future, and so on.

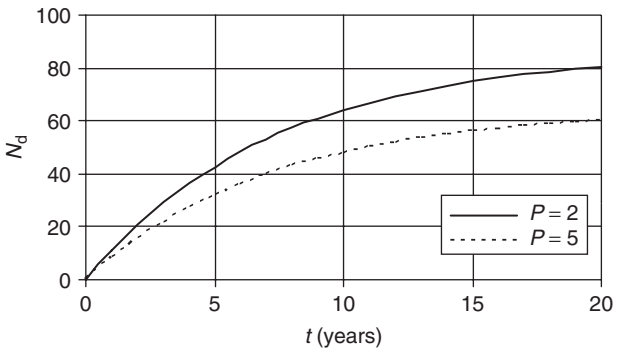



**FIGURE 2** Cumulative number of disabled cells $N_d$ as function of time, $t$: for initial number of cells $N_0 = 100$, disabling rate constant $\lambda = 0.139$ per year ($t_{1/2} = 5$ years), and different rates of formation of new cells $P = 2$ and 5.

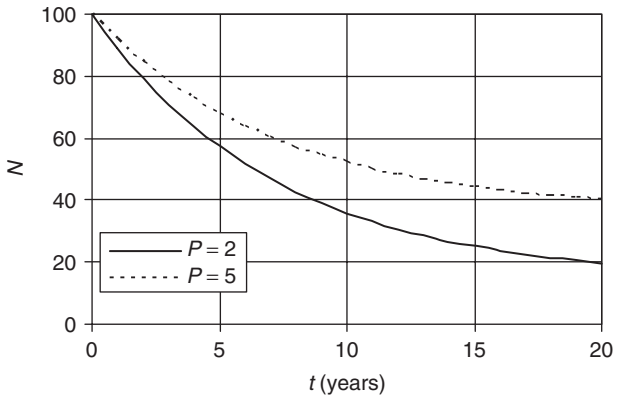



**FIGURE 3** Number of active cells $N$ as function of time, $t$: for initial number of cells $N_0 = 100$, disabling rate constant $\lambda = 0.139$ per year ($t_{1/2} = 5$ years), and different rates of formation of new cells $P = 2$ and 5.

## 4 TERRORIST POPULATION DYNAMICS MODEL AND LOTKA–VOLTERRA MODEL

As was mentioned above, one can find some analogy between the TPD model and the Lotka–Volterra model. This analogy is considered in more detail below. The Lotka–Volterra model was developed by the founders of Mathematical Ecology [7, 8, 10] as an attempt to understand the dynamics of biological system, in which a predator population interacts with a prey population.

Denote the prey population size by $N$. It is assumed that the prey population has unlimited food supply, and in the absence of predators, the prey population increases exponentially with a positive rate $r$, that is,

$$\frac{\mathrm{d}N}{\mathrm{d}t} = rN \tag{8}$$

On the other hand, the prey population decreases due to predator–prey encounters. If the current predator population size is $C$, then the predator consumption rate of prey is $\alpha CN$, so that

$$\frac{\mathrm{d}N}{\mathrm{d}t} = rN - \alpha CN \tag{9}$$

where $\alpha$ is the so-called attack rate.

In the absence of food, the size of the predator population $C$ decreases. Thus, in the framework of the Lotka–Volterra model, the predator population is assumed to decline exponentially in the absence of prey:

$$\frac{\mathrm{d}C}{\mathrm{d}t} = -qC \tag{10}$$

where $q$ is the predator mortality rate. This predator population decline is counteracted by predator birth. The predator birth rate is assumed to depend on two factors: the rate, at which the food is consumed, $\alpha CN$, and the predator's efficiency, $f$, at turning the food into predator offspring. Thus the following equation for the predator population size can be written:

$$\frac{\mathrm{d}C}{\mathrm{d}t} = f\alpha CN - qC \tag{11}$$

Eqs. (9) and (11) constitute the Lotka–Volterra model.

At this point, our objective is to adjust the Lotka–Volterra model to get the TPD model obtained in Section 3 using some nuclear physics analogy.

To get this model, one has to replace the notion of predators by counterterrorism forces and the notion of prey by a terrorist cell or individual. Using this new terminology, it is reasonable to begin with revising Eq. (9) and the main assumptions on which this equation is based.

In the framework of the Lotka–Volterra model, it is assumed that in the absence of counterterrorism forces (predators), the terrorist (prey) population has unlimited financial

and logistic support (food supply) and it increases exponentially according to Eq. (8), which solution is given by

$$N(t) = N_0 \, \mathrm{e}^{rt} \tag{12}$$

where $N_0$ is the initial (at $t = 0$) size of the population.

These assumptions applied to the TPD might be too strong to result in the exponential population growth. Keeping this in mind, the exponential terrorist population growth term in Eq. (9) has to be replaced by a linear growth term, which results in the following equation:

$$\frac{\mathrm{d}N}{\mathrm{d}t} = r - \alpha C N \tag{13}$$

Denoting $\alpha C$ by $\lambda$, one gets the TPD model (5) suggested in [9], but it should be noted that Eq. (13) has one more interpretable parameter $\alpha$ (the attack rate) when the information about factor $C$ (which was introduced above as the antiterrorist manpower, expenses related to antiterrorist operations, etc.) is available.

The solution of Eq. (13) can be written as

$$N(t) = \frac{r}{\alpha C}\left(1 - \mathrm{e}^{-\alpha C t}\right) + N_0 \, \mathrm{e}^{-\alpha C t} \tag{14}$$

From the data analysis standpoint, Eq. (14) is not convenient. In reality, one can observe only the cumulative number of disabled cells (denoted below by $N_\mathrm{d}$), which is given by

$$N_\mathrm{d}(t) = \left(1 - \mathrm{e}^{-\alpha C t}\right)\left(N_0 - \frac{r}{\alpha C}\right) \tag{15}$$

If $C$ is a time-dependent factor, Eq. (13) takes on the following form

$$\frac{\mathrm{d}N}{\mathrm{d}t} = r - \alpha C(t) N \tag{16}$$

The solution of the above equation is out of the scope of this article.

## 5 COST-EFFECTIVENESS ANALYSIS OF ANTITERRORIST EFFORTS

Let us assume that a steady amount of $S$ dollars is spent annually on the antiterrorist efforts in the framework of the model considered. The cost-effectiveness of the efforts can be evaluated using the following parameter $\varepsilon$:

$$\varepsilon(t) = \frac{S}{\dfrac{\mathrm{d}N_\mathrm{d}(t)}{\mathrm{d}t}} \tag{17}$$

which has the meaning of the cost of disabling one cell during a given year $t$. Using, for example, Eq. (7), the derivative in the denominator can be written as

$$\frac{\mathrm{d}N_{\mathrm{d}}(t)}{\mathrm{d}t} = \lambda \mathrm{e}^{-\lambda t}\left(N_0 - \frac{P}{\lambda}\right) \tag{18}$$

so that the cost-effectiveness equation (Eq. 17) takes on the following form:

$$\varepsilon(t) = S\frac{\mathrm{e}^{\lambda t}}{\lambda\left(N_0 - \dfrac{P}{\lambda}\right)} \tag{19}$$

Figure 4 illustrates the cost-effectiveness $\varepsilon$ time dependence for the same model parameters as it is shown in the previous figures. The figure shows that the cost per terrorist cell disabled is exponentially increasing as time goes on. The cost-effectiveness parameter $\varepsilon(t)$ can be applied to assess a time dependence of the risk associated with potential terrorist actions. The respective risk assessment is out of the scope of this article. Nevertheless, assuming that an acceptable risk level [11] is established, it is clear that the effectiveness parameter $\varepsilon(t)$ can be used for making a timely decision about the necessity of revising current antiterrorist policy.

## 6 STATISTICAL DATA ANALYSIS

The format of the data needed to fit the above discussed models can be given by a simple table with the following three columns:

1. Time (year or month)
2. Number of disabled cells
3. Optional column—cell origin (foreign or domestic)

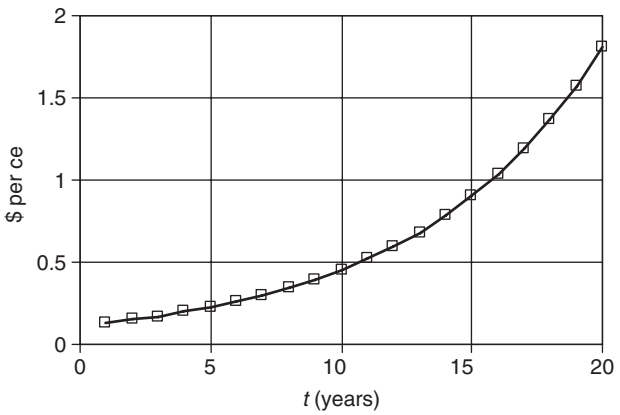



**FIGURE 4** Cost of disabling one cell during a given year $t$ per 1$ invested annually. Initial number of cells $N_0 = 100$, disabling rate constant $\lambda = 0.139$ per year ($t_{1/2} = 5$ years), and rate of formation of new cells $P = 5$.

Applying Eq. (7) to fit the respective data is far from being a trivial statistical problem, but it is doable. Moreover, applying Eq. (7) to real data can provide some extra benefits. For example, if the respective data can be divided into two groups—one for the terrorist cells of domestic origin and the other for the cells associated with terrorist penetration from outside [12], Eq. (7) can be applied separately to each group providing some more specific information, for example, one can get the following two equations with more informative parameters.

In the case of the terrorist cells of domestic origin, Eq. (7) takes on the following form:

$$N_{\mathrm{dd}}(t) = (1 - \exp(-\lambda_{\mathrm{d}} t)) \left( N_{0\mathrm{d}} - \frac{P_{\mathrm{d}}}{\lambda} \right) \tag{20}$$

where the parameters $N_{0\mathrm{d}}$, $P_{\mathrm{d}}$, and $\lambda_{\mathrm{d}}$ are associated with the cell of a domestic origin only. Compared to model (4), model (20) does not assume that the system of interest is 100% protected from the formation of the terrorist cells inside this system.

Correspondingly, in the case of the cells associated with (foreign) terrorist penetration only from outside is given by

$$N_{\mathrm{df}}(t) = (1 - \exp(-\lambda_{\mathrm{f}} t)) \left( N_{0\mathrm{f}} - \frac{P_{\mathrm{f}}}{\lambda} \right) \tag{21}$$

where the parameters $N_{0\mathrm{f}}$, $P_{\mathrm{f}}$, and $\lambda$ are related to the terrorist cells of a foreign descent.

Obviously, models (20) and (21), when their parameters estimated, provide the information that can be used for balancing the efforts related to counterterrorism actions inside the system and the efforts protecting its borders.

### 6.1 Case Study

The *Sourcebook of Criminal Justice Statistics 2003* [13] provides the data on terrorist incidents and preventions in the United States from 1980 up to 2001. In this source, terrorism prevention is defined as "a documented instance in which a violent act by a known or suspected terrorist group or individual with the means and a proven propensity for violence is successfully interdicted through investigative activity". For lack of other available data, it is excusable to assume that the annual number of preventions is close to the annual number of disabled cells (note that, strictly speaking, the number of terrorism prevention is equal or less than the number of the respective disabled cells).

Based on this assumption, one can use model (7) to fit the data on the terrorism preventions. In this case, model (7) takes on the following form:

$$N_{\mathrm{p}}(t) = \left(1 - \mathrm{e}^{-\lambda t}\right) \left( N_0 - \frac{P}{\lambda} \right) \tag{22}$$

where $N_{\mathrm{p}}$ is the cumulative number of preventions (disabled cells) and $\frac{P}{\lambda} < N_0$.

For the given case study, the selected data related to the time interval 1984–1994 were used. The data are displayed in the first two columns of Table 1.

In order to better interpret these data, the reader is referred to the Naftali's monograph on the history of modern terrorism [4].

Based on the data given in Table 1, the nonlinear least square estimates of the parameters of model (20) were obtained as follows:

**TABLE 1 Number of Terrorism Preventions**

| Year | Number of Terrorism Preventions | Cumulative Number of Preventions (Observed) | Cumulative Number of Preventions (Fitted Using Eq. (22)) |
|---|---|---|---|
| 1984 | 9 | 9 | 15.1 |
| 1985 | 23 | 32 | 27.4 |
| 1986 | 9 | 41 | 37.4 |
| 1987 | 5 | 46 | 45.5 |
| 1988 | 3 | 49 | 52.1 |
| 1989 | 7 | 56 | 57.5 |
| 1990 | 5 | 61 | 61.8 |
| 1991 | 5 | 66 | 65.3 |
| 1992 | 0 | 66 | 68.2 |
| 1993 | 7 | 73 | 70.5 |
| 1994 | 0 | 73 | 72.4 |

disabling rate $\lambda = 0.208$ per year ($t_{1/2} = 3.339$ years),
initial (related to 1983) number of cells $N_0 = 131$, and
rate of formation of new cells $P = 10.534$ per year.

Cumulative numbers of preventions fitted using Eq. (20) are given in the right column of Table 1, and illustrated in Figure 5. The fraction of variation of $N_p$ explained by the fitted model is 0.974.

## 7 CONCLUSIONS

Among the numerous methods of risk analysis related to the problems of combating terrorism, the data analysis does not always receive adequate attention mainly owing

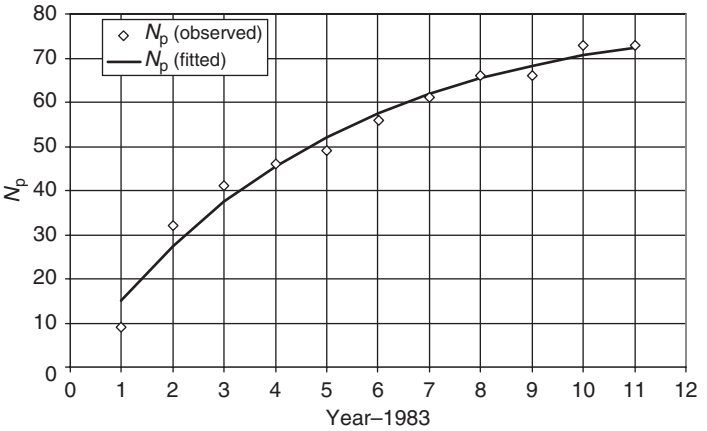



**FIGURE 5** Observed and fitted cumulative number of terrorism preventions $N_p$.

to the classified status of most relevant data. Nevertheless, developing methodology of the data analysis related to counterterrorist actions constitutes an important part of the respective methodological tools needed.

As an example of these tools, the TPD model is introduced. The model describes the evolution of the system in terms of time dependence of the number of terrorist cells $N(t)$ acting inside the considered system. The model includes only interpretable parameters, such as the initial number of terrorist cells $N_0$, the disabling rate constant $\lambda$ (or the cell half-life $t_{1/2}$), and the rate of formation of new cells $P$.

The suggested cost-effectiveness parameter $\varepsilon(t)$ is based on the cost per terrorist cell disabled as a function of time. If combined with a given acceptable risk level related to terrorist actions, the parameter can be used for making a timely decision regarding the necessity of revising current antiterrorist policy.

Another important issue raised concerns balancing the efforts related to counterterrorism actions inside the system and the efforts needed to protect its borders.

From the standpoint of data collection and analysis, it is important that the only observable variables needed are the annual (or monthly) numbers of disabled (or identified) terrorist cells. On the basis of these data, the suggested model can evaluate the number of terrorist cells $N(t)$ acting inside the system at any given time (including current and predicted numbers), the initial number of the terrorist cells $N_0$, the disabling rate constant $\lambda$ (or the cell half-life $t_{1/2}$), and the rate of formation of new cells $P$.

On the basis of the results of model parameter estimation, one can estimate such important characteristics like the time needed to reduce the number of active cells to a given level, the number of active cells at any given time in the future, and so on.

Using a case study, it is shown that the model parameters can be successfully estimated applying the nonlinear least squares fitting. It should be noted that the suggested models can be applied to other criminal populations, for example, illegal immigrants and drug offenders.

## REFERENCES


1. Smith, R. Armed Forces Communications and Electronics Association (AFCEA). (2001). Modeling and simulation adds insight on terrorism. *Signal Mag* December, 31–35.
2. Raczynski, S. (2004). Simulation of the dynamic interactions between terror and anti-terror organizational structures. *JASSS*. **7**(2), http://jasss.soc.surrey.ac.uk/7/2/8.html.
3. Linden, E. V. Ed. (2004). *Foreign Terrorist Organizations: History, Tactics and Connections*. Nova Science Publishers, Inc., New York.
4. Naftali, T. (2005). *Blind Spot. The History of American Counterterrorism*, Basic Books, New York.
5. Bertulani, C. A., and Schechter, H. (2002). *Introduction to Nuclear Physics*, Nova Science Publishers, Inc., New York.
6. Draper, N. R., and Smith, H. (1998). *Applied Regression Analysis*, 3rd ed., Wiley, New York.
7. Begon, M., Harper, J. L., and Townsend, C. R. (1996). *Ecology: Individuals, Populations, and Communities*, 3rd ed., Blackwell Science, Cambridge, MA.
8. Gotelli, N. J. (1998). *A Primer of Ecology*, 2nd ed., Sinauer Associates, Sunderland, MA.
9. Kaminskiy, M., and Ayyub, B. (2006). Terrorist population dynamics model. *Risk Anal. Int. J.* **26**(3), 747–752.

10. Volterra, V. (1931). Variations and fluctuations of the number of individuals in animal species living together. In *Animal Ecology*, Translated from 1928 edition by R. N. Chapman, Ed. McGraw-Hill, New York.
11. Ayyub, B. M. (2003). *Risk Analysis in Engineering and Economics*, Chapman & Hall/CRC Press, Boca Raton, FL.
12. Pate-Cornell, E. (2004). On signals, response, and risk mitigation. In *Accident Precursor Analysis and Management*, J. R. Phimister, V. M. Bier, H. C. Kunreuther, Eds. The National Academic Press, Washington, DC.
13. U.S. Department of Justice, Federal Bureau of Investigation. (2006). *Terrorism 2000/2001*, http://www.albany.edu/sourcebook/pdf/t3173.pdf.

## FURTHER READING

Harris, B. (2004). *Mathematical methods in combating terrorism*. *Risk Anal. Int. J.*. **24**(4), 985–989.

Farley, J. D. (2003) Breaking Al Qaeda cells: A mathematical analysis of counterterrorism operations (A guide for risk assessment and decision making). *Studies in Conflict & Terrorism*. **26**, 399–411.

Wilson, A. G., Wilson, G. D., Olwell, D. H., Eds. (2006). *Statistical Methods in Counterterrorism: Game Theory, Modeling, Syndromic Surveillance, and Biometric Authentication*, Springer, New York.

# SENSING AND DETECTION

# PROTECTING SECURITY SENSORS AND SYSTEMS

TODD P. CARPENTER
*Adventium Labs, Minneapolis, Minnesota*

## 1 INTRODUCTION

Security systems are key protection elements which prevent, detect, mitigate, minimize, and aid recovery from natural, accidental, and intentional threats ranging from weather effects, illness and disease, to misguided youth, hardened criminals, and terrorists. The security systems can be focused on the outside, perimeter, or be inward facing. The systems can be self-contained, such as common smoke detectors, or they can include multiple sensors of different types, integrated together over a distributed sensing and power network with storage of events, sensor fusion and event correlation, and automatic escalation of event notification based on severity. These systems can be purely physical (e.g. military trip wire and flash bang), or heavily supported by electronic sensing and analysis. Security systems considered in this article integrate some type of sensor, reasoning (is it an event or not?), and alarm or state annunciation. Simpler physical security systems, such as a door lock or a Sargent and Greenleaf [1] lock on a file cabinet, are not explicitly addressed. Locks have their own fascinating and evolving issues, which can be explored in [2–5]. Systems considered here share the potential for physical, cyber, and social engineering vulnerabilities that attackers can exploit to overcome the security system. This article provides an overview of threats, potential weaknesses, and some risk-reduction approaches and resources to consider when designing, developing, or applying a security system.

## 2 BACKGROUND

Prevention or deterrence, confidence bolstering, detection, mitigation, minimization of effects, and recovery, including providing forensic evidence, are potential benefits of security systems. The overt presence of a security system, such as visible cameras or biometric sensors, might deter some class of criminals or other adversaries from attempting to enter the premises. The same security system in a bank might inspire confidence in

potential customers—if the bank looks safe, they might be more inclined to do business there. Security event detection and subsequent notification of guards or other authorities are perhaps what people normally think of as security systems. Security systems support mitigation when they provide situation awareness that the responders can leverage to address ongoing events, such as cameras or motion detectors that indicate conditions or attacker locations. Minimizing the effects or reducing the potential impact of a successful attack, might be considered a side effect of a security system. (For instance, installing a real security system on a high-value asset, such as critical infrastructure, is rarely a trivial exercise. In the process, one might presume that subject matter experts analyze what is being protected. If toxic chemicals in storage tanks are the asset, one might reassess how much material needs to be on hand and reduce the amount if possible.) Security systems might also help recovery and forensics efforts by providing causal information and information used to identify the attackers.

Understanding why a security system is installed can give attackers clues about how to defeat aspects of the system about which the attacker cares, or it might completely deter the attacker. During reconnaissance, a potential attacker might size up security systems and select the least protected target. There's an old adage that says you only have to make your security better than the neighbor. That does not really apply when protecting our intertwined infrastructures. Seasoned professionals might note model numbers and designs of the security units (Decoy cameras might not provide much value in this case. Unfortunately, deterrence does not always work. Despite fences, locks, visible cameras, energized high-voltage lines, and fatalities from earlier attempts, thieves are attacking the US electric grid for copper to sell on the scrap market [6]), and devise specific attacks, or choose to accept the exposure that would go along with an attack.

The following subsections will describe the broad classes of attacks and provide an abstract model of a security system. The next section will discuss specific threats, attacks on the sensor and security systems based on attacker goals and capabilities, and possible solutions. The remaining sections will cover future directions and recommended approaches to designing and acquiring security systems.

### 2.1 Classes of Attacks

Social engineering is the practice of discovering and exploiting humans to gain information or access. It can be as simple as ignoring the security system and merely joining in with other people entering work in the morning, from their smoke break on the loading dock, or mingling with a crowd reentering a building after a fire alarm drill (which are common during fire-safety week in the United States), or as complex as wooing a bank staff personnel with chocolates, and walking away with €21m of diamonds [7]. Unfortunately, a worthy treatment of this topic is beyond the scope of this article. The Art of Deception [8] is a highly recommended read, because a fool with a tool is still a fool: If the people specifying, researching, designing, building, operating, and managing the security system are not appropriately trained, technology might not impede the determined attackers.

Cyber attacks are a broad class of electronic-based attacks, which affect code or data in the security system. For this treatment, physical attacks are those that employ physical effects or tangible material to cause desired sensor behavior (e.g. use of fingerprint

duplicate to gain access through a reader) or physically change the state of the security system (e.g. sever an alarm wire so that the alarm cannot be activated). We are not considering physical attacks such as armed attackers overcoming the guard, since you probably want your security system to provide enough notification that your guards would be prepared for and fend off any credible attack of that sort. Many attacks combine multiple aspects of physical and cyber attacks; for example, a denial-of-service cyber attack might create an opportunity for the compromised maintenance personnel to add access credentials enabling future attacks. Another attack could create specific false security events through some physical or cyber interactions. Eventually, the guards could get used to ignoring that particular alarm, or disable it altogether, which would be an example of leveraging cyber or physical attacks into social engineering. Incidentally, avoiding alarm saturation leading to guard conditioning of this sort is one of the reasons why low "false-positive" rates are so important.

## 2.2 Security Sensors and Systems

The abstract security system shown in Figure 1 identifies the external interfaces to a security system and major internal components. Examples of classes of security sensors and how they are used and implemented are shown in Table 1. Information from the sensors is processed according to configuration settings, optionally stored in a historical database along with timestamp and other identifying information, and state and alarms are presented to the operator. The security system might also actuate some mechanical device, such as unlocking a door. The primary inputs to the security system are power, environmental conditions (e.g. ambient light, temperature, motion, the supporting structure, humidity, or precipitation), control inputs from the operator, and the actual sensed security events. Processing can be performed on custom hardware (e.g. smoke

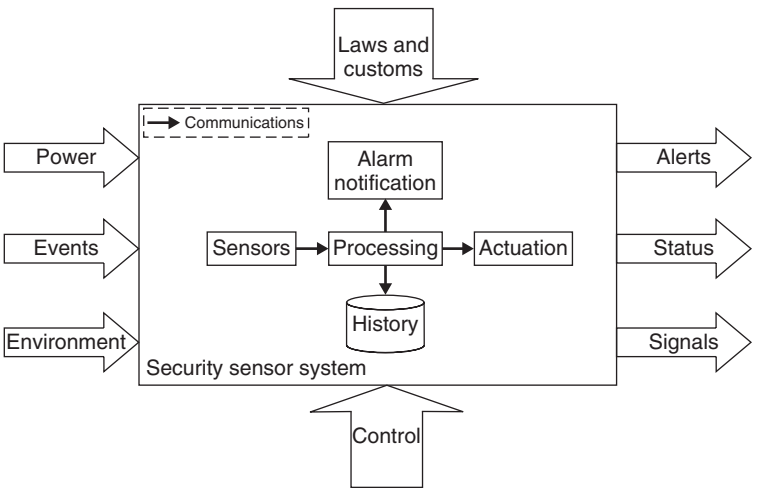



**FIGURE 1** Abstract security system: showing both the external environment with inputs, constraints, outputs, and control, and internal system components of sensor(s), communications, processing, history, and notification.

**TABLE 1 Security Sensor Examples: Broad Classes of Sensors Employed in Security Systems, Including Example Applications and Implementations**

| Sensor | Example Uses | Example Sensor Implementations | See Also |
|---|---|---|---|
| Contact | Door open/close/event | Simple mechanical or magnetic reed switches, photoelectric or hall effect sensors | Perimeter Security Contact and Proximity Sensors |
| Motion | Identify motion in area | Passive infrared, active IR, visible light camera, microwave, buried cable capacitance, accelerometers | Video Surveillance Sensors: Cameras and Digital Video Recorders; Video Sensor Systems and Integrated Cameras |
| Fingerprint | Identify individuals | Capacitance, thermal, visual, pressure | Checkpoint Access Control Sensors for Identity Management; Automated Fingerprint Indentification Systems |
| Hand geometry | Identify individuals | Capacitance, thermal, visual, pressure | Checkpoint Access Control Sensors for Identity Management |
| Iris | Identify individuals | Visible, IR camera | Checkpoint Access Control Sensors for Identity Management; Video Surveillance Sensors: Cameras and Digital Video Recorders; Video Sensor Systems and Integrated Cameras; Eye and Iris Sensors |
| Voice | Identify individuals | Microphone | Voice Recognition and Speaker Identification Sensors |
| Facial | Detect and identify individuals | Visible, IR camera, light detecting and ranging (LIDAR) laser | RADAR and LIDAR Perimeter Protection Sensors; Infrared Sensors and Systems; Face Recognition Sensors 2D Face Recognition Sensors and Their FR Algorithms; 3D Face Recognition Sensors-Technological Challenges and Potential Benefits; Normalization and Morphing of Face Images for Improved Face Recognition Sensors |
| Pressure plate | Detect occupation | Mechanical, piezo, and accelerometers | Perimeter Security Contact and Proximity Sensors |

**TABLE 1 (*Continued*)**

| Sensor | Example Uses | Example Sensor Implementations | See Also |
|---|---|---|---|
| Particulate | Detect smoke or other particulates | Ionization, optical detection | Knowledge Extraction from Surveillance Sensors; Checkpoint Access Control Sensors for Identity Management; Perimeter Security Contact and Proximity Sensors; RADAR and LIDAR Perimeter Protection Sensors; Video Surveillance Sensors: Cameras and Digital Video Recorders; Video Sensor Systems and Integrated Cameras; Infrared Sensors and Systems; Remote Un-Manned Surveillance Sensors; Sensors for Airborne Video Surveillance Applications; Physical Forms of CB Threats; Design Considerations in Development and Application of Chemical and Biological Agent Detectors; Sensing Dispersal of Chemical and Biological Agents in Urban Environments; Technologies for Sensing Terrorist use of Chemical and Nerve Agents Threats; Use of Biological Agent Sensors in Homeland Security; Sensing Releases of Highly Toxic and Extremely Toxic Compounds |
| Chemical | Detect presence of chemical agent | Capacitive, reactive, micro-electro mechanical systems (MEMS) vibration | Knowledge Extraction from Surveillance Sensors; Checkpoint Access Control Sensors for Identity Management; Perimeter Security Contact and Proximity Sensors; RADAR and LIDAR Perimeter Protection Sensors; Video Surveillance Sensors: Cameras and Digital Video Recorders; Video Sensor Systems and Integrated Cameras; Infrared Sensors and Systems; Remote Un-Manned Surveillance Sensors; Sensors for Airborne Video Surveillance Applications; Physical Forms of CB Threats; |

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| Sensor | Example Uses | Example Sensor Implementations | See Also |
|---|---|---|---|
| | | | Design Considerations in Development and Application of Chemical and Biological Agent Detectors; Sensing Dispersal of Chemical and Biological Agents in Urban Environments; Technologies for Sensing Terrorist use of Chemical and Nerve Agents Threats; Use of Biological Agent Sensors in Homeland Security; Sensing Releases of Highly Toxic and Extremely Toxic Compounds |
| Biological | Detect presence of biological agent | Reactive, fluorescence | Knowledge Extraction from Surveillance Sensors; Checkpoint Access Control Sensors for Identity Management; Perimeter Security Contact and Proximity Sensors; RADAR and LIDAR Perimeter Protection Sensors; Video Surveillance Sensors: Cameras and Digital Video Recorders; Video Sensor Systems and Integrated Cameras; Infrared Sensors and Systems; Remote Un-Manned Surveillance Sensors; Sensors for Airborne Video Surveillance Applications; Physical Forms of CB Threats; Design Considerations in Development and Application of Chemical and Biological Agent Detectors; Sensing Dispersal of Chemical and Biological Agents in Urban Environments; Technologies for Sensing Terrorist use of Chemical and Nerve Agents Threats; Use of Biological Agent Sensors in Homeland Security; Sensing Releases of Highly Toxic and Extremely Toxic Compounds |
| Radiation | Detect presence of ionizing radiation | $\alpha$, $\beta$, $\gamma$, neutron, X-ray radiation detectors using photomultipliers, charge-coupled devices, gaseous detectors | Radioactive Materials Sensors; Sensing Dirty Bombs |

**TABLE 1 (*Continued*)**

| Sensor | Example Uses | Example Sensor Implementations | See Also |
|---|---|---|---|
| Temperature | Detect temperature variations | IR sensor, thermistor, thermocouple | Perimeter Security Contact and Proximity Sensors |
| Card reader | Identify bearer | Magnetic, RF | Checkpoint Access Control Sensors for Identity Management |
| RFID | Identify bearer | Passive RF, active RF | Checkpoint Access Control Sensors for Identity Management |
| Explosives | Detect explosives | Chemical vapor detectors, neutron detectors | Sensors for Weapons Concealment in Shipments; Sensing Body Worn Concealed Weapons and Explosives; Detection of Metallic and Ceramic Concealed Weapons in Hand Carried Articles; Detection of Concealed Explosives and Chemical Weapons in Hand carried Baggage |

detectors, embedded motion sensors) or on general purpose processors running standard operating systems (e.g. web-enabled cameras running on Linux or integrated security systems built on top of Microsoft Windows). The communications connecting all these elements might be copper, fiber, wireless (radio frequency (RF) or microwave), or any combination thereof. The sensor communications network might be separate from the rest of the security network, or everything might be hosted on the corporate local area network (LAN). The next section describes how all of these elements can be exploited by attackers to gain some desired advantage.

## 3 THREATS, VULNERABILITIES, AND RISK MITIGATION

We begin here with an overview discussion of specific threats, vulnerabilities, and risk mitigation without going into exhaustive detail. More detail will be provided in the various technical articles and case studies in the rest of the handbook. Other sources of vulnerability information can be found at popular conferences such as DEFCON [9] and Black Hat [10] and online security tracking and reporting such as 'SysAdmin, Audit, Network, Security (SANS) Institute' [11].

### 3.1 Threats

Considered generically, attackers might be grouped into different categories, including petty thieves, disgruntled employees, and criminal organizations. If we consider security systems protecting US critical infrastructure, we might also include joy riders (teenagers in the countryside with a new rifle shooting insulators on high-voltage power lines),

environmental terrorists (ranchers toppling high-voltage power towers), state-sponsored terrorists, strategic threats, and naturalized radical elements. Of these, the deterrence effects of strong security systems might eliminate many of the nuisance attacks and petty theft; though we have seen it does not deter copper theft. The other threats are interesting because they possess technical and monetary resources, and indirectly affecting US critical infrastructure is plausibly within their goals. See also Part I, Organizational, Structural, and Policy Issues for a more detailed treatment of possible threats and motivations.

Of particular note are the capabilities that potential attackers bring to bear, whether it is cash to buy off-the-shelf tools, fabricate new tools, or invest in research and evaluation of sensors and systems to identify vulnerabilities. Such attackers can also expend human capital—people willing or coerced into probing security systems.

### 3.2 Individual Vulnerabilities

Considered independently, the ways by which physical phenomenology is sensed by each of the security sensors, shown in Table 1, have characteristics that can be exploited. Switches can be shorted or mechanically altered. Motion sensors can be overwhelmed by intense light or fooled by slow movement. Voiceprints can be fooled by recordings.

Security sensors that interact with cards and radio frequency identification (RFID) also have issues. Barcode and magnetic strip cards can be duplicated. Smart cards, such as in the new contactless e-passports, can be cloned [12–15]. RFID and card readers can be spoofed and jammed [16, 17] or communicated with from a distance far exceeding their design specifications [18]. Industry advocates claim that this is not a problem [19], perhaps ignoring the fact that one difference with contactless cards is that the bearers have no way of detecting when their personal information have been compromised.

Additional problems might arise when vulnerable biometrics on the smart cards are solely relied upon, especially if the biometric sensing and matching is automated. Vulnerabilities of biometric sensors is a whole topic by itself [20–23] and the handbook section Terrorist Identification and Recognition, and it is recognized that “there is no one perfect biometric that fits all needs” [24]. Hollywood is full of tales of biometric compromises, some of which even work, such as disguises, lifting fingerprint from surfaces, reactivating latent fingerprints on readers, and gelatin fingerprints made with molds or inkjet printers [25]. To combat latent fingerprint reactivation, fingerprint “swipe” readers require a finger to be drawn across a linear imager, as opposed to pressed against a 2D plate. However, such systems do not inherently address the problem of prosthetics made from fingerprints left elsewhere or photographed.

Iris recognition systems are attractive due to the reliability and ease of biometrics capture without having to touch sensors that other people have touched or submit to possibly intrusive or damaging scans. This is an issue with fingerprint and handprint devices, and a concern with retina scans. However, some iris systems have been compromised with paper copies of irises [26] and printed contact lenses, and have had to develop countermeasures [27].

Facial recognition systems are similarly attractive since faces are generally considered public information and do not require contact for acquiring images. This is not

universal—some cultures claim that it is their right to keep their faces covered. The 2D facial recognition systems have been spoofed with photocopied images and disguises. Researchers have even regenerated (false) images from stored templates (a template is an abstraction of biometric characteristics, so the original image does not need to be stored) that are sufficient enough to fool biometric systems [28].

Chemical and biological sensors can be vulnerable to false positives (getting swamped with false readings), suffer time lag for individual measurements, and can require significant maintenance and upkeep. Radiological and nuclear sensors are vulnerable to shielding, though detection technology continues to advance (*see* Radioactive Materials Sensors).

### 3.3 Combined Sensor Vulnerabilities

Since all these sensors are individually vulnerable, the careful user will apply sensors in combination to secure an area. For instance, "liveness" detectors coupled with a biometric sensor can rely on different physical attributes, such as conductivity, moisture content, temperature or thermal emissions, and movement. However, when the specific measured characteristics are understood, prosthetics can be developed to mimic "liveness" [26].

Movement can be simulated with motion video (e.g. playback on a monitor held in front of the video capture device), eyeholes cut though a face picture and held over the attacker's face, or even clipping a pupil hole in a picture of an iris and holding it over the attacker's eye. Video systems that capture multiple bands (e.g. visible, near, and far infrared (IR)) make spoofing more complex, but not impossible. Of course, such trivial attacks are unlikely to work when a security guard is present and attentive, but makeup printing systems [29], prosthetics, and printed contact lenses can potentially help the attacker blend appropriately.

However, as the complexity of spoofing the sensor(s) increases, at some point the attacker will start to look at other parts of the security system. This might also be driven by the attacker's risk sensitivities. For instance, suicide terrorists might only care about premature detection, but once the attack is underway, detection and identification might even serve the cause. Such attackers might be satisfied with a quick-and-dirty approach that gets them through the obvious security sensors, even though the whole attack might not stand up to forensics or even close scrutiny. In contrast, state-sponsored strategic threats, such as long-term economic warfare, might rely on clandestine operations, so detection and identification are highly undesirable. Overt sensor jamming might prevent identification, but unless it looks like a normal system failure, it might be enough to detect an attack is underway, and other system evidence could lead to threat mitigation and exposure.

### 3.4 Security System Vulnerabilities

When overcoming the sensors themselves becomes too complex or costly, the attacker can turn to vulnerabilities in the supporting system. The first thing that the attacker might do is avoid sensors altogether, for example, by entering through an unprotected window or at the loading dock. We will rashly assume that a security system installation is better designed than that, and focus on the elements described in Figure 1. One method to attack the sensor system is a simple denial of service: disable the power, for instance, by cutting cables or shorting lines. One would expect critical installations to have backup

power, so the thoughtful attacker might also foul the diesel backup fuel. A remote site might have internal battery backups, so attacks on the backup power might not be easy to carry out. However, depending on the responsiveness of repair crews, the batteries might run out before crews can arrive. A good system's design would ensure that the repair service-level agreement is within the worst-case battery lifetime. It would also require a hard-to-masquerade heartbeat from the security system, so losing either power or communications would invoke an immediate response.

A more extreme power-based attack is to invoke a high-voltage transient on the power or communications lines to destroy security sensors and systems. Well-designed equipment will have surge protection. However, surge protection has voltage, energy, and frequency limits, which mean the attack can escalate. A disadvantage of this type of attack is that it is difficult to remain clandestine, especially if there is collateral damage on the surrounding power grid.

The attacker might also leverage environmental conditions to exploit weaknesses in the security system. For instance, heavy precipitation storms might temporarily reduce the effectiveness of exterior sensors, such as motion detectors, visible light cameras, acoustic sensors, and even buried RF and microwave loops. Extreme temperatures and humidity might affect a variety of systems, including visible and IR cameras and even fingerprint readers. Such systems should be carefully evaluated under worse case situations, and if the sensors fail, at least the guards should be warned to be particularly vigilant under those circumstances.

Environmental effects might also be induced by the attacker. For example, IR lasers can cause localized heating that could temporarily disable or destroy sensors or communications. This could be done from a distance, over a long period of time, during warm days so that it looks like a normal, heat-induced failure. Heating, ventilation, and air conditioning (HVAC) systems and controls could be tampered with; causing control or server-room conditions that can result in downtime for the security system or supporting infrastructure. The author has been on security audits in critical infrastructure where there was no access control beyond the front door of the installation, where the HVAC control workstation sat in a dusty corner without the benefit of even a screen blanker with password protection. It would have been trivial to update HVAC set points for some desired future time.

Inputs can also be forged, such as submitting false enrollment documents, then showing up for badging. Hopefully this requires significant social engineering, on-site presence, and explicit signature from an authority, rather than just a couple of forged e-mails to security staff. It would be unfortunate if industry-wide cost-cutting approaches (e.g. six sigma and lean manufacturing) optimized away necessary security cross-checks due to overemphasis on short-term cost.

Everything within the security system in Figure 1 can itself be a target to the attacker. Communications can be physically interrupted, corrupted, or altered, especially if cables are insufficiently protected. Wireless networks are growing in popularity, yet common standards like 802.11b/g have serious weaknesses [30]. Wired equivalency privacy (WEP) and WiFi protected access (WPA), security protocols for Wi-Fi networks attack toolkits are available on the Internet (*see* Wireless Security), so industrial grade security must be layered on top of whatever is provided by the underlying protocol. The wired protocols are not inherently secure anymore; it is just that the attacker needs a closer physical proximity than required by wireless. Therefore, security communications should be secured even on internal wired networks, lest a daytime visitor or nighttime cleaning crew inserts a

router between a legitimate host and the network jack on the wall and siphons away all sorts of useful information.

The security processing itself can be attacked. Unless the operating systems that host the security software are locked down (all unnecessary services disabled, strict access policies, etc.) and operating system (OS) patches are applied as soon as they are available, the underlying platform can be corrupted. Once that platform is owned by an attacker, software on top of it can no longer be trusted. Attackers could potentially have arbitrary control authority, including remote control of the display console using popular tools such as VNC or PCAnywhere. Even without an operating system level attack, access to the security system software might be gained by something as basic as default passwords or shared passwords. Installation policies should require changing all default passwords, but this can be tricky if the vendor buries features. For example, I once had a web-enabled security camera with a 10/100 Ethernet port on it, so it could sit right on the LAN, and it could serve FTP images, push images over e-mail or FTP, stream video, and so on, and included quite capable video compression and motion detection software. Unfortunately, I lost the administrator password and could not find a hardware reset pin; so I checked the manufacturer's website. Someone else had asked about recovering the administrator password, and the response was to provide the IP address of the camera, and the manufacturer would reset the camera remotely. Note that the manufacturer was in Korea.

The security system's history and configuration information are also target rich for an attacker. Such information might be contained in application files or in a commercial database that has its own cyber vulnerabilities. Attackers can change configuration information to disable features or add themselves to access control lists or insiders who could escalate their existing privileges. They can also delete incriminating events from the historical logs, or add/modify events to incriminate others or obfuscate causality to impede forensic investigations.

The actuators and alarms, including displays, can also be attacked. Examples of actuators controlled by the security system include access control portals (doors) and illuminators. Promiscuous eavesdropping on communications might enable capture of commands that unlock the desired doors. Security systems should have strong cryptographically secured communications that prevent such playback attacks and spoofing attacks. Displays can be altered to misdirect or suppress alerts. For instance, HTML-injection attacks can intercept and modify display information on web-based security interfaces.

In summary, all of the elements of a security system have vulnerabilities which, if exploited, can subvert the intent of the security system. The following section describes possible techniques to help assess the risk in the system and make decisions about mitigation techniques.

### 3.5 Risk Mitigation

Risk is a key security concept and is often considered as a product of the threat, vulnerability, and consequences. Therefore, a big threat with small vulnerability and consequences might be less important to address than something that is medium in all those categories. Humans do not always assess risk uniformly [31], so transparent methods that capture incremental results and rationale, and track the reasoning process are important for making reasoned and defensible decisions. There are, of course, multiple

ways to design, select, install, staff, train, and maintain security systems to minimize risk. Presumably there are even multiple correct methods, but there are some clear-cut bad ideas.

One example of what not to do is blindly trust vendor claims. Consider a USB memory stick that claimed a self-destruct system activated if users do not know the correct password. This is conceivably the type of device that well-intentioned people could use to store passwords, private keys, or personal information. One group purchased several such devices and discovered multiple hardware and software hacks to defeat the protections. Perhaps even worse, no evidence of any "self-destruct" capability was discovered. [32]

However instructive such tales are, there are probably infinitely many ways to do things wrong. The next subsections describe some process steps that one can employ to better design, specify, implement, and maintain security systems. These, or equivalent processes, can be (should be) addressed by security sensor developers, security system providers, and the end users.

If trained staff is unavailable for the necessary analysis, design, and assessment, appropriately credentialed third-party services should be acquired. Credentials to consider include, but are certainly not limited to, Physical Security Professional (PSP), Certified Information Systems Security Professional (CISSP), Certified Information Privacy Professional (CIPP), Information Systems Security Architecture Professional (ISSAP), and appropriate training provided to US military, such as force protection and the full spectrum integrated vulnerability assessment (FSIVA). If you intend to rely on an individual, do not take his/her credential claim at face value—check up on it to see if it is valid. In addition, do not rely too much on single individuals. As mentioned before, security systems face social engineering, physical, and cyber threats. So, build a team versed in all these aspects, as well as understand the objectives of the business or infrastructure applying the security system, and has someone who understands the threat environment.

Credentials can also apply to the security systems and individual components in the system. Listings of Underwriters Laboratories provide an indication that professionals have looked at some aspects of the system. A common criteria certification is another good indicator that the system or component has undergone some level of structured design and evaluation by security experts.

Next, pick an assessment process, rather than creating your own. There are multiple processes out there, and you can select one to suit your needs and adapt as appropriate. For example, a long-time-available approach is NIST SP-800-30, "Risk Management Guide for Information Technology Systems" [33]. The security risk assessment methodologies (RAM) of Sandia National Laboratories [34] are possibly already tailored for your critical infrastructure. American Society of Mechanical Engineers (ASME) offers risk analysis and management for critical asset protection (RAMCAP), a risk-based methodology to support resource allocation for critical asset protection [35]. FSIVA and the related Joint Staff Integrated Vulnerability Assessment (JSIVA) are supported by the National Guard and the Defense Threat Reduction Agency (DTRA). In the author's opinion, these methods are all excellent and share many similarities. You are encouraged to pick one—when multiple good choices are available, it is more productive to make progress following a good process rather than spending a whole lot of time deciding which one to follow.

The rest of this article uses NIST SP-800-30 as the baseline for an extremely brief overview of an assessment process, identifying several critical steps. NIST SP-800-30 is convenient since it is a freely available public standard. It is adaptable to multiple domains—it works for evaluating the security sensors, the system in which the sensors

reside, and the installation at the end user. One minor adaptation we make is to explicitly consider it a cyclic, repetitive process, since security is not a finished product. Good security must continually adapt to evolving threats, so assessments and changes to the system are periodically necessary.

The first step of the risk assessment is to define the scope of the effort. The boundaries of the system, area, region, base, or critical are identified, along with the resources and the information that constitute the system under evaluation. Characterization establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g. infrastructure dependencies, personnel, communications, and responsible division or support personnel) essential to defining the risk.

Next, we consider the various threat actors or adversaries that might be motivated to attack the system. One approach is to have the stakeholder decision makers (not necessarily the analysts in subsequent steps) rank the relative importance of the various adversary organizations, based on business or political realities. For instance, it might not be reasonable to expect a rural infrastructure operator to withstand a focused attack from a state-sponsored strategic threat. Early knowledge of the threat allows the remaining analysis resources to focus on more realistic threats. One approach to ranking the adversaries once they are identified is to use Dr Thomas Saaty's Analytic Hierarchy Process [36, 37] for implementing this ranking, since a potentially a large number of items need to be ranked relative to each other. Note that this mechanism does not say these are the biggest threats; but will just show where the assessment is going to focus resources. This is already common practice; for instance, studies document the significance of the insider threat [38, 39], yet many organizations still focus their resources outwardly. Motivation for this could be political and marketability reasons as well as technical reasons.

After the attackers are identified and ranked, experts familiar with the adversary groups capture abstract attackers' goals, methods, and capabilities. Do they want to steal things or destroy them? Do they plan to get away or are they suicides? Are security systems deterrents for them? Can your system provide early enough detection of an imminent attack to provide opportunity for mitigation? The point is not to try to predict what the attacker will do, but rather to develop guidance on what security measures might provide utmost benefit for the resources you have available. These can be combined and ranked, using the earlier adversary ranking as weighting factors to the individual goals and capabilities, using matrix-based decision support techniques such as quality function deployment (QFD). It is useful to separate goals and ways of achieving those goals from capabilities and resources.

Now we focus on the system which is being secured, and assume the attacker's perspective and consider what within that system can be used to achieve the attacker's goals. Next we develop high-level scenarios that might achieve these goals and capture associated attack costs and results. These scenarios can then be ranked against the attacker's goals and capabilities to give a relative ranking of attractiveness from the attacker's perspective. Then the scenarios are mapped according to their attractiveness against their significance or impact from the defender's perspective. This is an analog to the typical likelihood versus impact risk mapping, and provides an overall ranking of scenarios that fuses both attacker and defender perspectives.

Since protecting against individual scenarios is a losing proposition, the next step is to disassemble and rank the vulnerabilities that enable these scenarios. Mitigating controls (e.g. specific security sensors, protections on communications, redundant power

supplies, and maintenance and backup schedules) are then identified and mapped against these common mode enablers according to potential efficacy. This provides a ranking of which mitigations are most valuable, as well as a long-term plan for what to address as new resources become available.

Finer grained analysis can help determine the residual risk. An attack tree process [40] allows one to model the system under assessment and include specification of defensive mitigations (e.g. layered defenses such as cameras, locks, multiple barriers, and guards), and costs of overcoming these mitigations. Attackers are modeled with abilities and the attack tree tool maps the attackers' capabilities to the attack graph, and prunes infeasible attacks. It is particularly useful for prevention/detection/mitigation trade-offs, and can help to quantify the difference in residual risk between adding, for instance, cameras versus additional security staff, and where the "sweet spot" is for a particular site.

Another approach to consider is penetration testing, although this should be viewed as additional information—penetration tests are insufficient by themselves. It is worth the effort to consider standard steps in a penetration test framework [41] and make sure that the low hanging fruit documented there does not apply to you.

## 4 FUTURE RESEARCH DIRECTIONS

For the security sensor or system designer, much work remains in standards to specific security requirements, especially to cover multidisciplinary attacks that cover social engineering, physical, and cyber attacks. There is a lot of security art and lore in the industry (e.g. security checklists), but the underlying science and ability to quantitatively rate all aspects of security is lacking. Basic academic research is necessary to advance the science, followed by investment in engineering tools that can bring the science into the state of the practice.

Antitamper capabilities are an additional aspect to consider for system components. However, the state-of-the-art in commercial systems is still evolving, and one can search the Internet for Xbox hacks to see how effective tenacious, organized attackers are. New "trusted platform modules" (TPM), if properly integrated with the operating system (either of smart sensors or the security integration system), can provide a foundation for a chain of trust, but the effort required to achieve the necessary integration is still significant, and attacks on TPM-enabled machines have been reported. Beyond the TPM, IBM's secure processor architecture, which brings the protection boundary onboard the main CPU, is another step up, and is something to watch in the future; especially as such systems gain traction. Clearly, pure software-based approaches are insufficient for protection, as is any single-mode defense. Aspects of an antitamper defense-in-depth strategy might include device level protections, such as those provided by Altera Stratix II FPGA or Xilinx CoolRunner II CPLDs. Coatings, such as Foster-Miller Inc. provide, offer additional protections that raise the cost of getting into chips. Enclosure protections, such as those provided by Mektron Systems Limited and WL Gore, can wrap the alarm devices with tamper resistant coatings. Several software packages are available, which can help resist attack, such as Accord Solutions—BruteSafe, Arxan Defense Systems—EnforcIT, and Architecture Technology Corporation—Tornado, Twister, and Cloakware. However, all of these techniques, even when applied together, might only delay certain classes of attackers.

## 5 CONCLUSIONS

Security systems are an important aspect of protecting our critical infrastructure, but automation, sensors, and reliance on vendor claims can only go so far. Careful design, attention to policies, training of staff, and continual reassessment are necessary to maintain a strong security posture.

## REFERENCES


1. Sargent and Greenleaf. http://www.sglocks.com/, 2007.
2. Locksport International. http://www.locksport.com/, 2007.
3. Lock Picking 101. http://www.lockpicking101.com/, 2007.
4. The document formerly known as *The MIT Lockpicking Guide*, http://people.csail.mit.edu/custo/MITLockGuide.pdf, 2007.
5. Blaze, M., Safecracking for The Computer Scientist, Department of Computer and Information Science University of Pennsylvania. (2004). http://www.crypto.com/papers/safelocks.pdf.
6. Central Electric Cooperative Connections. (2007). *Copper Wire Theft Can be Deadly*, http://www.cme.coop/miscellaneous/pdf/May07/May12–13.pdf, 2008.
7. The Independent. (2007). *Thief Woos Bank Staff with Chocolates—then Steals Diamonds Worth £14m*, http://news.independent.co.uk/europe/article2369019.ece.
8. Mitnick, K. D. (2001). *The Art of Deception*, John Wiley & Sons, New York, ISBN: 978-0471237129.
9. DEFCON, http://www.defcon.org/, 2007.
10. Black Hat Conference, http://www.blackhat.com/, 2007.
11. SANS Institute, http://www.sans.org/, 2007.
12. Grunwald, L., DN-Systems GmbH Germany. (2004). *New Attacks against RFID-Systems*, Black Hat, https://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Grunwald.pdf.
13. Jacobs, B. and Wichers Schreur, R. (2005). *"Biometric Passport", Security: Applications, Formal aspects and Environments, in the Netherlands Workshop*, Radboud University, Nijmegen, http://wwwes.cs.utwente.nl/safe-nl/meetings/24-6-2005/bart.pdf.
14. The Register (2007). *How to Clone a Biometric Passport While it's Still in the Bag*, http://www.theregister.com/2007/03/06/daily_mail_passport_clone/.
15. Wired (2006). *Hackers Clone E-Passports*, http://www.wired.com/science/discoveries/news/2006/08/71521.
16. Rieback, M. (2006). *A Hacker's Guide to RFID Spoofing and Jamming*, DEFCON 14, Vrije Universiteit Amsterdam, Amsterdam.
17. Mahaffey, K. (2005). *Flexilis "Passive RFID Security"*, Black Hat, Las Vegas, United States, https://www.blackhat.com/presentations/bh-usa-05/bh-us-05-mahaffey.pdf.
18. Kfir, Z. and Wool, A. (2005). *Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems*, Tel Aviv University, http://eprint.iacr.org/2005/052.pdf.
19. RFID Journal Industry Group. (2007). *Says E-Passport Clone Poses Little Risk*, http://www.rfidjournal.com/article/view/2559/.
20. NIST Biometrics http://www.itl.nist.gov/div893/biometrics/, 2007.
21. International Biometric Group IBG. http://www.biometricgroup.com/, 2007.
22. Biometrics Consortium. http://www.biometrics.org/, 2007.

23. InterNational Committee for Information Technology Standards (2006). *Study Report on Biometrics in E-Authentication*, INCITS M1/06-0112, http://www.incits.org/tc_home/m1htm/2006docs/m1060112.pdf.

24. Podio, F. L. and Dunn, J. S. (2001). *Biometric Authentication Technology: from the Movies to Your Desktop*, NIST, http://www.itl.nist.gov/div893/biometrics/Biometricsfromthemovies.pdf.

25. Matsumoto, T. Matsumoto, H., Yamada, K., Hoshino, S. (2002) Impact of artificial gummy fingers on fingerprint systems. *Proceedings of SPIE Volume No. 4677*, Optical Security and Counterfeit Deterrence Techniques IV http://www.imaging.org/store/physpub.cfm?seriesid=24&pubid=562, San Jose, CA.

26. Matsumoto, T. (2004). *Gummy Finger and Paper Iris: An Update*, Yokohama National University, Workshop on Information Security Research, Fukuoka, http://www-kairo.csce.kyushu-u.ac.jp/WISR2004/presentation12.pdf.

27. International Biometric Industry Association. (2005). *Iridian Technologies Announces Enhanced Countermeasures to Detect Printed Contact Lenses*, http://www.ibia.org/biometrics/industrynews_view.asp?id=148.

28. Adler, A. (2003). *Sample Images can be Independently Restored from Face Recognition Templates*, University of Ottawa, Ontario, http://www.site.uottawa.ca/~adler/publications/2003/adler-2003-fr-templates.pdf.

29. Liang, J. J. (2006). Desktop Personal Digital Cosmetics Make Up Printer, US Patent Application 20060098076.

30. Wagner, D. (2004). Security in wireless sensor networks. *Commun. ACM* **47**(6), 53–57, ISSN:0001-0782.

31. Slovic, P. (2000). *The Perception of Risk*, Earthscan Publications, London, ISBN: 978-1853835285.

32. Tweakers.Net. (2007). *Secustick Gives False Sense of Security*, http://tweakers.net/reviews/683/1.

33. NIST SP 800 30. (2007). *Risk Management Guide for Information Technology Systems*, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

34. Sandia National Laboratories. *Security Risk Assessment Methodologies*, http://www.sandia.gov/ram/, 2007.

35. ASME. (2007). *Risk Analysis and Management for Critical Asset Protection (RAMCAP)*, http://www.asme-iti.org/RAMCAP/.

36. Saaty, T. L. (1980). *The Analytic Hierarchy Process*, McGraw-Hill, New York.

37. Using the analytic hierarchy process for decision making in engineering applications: some challenges. *Int. J. Ind. Eng. Appl. Pract.* **2**(1), 35–44, 1995.

38. National Security Telecommunications And Information Systems Security Committee. (1999). *The Insider Threat to U.S. Government Information Systems*, http://www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf.

39. Reconnex. (2005). Insider Threat Index—Year to Date Findings, http://akamai.infoworld.com/weblog/zeroday/archives/files/Reconnex%202005%20Insider%20Threat%20Findings.pdf.

40. Amenaza. *SecurITree: The Hostile Risk Modeling Software*, http://www.amenaza.com/, 2007.

41. Orrey, K. and Lawson, L. (2007). *Penetration Testing Framework*, http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html.

## FURTHER READING

A highly recommended book is Ross Anderson's "Security Engineering," especially for system's designers. He drives home the point that the little details really do matter, and good security is

an engineering process, not just cobbling together functionality. Anderson, R. J. (2001). *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, ISBN: 978-0471389224.

The TRADOC DCSINT Handbooks on terrorism are also recommended to put the threat in perspective. *A Military Guide to Terrorism in the Twenty-First Century*, US Army Training and Doctrine Command, August 2005, http://handle.dtic.mil/100.2/ADA439876.

If you are a security system developer who thinks they are smart enough to develop or use anything other than standard, approved encryption packages, you must first read the basics such as Bruce Schneier's "Applied Cryptography" and "Secrets and Lies". Then read the crypto mini-FAQ and follow sci.crypt for a couple years. If you are a purchaser of security systems, I do not encourage you to use security systems (or any other systems) that claim proprietary encryption algorithms.

Schneier, B. (1995). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd Edition, John Wiley & Sons, New York, ISBN: 978-0471128458.

Schneier, B. (2004). *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, ISBN: 978-0471453802.

# THREAT SIGNATURES OF EXPLOSIVE MATERIALS

LISA THEISEN

*Contraband Detection, Sandia National Laboratories, Albuquerque, New Mexico*

## 1 INTRODUCTION

Explosives detection systems can be categorized by application (e.g. detect explosives concealed on people, in packages, or in vehicles) as well as by technology (e.g. imaging or anomaly detection vs. trace detection). The unique characteristics of explosives have enabled researchers to develop a variety of explosives detection systems that capitalize on those properties that separate explosives from other materials. Properties such as vapor pressure, density, dielectric number, and effective atomic number are exploited in the detection of explosives.

Explosives detection methods are divided into two main technologies: trace detection and bulk detection. Trace detection technology searches for residue of explosives and bulk detection technology for larger amounts of explosives. Trace explosives techniques collect and analyze a sample of air or residue to detect explosive vapor and/or particles. The sample is collected and analyzed, and on the basis of a chemical analysis the material

is detected. To generate a sample to collect and analyze, trace detection depends on vapor pressure. Sometimes taggants, which are additions to commercially manufactured explosives, can be the target for a successful trace detection. Bulk explosives techniques measure characteristics of the materials in question in an attempt to detect the possible presence of large amounts of explosives. Bulk techniques use a probing radiation source to detect variations in density, dielectric number, and effective atomic number of explosives. While none of these characteristics are unique to explosives, they can indicate a high probability of the presence of explosives.

## 2 SCIENTIFIC OVERVIEW

### 2.1 Explosive Terms Defined

An *explosive* is defined as a chemically unstable solid or liquid material that undergoes an extremely rapid conversion to form other stable gaseous materials (or products). The transformation is self-propagating, and results in explosion with the liberation of heat and the production of a shock wave from the rapid gas formation. This transformation is called *combustion* and requires sufficient oxygen and fuel to be present to maintain the reaction.

The three main types of chemical explosives are propellants, primary, and secondary. Propellants are combustible materials that burn violently and produce large volumes of gas, but do not detonate. Propellants are used to propel projectiles such as bullets or rockets. Primary explosives are characterized by their sensitivity to heat or shock and tend to detonate readily and rapidly and are used mainly to detonate secondary explosives and thereby initiate an explosive chain. Secondary explosives are generally more powerful (larger detonation velocity) than primary explosives. Secondary explosives are designed to be insensitive to heat and shock to ensure safe handling and storage. Therefore, explosive devices typically utilize a small amount of primary explosives to detonate a larger amount of secondary explosives. This article focuses on secondary explosives (also known as *high explosives*) and there will be no further discussion of propellants and primary explosives.

## 3 ELEMENTS THAT COMPRISE EXPLOSIVE MATERIALS

Generally, secondary explosives contain oxygen (O), nitrogen (N), carbon (C), and hydrogen (H), where the fuel and the oxidizer bond together in the same molecule. In an explosive, carbon and hydrogen are the fuel and oxygen is the oxidizer. Figure 1 shows a selection of secondary explosives that have a wide variety of structures. Explosive compounds can be divided into classes, which are characterized by their functional groups, as follows:

- nitroaromatic compounds contain $C-NO_2$ groups (e.g. TNT, 2,4,6-trinitrotoluene);
- nitramines contain $N-NO_2$ groups (e.g. RDX, also known as *hexogen* or *cyclonite*);
- nitrated esters contain $C-O-NO_2$ groups (e.g. PETN, pentaerythritol tetranitrate);
- peroxide compounds contain O–O bonds (e.g. TATP, triacetone triperoxide).

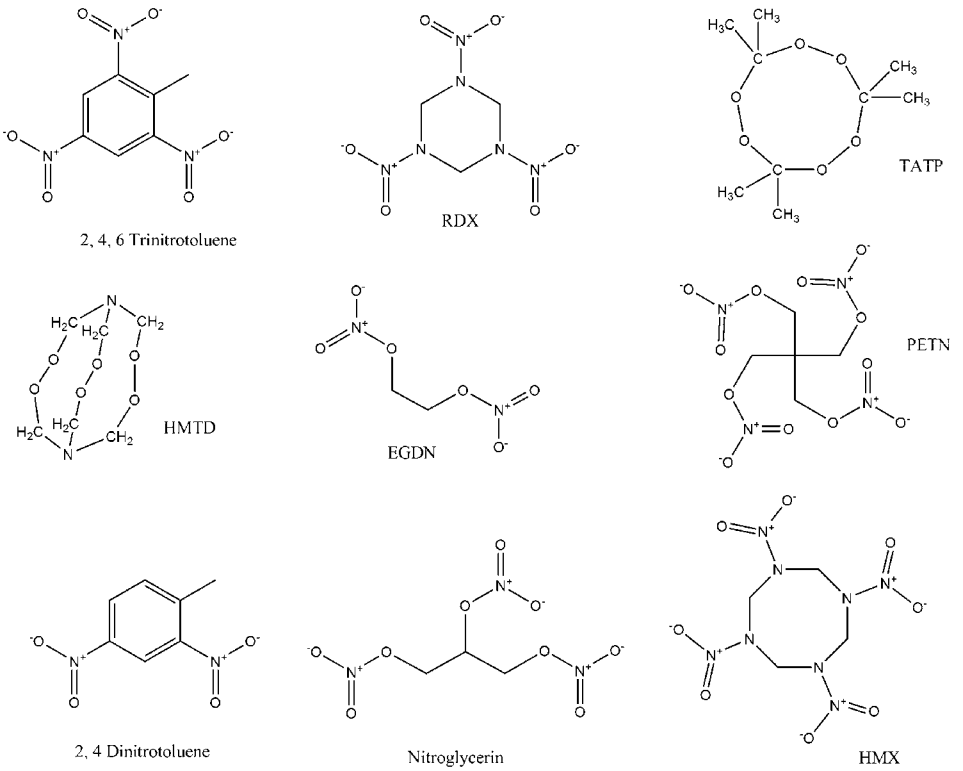



**FIGURE 1** Structures of secondary explosives including nitramines (RDX and HMX), nitroaromatics (TNT and DNT), and nitrated esters (PETN, EGDN, and NG) and of peroxide-class compounds (TATP and HMTD).

## 4 VAPOR PRESSURE OF EXPLOSIVE MATERIALS

All solids and liquids emit some amount of vapor into their surroundings (the environment). The released vapor is in equilibrium with the remaining solid or liquid and this unique property is called *vapor pressure*. Some explosive materials do not readily form a vapor (low vapor pressure explosives) and therefore have a low amount of vapor in the air. Some explosive materials exhibit a high vapor pressure and thus have a substantial amount of vapor in the air. The quantity of available vapor can affect opportunities for detection.

Figure 2 shows the maximum vapor concentrations of different explosives in air at room temperature. Note that the vertical axis is logarithmic; each hash mark corresponds to a factor-of-ten increase in vapor concentration. The vapor pressures of explosive materials (as illustrated in Fig. 2) span more than 12 orders of magnitude. This variation means that, depending on the vapor pressure of the explosive of interest, one would or would not anticipate the presence of explosive vapor for detection purposes.

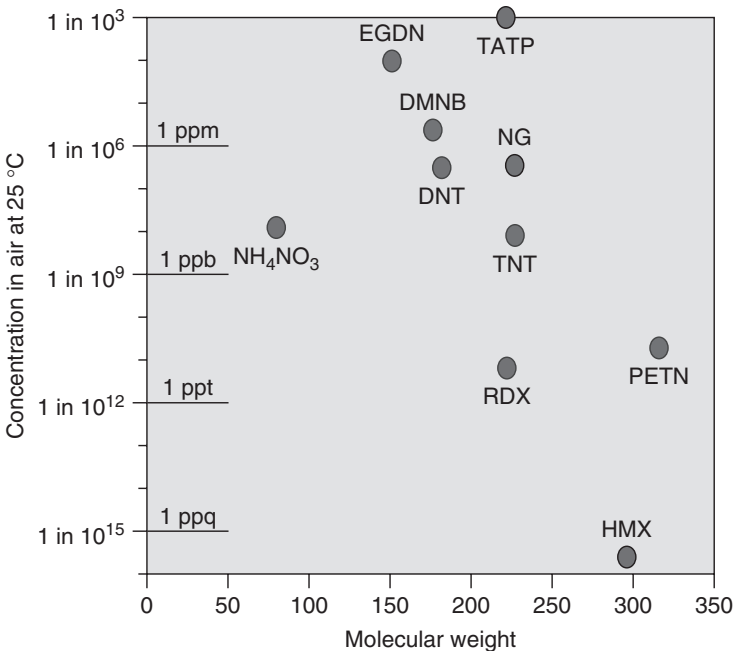



**FIGURE 2** Vapor concentration of high explosives in saturated air at 25°C (vapor concentrations are approximate). Top—high vapor pressure compounds. Bottom—low vapor pressure compounds.

In general, explosives can be categorized by their vapor pressures and vapor concentrations, as follows:

- *High* vapor pressure explosives include ethylene glycol dinitrate (EGDN), TATP, nitroglycerin (NG), and 2,4-dinitrotoluene (DNT). These explosives have equilibrium vapor concentrations in air on the order of about 1 ppm or greater, which means that there will be roughly one molecule of explosive vapor for every million molecules in the air.
- *Medium* vapor pressure explosives have equilibrium vapor concentrations in air near 1 ppb. The medium vapor pressure group includes TNT and ammonium nitrate ($NH_4NO_3$).
- *Low* vapor pressure explosives have equilibrium vapor concentrations in air near or below 1 ppt, approximately 1000 times lower than the medium vapor pressure explosives. The low vapor pressure group includes HMX (octogen), RDX, and PETN. These vapor pressures are for the pure materials.

## 5 EXPLOSIVES DETECTION

### 5.1 Overview

Explosives detection methodologies are divided into two major categories: trace detection and bulk detection methods (Fig. 3.) Trace and bulk explosives detection methods are very complementary and exhibit different strengths.

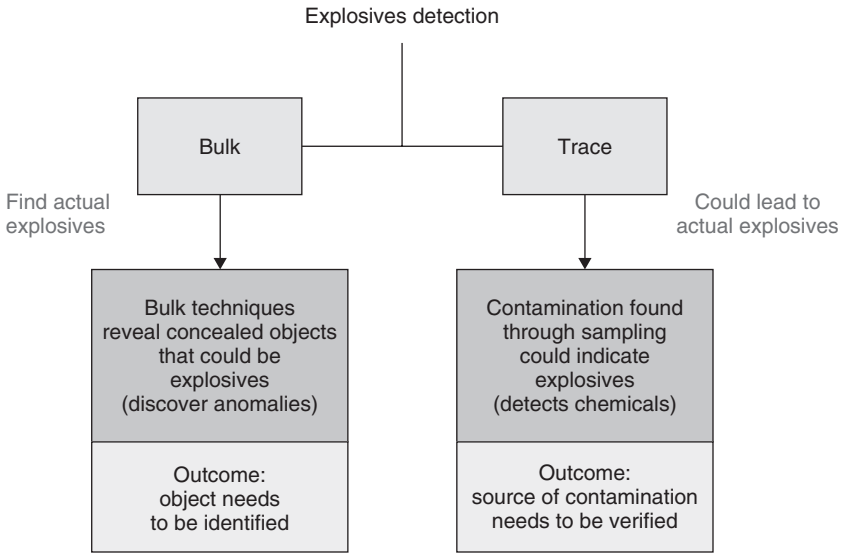



**FIGURE 3** The two types of explosives detection methodologies: trace and bulk.

- *Trace explosives detection* looks for *residue or contamination* from handling or being in proximity to explosive materials. Trace detection involves the chemical detection of explosives by collecting and analyzing a sample that contains tiny amounts of explosive vapor or particles. Canines are considered a biological trace detection method because they sample odors.
- *Bulk explosives detection* seeks the *actual explosive material* (a visible amount of explosives). The detectable mass is much larger for bulk detection than the quantity of material for trace detection. Bulk detection is usually imaging based or exploiting other molecular properties (i.e. density) of the explosive. Bulk detection methods are less dependent than trace detection methods on sample collection due to the anticipated larger amount of material present. Bulk detection is not affected by an explosive contamination background.

## 5.2 Trace Explosives Detection

Trace explosives detection is the acquisition and analysis of small, physically acquired samples in search of explosive residue (or contamination) in very low quantities, either in the form of vapor or particles (Fig. 3).

With trace detection, not all explosives alarms indicate a real bomb threat. A valid explosives detection alarm can occur if the object under inspection has been exposed to trace amounts of explosive material for legitimate reasons. For example, when screening people, it is possible to generate a valid alarm with a frequently prescribed heart medication, even though no bomb is present. Additionally, some regions around the world may have an environment contaminated with a background signature of explosive residues.

Even though trace explosives detection seeks out only the residue present on an item, person, or vehicle, an alarm may ultimately reveal a large amount of explosives. For example, a shipping box is examined by a trace technology; the sensor may detect trace

residue on the box exterior. The magnitude of the detection from the trace technology does not necessarily relate to the quantity of explosive that may be present.

Alarm resolution is a very important issue when using trace explosives detection technologies, because the explosive materials could be legitimately used.

The following are two sample types for trace detection analysis:

- *Vapor.* Gas-phase molecules that are emitted from a solid or liquid explosive. The concentration of explosives in the air is related to the vapor pressure of the explosive material and to other factors such as temperature, humidity, and air circulation.
- *Particle.* Microscopic particles of the solid explosive materials that adhere to surfaces (i.e. by direct contact with the explosive or, indirectly, through contact with someone's hands who has been handling explosives).

### 5.3 Explosive Vapor Detection

Explosive vapor detection is the sampling and analysis of airborne, vapor-phase explosive materials. The sample is collected without contacting the surface of the sampled item. Sampling strategies are critical because of the broad range of vapor pressures that could be encountered. The large variation in the range of all explosive materials' vapor pressures presents a huge challenge in the successful detection of trace amounts of explosives via a vapor sample.

High vapor pressure explosive materials have a significant amount of vapor present at any time, and any small particles that may be present tend to evaporate. Usually, high vapor pressure explosive materials are best detected with vapor detection. Dynamites, which usually contain EGDN and/or NG as an explosive ingredient, are examples of high vapor pressure materials and these can usually be detected from their vapor. Detecting these compounds by swiping surfaces (i.e. particle collection) is also possible, but may be less effective.

### 5.4 Explosive Particle Detection

Particle detection is the acquisition and analysis of microscopic solid explosive materials. The sample is collected by swiping the surface of the item. This sampling method requires direct contact to remove explosive material particles from a surface with a swipe pad provided by the manufacturer. The swipe pad is then inserted into a sampling port on the explosives detection system, and within seconds, it is analyzed for the presence of explosives. Personnel screening is not usually performed with surface swiping because many individuals would find the method invasive.

Low vapor pressure explosive materials have a significant amount of solid material present and produce very little vapor. Efforts to detect these compounds using trace technology must focus on swipe collection of particles.

Low vapor pressure explosives tend to be sticky, and a person handling a piece of solid explosive material will quickly transfer large amounts of contamination (explosive particles) to the hands. Explosive material contamination will be transferred to any additional surfaces touched by the hands, which likely will include the person's clothing as well as doorknobs, tabletops, and other objects he or she touches.

Particle contamination consists of microscopic solid particles, often on the order of a few micrograms. Most bomb builders and carriers will not be meticulous, which would result in particle contamination.

Although it is difficult to generalize how much explosives contamination is in a fingerprint, a typical fingerprint will contain numerous particles. When working with low and medium vapor pressure explosives at room temperature, more explosive materials are found to be contained in the fingerprint than would be present in a liter of air saturated with vapor (by a factor of 1000–1,000,000). Thus, for low and medium vapor pressure explosives, explosives detection is usually based on particle detection. The pure explosive materials, RDX and PETN, have extremely low vapor pressures, and the vapor pressures of plastic explosives such as C–4, Semtex, and Detasheet (which contain RDX and/or PETN as the explosive material) are even lower due to the presence of oils and plasticizing agents that give the material its form. Swipe collection is the preferred method to obtain a sample for these explosives.

Surface swiping (also called *particle sampling*) works best with small packages, briefcases, and purses (most notably, at many airports), but can be adapted to sampling larger suspect items, such as vehicles.

The choice of obtaining a vapor or particle sample is dependent on the explosive's vapor pressure. Vapor pressure is highly temperature dependent and has a dramatic effect on the amount of explosive vapor present. On a cold day, little explosive vapor is available and more vapor is available on hot days. Therefore, the most appropriate trace detection method depends on the explosive material and environmental conditions. Sometimes the situation will determine the most appropriate trace detection method. For an unknown or unattended item that may contain a detonable explosive, vapor collection is preferred in spite of the advantage of better sample collection through swipe methods.

## 5.5 Taggants

When low vapor pressure explosives (such as plastic explosives) are manufactured by legitimate suppliers, they are spiked with a high vapor pressure, nitrogen-containing compound called a *taggant* to make them more easily detectable. In 1989, the United Nations' International Civil Aviation Organization (ICAO) adopted a standard on the addition of taggants to manufactured plastic explosives. These taggants have high vapor pressures (similar to NG or EGDN) that make vapor detection of plastic explosives possible. However, relying on the presence of the taggant for vapor detection of plastic explosives is risky. Homemade (and some foreign-made) plastic explosives do not contain taggants. Also, as plastic explosives age, taggant material is lost to the environment because of its high vapor pressure. Nevertheless, detection of one of the taggants using vapor sampling with a trace explosives detection system should be interpreted as possibly indicating the presence of a plastic explosive.

## 5.6 Trace Detection Technologies Equipment

The explosives and security sector is evolving and the list of new commercially available detector technologies is expanding. A critical part of any trace explosives detection system will be the ability to separate different materials in the sample to individually analyze them. The individual component's separation is accomplished typically by the addition of a gas chromatographic (GC) column on the inlet portion of the detector. A GC column is a very adaptable hardware and can be used in combination with almost any detector that uses gas flow.

### 5.7 Canine Detection of Explosives

Trained canines (dogs) are used more than any other technology for the detection of explosives under real-world conditions. A dog's nose is the best vapor sensor that evolution has offered and it competes favorably with man-made detection technologies under many circumstances. A dog's nose is orders of magnitude more sensitive than a human's nose for detecting airborne odors.

Dogs are the detection method of choice for applications that involve any search component. Dogs are highly mobile and can search a building significantly faster than any other technology. Dogs can also rapidly follow a scent to its source.

In principle, dogs can be trained to detect any explosive material. Training is crucial in the development of an effective explosive-detecting dog. Dogs undergo a regular retraining program to maintain optimal performance. A dog will perform best when work conditions closely match the training conditions.

Dogs have a low purchase cost but have high continuing costs, including the handler's labor and refresher training for the handler and dog team. Dogs require a dedicated handler throughout their working lifetime. A handler–dog team's schedule might be 8- to 10-h days, 5 days a week, with rest-times every 2 h. If a dog has no major health problems, it can work from 8 to 10 years.

### 5.8 Bulk Detection

Bulk explosives detection is the second major category of explosives detection methodologies (as shown in Fig. 3). Bulk detection is characterized by the inspection of a sample *in situ* (where no attempt is made to obtain a sample for analysis) for visible, or macroscopic, amounts of explosives. Bulk explosives detection techniques use a probing radiation source (i.e. electromagnetic (EM) radiation or neutrons) to irradiate and interrogate an object, such as a suitcase full of clothing and toiletries. Upon irradiation, the response is measured from all the materials present in the object and a decision is made whether any material in the object is an explosive or not.

Bulk explosives techniques measure some bulk properties of the material in question in an attempt to detect the possible presence of visible quantities of explosives. Some of the properties of interest are density, dielectric number, and effective atomic number ($Z$ number) of the material.

Bulk explosives techniques are divided into two broad technology categories called *imaging* and *nuclear based* (Fig. 4). Imaging techniques are typically X-ray, microwave, or millimeter-wave interrogation technologies. Nuclear-based techniques probe the atomic nuclei of the material under inspection. Some nuclear-based techniques interrogate a sample with high-energy radiation and monitor the detection of $\gamma$ rays. Another nuclear-based technique uses radio waves for determining the presence of quadrupolar nuclei.

### 5.9 Electromagnetic Radiation

EM radiation can be defined as the energy of a specific wavelength traveling through space, such as solar rays. Figure 5 shows the EM spectrum with wavelengths ranging from short ($10^{-12}$ m) to long ($10^{2}$ m). The long-wavelength radiation on the left-hand side of Figure 5 has low energies and the short-wavelength radiation has high energies.

EM radiation can be categorized as ionizing or nonionizing radiation. The terms *ionizing* and *nonionizing* radiation indicate whether the EM radiation possesses enough

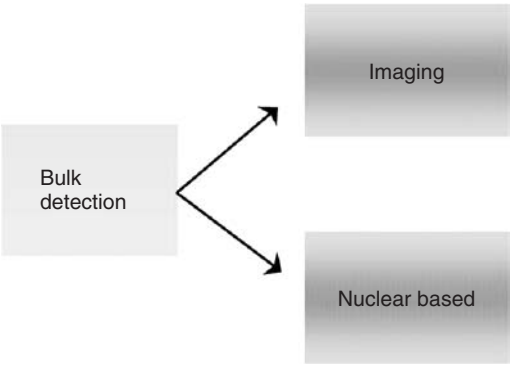



**FIGURE 4** Two broad categories that describe bulk explosives detection. Imaging-based techniques examine a material's bulk property. Nuclear-based techniques probe the nucleus of the material under inspection.

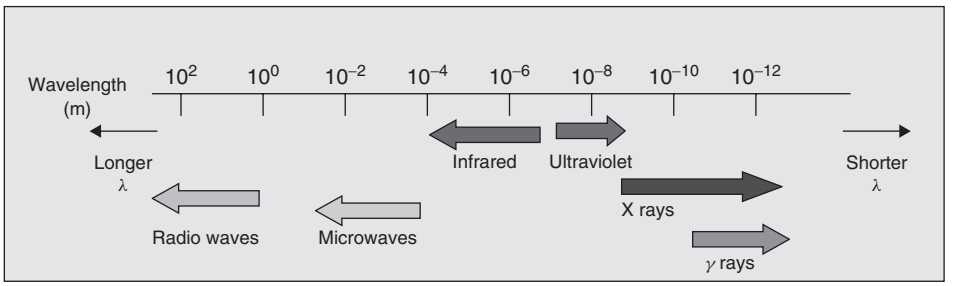



**FIGURE 5** Electromagnetic spectrum illustrates the broad range of radiation and how the different wavelength regions are designated. Only a very tiny portion of the electromagnetic spectrum is visible to the human naked eye and it encompasses a range of approximately $4–7 \times 10^{-7}$ m, which is in between infrared and ultraviolet radiation.

energy to cause ionization in the atoms with which it interacts. Ionization is the process of removing electrons from atoms in molecules (such as water, protein, and DNA) with EM radiation. Nonionizing radiation is lower in energy than ionizing radiation and will not remove electrons from atoms. Examples of nonionizing radiation are radio waves, microwaves, and visible light.

Energy of ionizing radiation can be high, and it can originate from radioactive materials, high-voltage equipment, and stars. There are four types of ionizing radiation: $\alpha$ particle, $\beta$ particle, $\gamma$ ray (X rays), and neutron particle. The main difference between X rays and $\gamma$ rays is their different origins. X rays originate from energetic electrons and $\gamma$ rays from an atom's nucleus.

## 5.10 Imaging Technologies

The imaging category encompasses bulk techniques that use EM radiation of different wavelengths to interrogate items of interest to produce an image of the object.

Commercially available imaging technologies utilize X rays (including single- and dual-energy X rays, and backscatter X rays), microwaves, and millimeter waves.

Microwaves and millimeter waves use nonionizing radiation. X rays are ionizing radiation and can potentially affect the normal function of cells in the human body, and so should be used with caution. A cumulative radiation dose could have adverse health effects.

Figure 6 pictorially represents three common ways that EM radiation interacts with matter, composed of atoms and molecules. The three interaction outcomes are

- passes through the material with no interaction (transmission);
- interacts with the material (absorption and/or emission process);
- strikes the material and deflects off its original course (scattered or backscattered).

The three outcomes occur in distinct percentages determined by the energy of the probing radiation and the bulk characteristics of the materials.

X-ray techniques exploit the interaction characteristics of explosives as compared to other common materials. The properties such as density and effective atomic number ($Z$) are keys for distinguishing high-$Z$ materials (metals) from low-$Z$ materials (including H, O, and C elements).

Imaging technologies that are not X-ray-based are sometimes called *anomaly detectors*. These techniques seek changes in a material's property (other than elemental composition) as it scans the material under inspection. For example, dielectrometry measures the dielectric constant differences in an item with microwaves.

## 5.11 Nuclear-Based Technologies

Nuclear-based technologies interrogate the nucleus of the material under inspection with EM radiation and monitor for its characteristic emission. Current commercially available nuclear-based technologies utilize neutrons or radio waves as the interrogating radiation.

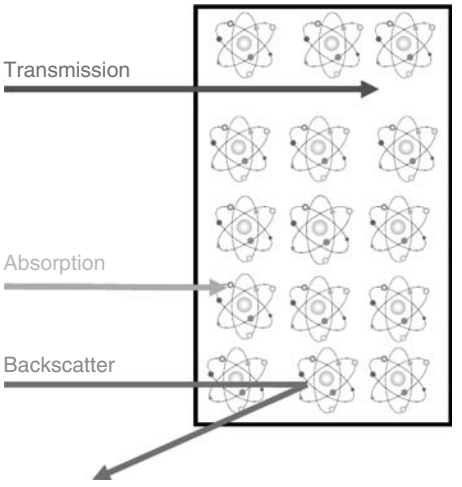



**FIGURE 6** Interaction of electromagnetic radiation with matter. Matter (composed of atoms and molecules) is represented by the rectangle. The top line shows transmission, where there is no interaction between the matter and radiation. The middle line shows absorption, where there is an interaction between the atoms (molecules) of the matter and the radiation. The amount of absorption varies with the wavelength of the original radiation. The bottom line shows backscatter where the radiation is no longer on its original trajectory.

Neutron technologies utilize thermal or high-energy neutrons to interrogate the material under investigation. The neutrons are absorbed by atoms in the material and the atoms with incorporated neutrons are energetically excited. The excited atoms release their excess energy by emitting $\gamma$ ray with characteristic energy. Neutrons and $\gamma$ rays are ionizing radiations and so care should be exercised with this radiation hazard.

A radio frequency (RF) field is used to interrogate quadrupolar nuclei. The exposed quadrupolar nuclei are excited to a higher-energy state. Upon removal of the field, the nuclei relax back to their original lower-energy state along with the emission of radiation of characteristic energy. The energy depends on many factors, including the type of atom in the material. RF radiation is nonionizing radiation, but care should still be exercised not to unnecessarily expose humans.

Nuclear-based technologies can provide greater specificity and are more material specific for explosives than imaging technologies. To positively identify a material uniquely as an explosive, a chemical analysis technology such as mass spectrometry is required. All of the bulk detection technologies have strengths and weaknesses. If enough information is gathered on a suspect material, a determination of the presence of explosives may be made.

Although not all properties measured with a bulk technique are unique to explosives, they can indicate a high probability of the presence of explosives. The false alarm rate for bulk detection devices can be low enough in general to allow for automatic detection of explosives-like materials (e.g. in luggage screening). Alarm resolution is still an important issue when using bulk detection technologies.

### 5.12 Summary and Future Research Directions

Trace and bulk explosives detection techniques are complementary and have different strengths. The feasibility of having multiple pieces of purchased equipment on hand is usually constrained by equipment cost, throughput, and operational needs of a facility. Future equipment design should incorporate multisensor platforms to increase the detection functionality.

Until recently, low vapor pressure explosives, especially military explosive materials, have been the main materials of interest for explosives detection. The recent emergence of nontraditional explosive materials is challenging and the following are areas of recent interest:

- standoff explosives detection
- improvised explosive devices (IEDs)
- homemade explosives

## 6 RESEARCH AND FUNDING DATA

In December 2006, the US government still did not have a FY2007 budget in place and was operating in a continuing resolution mode. As the budget progressed through Congress, there was some fluctuation in the numbers.

The two largest agencies receiving explosives detection funding are the Department of Homeland Security (DHS) and the National Science Foundation (NSF). DHS earmarked $87 million for explosives countermeasures research, which is an increase over previous

years [1, 2]. The overall budget dollars for all DHS R&D activities is expected to drop approximately 10%. NSF's total budget is expected to grow about 8% from the previous year. A $20 million request was earmarked within NSF for fundamental research for new explosives sensor systems and technologies [3–5].

The European Union is spending approximately €15 million for security research projects. One of the new projects is for improving the detection of explosives, including liquids at airports [6].

The outlook for explosives detection funding in FY2008 looks promising. The Bush administration has placed emphasis on efforts that support standoff detection of conventional explosives [7].

## 7 CRITICAL NEEDS ANALYSIS AND RESEARCH DIRECTIONS

The recent emergence of nontraditional, homemade explosive materials has forced the broadening of the term *explosives threat*. The adversary is not constrained by politics or layers of bureaucracy and the explosives research community should not be either.

The explosives research community (which includes government, industry, and academia) needs to become more agile and nimble to meet this evolving threat by thinking outside of the box and streamlining proposals to minimize politics and bureaucratic red tape.

A knowledge-base center comprising researchers with broad, cohesive, diversified backgrounds needs to be set up to provide a network for the explosives research community. The network would have innovative ways to share information between collaborators. The enhanced communication would minimize the duplication of research efforts and pass along research dead ends. The network would allow the community to be more nimble and responsive when a new threat arrives.

## ACKNOWLEDGMENT

This technical article has been authored by a contractor of the US government. Accordingly, the US government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this article, or to allow others to do so, for US government's purposes. Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the US Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL8500.

## REFERENCES

1. American Association for the Advancement of Science *DHS R&D Falls in 2007 Budget*, http://www.aaas.org/spp/rd/dhs07p.htm, accessed November 2006.
2. Knezo, G. J. *Homeland Security Research and Development Funding, Organization, and Oversight*, CRS Report for Congress, Congressional Research Service, the Library of Congress, Order Code RS21270, accessed November 2006, http://www.fas.org/sgp/crs/homesec/RS21270.pdf.

3. Office of Science and Technology Policy, Executive Office of the President, Homeland Security *Research and Development in the President's 2007 Budget*, http://www.ostp.gov/html/budget/2007/1pger_HomelandSec.pdf, accessed November 2006.
4. Davey, M. E., Matthews, C. M., Moteff, J. D., Morgan, D., Schact, W. H., Smith, P. W., and Morrissey, W. A. *Federal Research and Funding: FY2007*, CRS Report for Congress, Congressional Research Service, the Library of Congress, Order Code RL33345, accessed November 2006. http://www.fas.org/sgp/crs/miisc/RL33345.pdf.
5. Ember, L. R., Janson, D. J., Hess, G., Hileman, B., Johhson, J., and Morrissey, S. (2007). R&D Budget Lacks Balance. *Chem. Eng. News* **84**(8), 27–32. February 20, 2006.
6. *Europa Press Releases, 15 Million Funding for Security Research to Combat Terrorism*, (2006). Reference: IP/06/1390 Date: 13/10/2006, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/06/1390&format=HTML&aged=0&language=EN&guiLanguage=en, accessed November 2006.
7. Marburger, J. H. III, and Portman, R. *Memorandum for the Heads of Executive Departments and Agencies*, http://www.ostp.gov/html/m06-17.pdf, accessed November 2006.

## FURTHER READING

Akhavan, J. (2004). *The Chemistry of Explosives*, Royal Society of Chemistry, Cambridge.

Theisen, L., Hannum, D. H., Murray, D. W., and Parmeter, J. E. *Survey of Commercially Available Explosives Detection Technologies and Equipment 2004*, National Institute of Justice, http://www.ncjrs.gov/pdffiles1/nij/grants/208861.pdf, accessed November 2006.

Yinon, J. (1999). *Forensic and Environmental Detection of Explosives*, John Wiley and Sons, Chichester.

# RADIOACTIVE MATERIALS SENSORS

R. M. MAYO[1]

*U.S. Department of Energy, National Nuclear Security Administration, Washington, D.C.*

D. L. STEPHENS[2]

*Pacific Northwest National Laboratory, Richland, Washington*

[1] Present Address: Johns Hopkins University Applied Physics Laboratory, Baltimore, Maryland
[2] Present Address: Battelle Boulevard, P.O. BOX 999, MSIN K8-34, Richland, Washington

## 1 INTRODUCTION

The likelihood of a radiological or nuclear (RN) attack on the United States or its allies is a subject of contemporary debate and concern [1, 2]. What is undeniable, however, is the potential consequence of such an incident, making the risk unacceptable to ignore. Means of preventing such events are many and diverse, and constitute much of the federal government's efforts in nuclear nonproliferation, counter-proliferation, and counter-terrorism. Such efforts include an array of activities like the establishment of treaties and agreements that limit the use of nuclear technologies and materials, and provide for enforcement measures like MPC&A (materials protection, control, and accountability) designed to secure nuclear materials in place at the point of origin or during transit. As well, safeguards are established by international agreement to secure nuclear facilities and processes against diversion of material [3]. Dismantlement of nuclear devices and facilities is also an integral part of establishing international nuclear security, as are capabilities to interdict stolen, diverted, or smuggled material in such programs as the Second Line of Defense (SLD) and Mega-Ports Initiative (MI) that monitor land border crossings and seaports, the Proliferation Security Initiative (PSI) that provides for interdiction at sea, and cargo and vehicle screening at US ports of entry. The discovery of undeclared material or devices triggers an incident response architecture with the end goal of material disposition or consequence management in the event of a detonation or dispersal.

The common thread in the aforementioned is an implied ability to sense or detect material as it is being diverted, smuggled, moved, or stored for an illicit purpose [4, 5]. All RN materials emit nuclear radiation, making radiation sensing among the most common and effective means of detecting, locating, identifying, and characterizing the form, function, and threat associated with RN materials. The consequent nuclear or radio-activity of these materials emits sub-atomic particles of radiation: alpha($\alpha$), beta($\beta$), gamma($\gamma$), and neutrons(n). Among these, the most important for the search and screening applications that will be the subject of this discussion are $\gamma$ and n as they are charge neutral and, hence, much more highly penetrating of intervening or shielding material. These particles are typically emitted by RN materials with energies in the range $\sim$0.06 to 10 MeV for $\gamma$s and $\sim$0 to 14 MeV for neutrons, and carry information in their energy content that is useful in identifying the source material. Indeed, the emission spectrum is characteristic of the parent isotope (decay) or interaction process (induced reactions), making spectroscopy a useful tool in identification.

Radiological threats might take the form of a radiological dispersal device (RDD) or a radiological exposure device (RED). In the former, a conventional explosive detonation, aerosolization, or other means of dispersement might be used to spread radioactive material, while in the latter a large quantity of material may simply be accumulated and placed in a common meeting location or other venue where people congregate or pass-by thereby exposing them to high doses of radiation. Common radioisotopes used in medicine and industry such as $^{60}$Co (1.17 and 1.33 MeV $\gamma$) or $^{137}$Cs (0.662 MeV $\gamma$) are among those considered likely to be misused in this way for their availability and relatively high specific activity. Nuclear threat materials, on the other hand, are much more weakly radioactive and, therefore, more difficult to detect with passive radiation instruments. Materials in this class include highly enriched uranium (HEU, comprising greater than 20% $^{235}$U) and weapons grade plutonium (WGPu, comprising $\sim$90% or greater $^{239}$Pu). These and other materials are classified as special nuclear materials (SNM) for their ability to sustain fission chain reactions and constitute the fuel for nuclear explosive

devices. SNMs, and especially HEU, have difficult detection problems by virtue of lower radiation emission rates per unit mass and weaker radiation energy. In addition, threat materials containing uranium are more difficult to distinguish from background and normally occurring radioactive materials (NORM) since uranium and its decay products (also radioactive) are naturally occurring in the environment. SNM is also an emitter of neutrons through the spontaneous fission decay branch, and many plutonium detection and assay techniques rely upon the detection of neutrons by the minor isotope $^{240}$Pu. As there are few natural sources of neutrons in the environment, sensing these particles is considered a strong indicator of threat, though not a definitive one. Spallation reactions in high Z materials induced by cosmic ray shower products also produce neutrons. This source needs careful characterization to distinguish from threat sources. In addition, HEU is a particularly weak emitter of neutrons. Passive detection is often not practical.

For much of what follows it will prove beneficial to consider two general classes of detection scenarios, search and screening, as a framework to guide discussion. Many of the nonproliferation, counter-proliferation, and counter-terrorism problems mentioned above take advantage of these operational schemes to conduct effective material control and interdiction operations. Screening includes procedures such as the establishment of radiation monitoring portals or other choke points at ports of entry, ports of departure, or facilities entrances. The objective is to survey persons, vehicles, and cargo for sources of radioactivity. Once radiation detection is confirmed, it is required to divert suspect conveyances to secondary inspection for identification or adjudication of the radiation alarm, so that both detection and identification equipment are required. In search, the scenario is quite different, especially in the early stages of the process in which a search team may be required to scan a limited region or building for threat sources of radiation. Proximity detection through gross counting detection and operational procedures, direction finding sensors, or imagers may prove useful to locate a source. Identification instruments employed as high confidence ID are almost always required.

In the following sections, we discuss the state-of-art and ongoing research and development for these and other radiation sensing technologies that have application to the above scenarios. A brief mention has already been made regarding the importance of spectroscopic (or energy information) especially in $\gamma$-ray sensing for threat identification. The next section elaborates on this substantially. This will be followed by a discussion of radiation imaging and its particular importance to the search mission. Interrogation of nuclear materials by active means (external stimulation of nuclear signatures by energetic particles of radiation) will be covered in a subsequent section followed by a discussion on advancement on detector materials. Finally, a discussion is provided on the integration of sensor component technologies into detection systems and associated electronics, before a brief closing discussion on Federal involvement and resources.

## 2 GAMMA RAY AND NEUTRON SENSING AND SPECTROSCOPY

The detection of $\gamma$ rays and neutrons is a mature field with significant and continuing innovation over the last several decades. Realizing the potential for nuclear/radiological terrorism, these detectors have received renewed interest in the first decade of the twentifirst century for their role in the detection of SNM and other radioactive threat materials. This renewed effort has focused on improving energy resolution, efficiency, and in some cases the mechanical properties of detectors. The national and homeland security

application of $\gamma$ and neutron detectors has focused on the detection of characteristic radiation that can uniquely identify threat materials from other benign radioactive material. This diverse set of missions employing $\gamma$ and neutron detectors results in a large variety of different sensor systems when optimized for the particular operational environments and applications. These may vary from the screening of material at a fixed point of entry, often called portal monitoring, to the search for materials where the detector is moving through an environment to find nuclear materials. There are many operational and technical differences between these two scenarios, yet the single factor that dominates detection sensitivity differences is the way radiation background is experienced in each scenario. In the case of a fixed system, the detector operates in a predictable background that typically varies slowly when compared with the frequency and duration of screened items. It can be carefully recorded and characterized, sometimes over long times, before the sensor witnesses a radioactive material event passage. In the search scenario, however, variations in background are often substantially larger in magnitude and of significantly increased frequency. When combined, these effects generally reduce the overall system sensitivity for a desired rate of false positive detection [6]. The false positive detection rate is of paramount importance to the discussion of operational practicality since the total cost of operating a sensor system is proportional to the total number of detections or alarms (including false alarms) that need to be resolved. For most real world situations, it is reasonable to expect that the number of real events where an SNM anomaly is encountered is diminishingly small, yet because of the relative abundance of NORM materials and other nuisance alarms, the number of false positives will dominate the operational cost in the deployed system. Research in radiation detection systems must be viewed in this context, placing a premium in high confidence performance. In an idealized system the false detection probability must approach zero while the detection of defined threats, especially SNM, must simultaneously approach unity. Advancing deployed detection systems toward this ideal operational condition is driving much of the current research and development for national and homeland security applications of radiation detection. Specific R&D focus areas resulting from this operational need include the improvements in unique identification, and in some cases quantification, of radioisotopes present. This can be accomplished by achieving better energy resolution, better timing resolution, and higher detection efficiency.

The detection of $\gamma$ rays and neutrons is possible because of their ability to produce ionization in materials. This *Ionizing Radiation* deposits energy in the detector material producing an electrical signal that can be recorded. Detector development, therefore, focuses on the optimization of detector materials and electrical signal readout technologies. For a more complete treatment on the fundamentals of radiation detection see Ref. [7].

There are two basic $\gamma$-ray detector classes common in national and homeland security applications, semiconductor and scintillation detectors. In semiconductor detectors electron–hole pairs are produced directly in incident $\gamma$-ray interactions with the detector material. These electrically charged particles are subsequently drifted to oppositely biased electrodes and collected. The highest performing among the semiconductor detectors is the high-purity germanium (HPGe) single crystal detector. Semiconductor detectors are capable of very good $\gamma$-ray energy resolution and have moderate efficiency. The HPGe detector, while unsurpassed in overall performance, has a significant operational drawback; it must be cooled to liquid nitrogen temperatures for effective operation. Initial cooling often requires many hours to days, and this low temperature must be

maintained during operation. In field situations, the logistics of providing the consumable liquid nitrogen can be operationally limiting or at least cumbersome. In the past decade there have been advances, including the introduction of mechanical coolers for these devices. To date, these systems are not capable of supporting large efficient crystals in person-portable devices with operational lifetime longer than a few hours. This has led to renewed interest in identifying new semiconductor materials for radiation detection that can optimally operate at room temperature. Additional information is provided in the section Radiation Detection Materials. A notable example of recent success in the search to replace HPGe with a room temperature material is the development of cadmium zinc telluride (CdZnTe, or CZT) detectors. These detectors have been the subject of much research over the past 15 years and are just now penetrating the market as radiation detectors for operational use. While this new detector material is capable of operating at room temperature, it has yet to demonstrate as high an energy resolution as HPGe and is only available in volumes of a few cubic centimeter, whereas HPGe is available in hundreds of cubic centimeter volume. Recent developmental progress, however, is continuing to push the performance of detectors based on this material so that energy resolution is now within a factor of three of HPGe and larger volume crystals are becoming available. In light of recent advancement CZT promises to be an important new detector material for national and homeland security applications because of its room temperature operation, low relative power draw, and relatively high energy resolution resulting in a potentially more practical isotope identification capability. The first ever high efficiency (∼20%), high resolution (∼1%) handheld detector with source directional indication based on an array of 18 pixilated CZT detectors is the "Gamma Tracker" system [8] shown in Figure 1.

The second class of $\gamma$-ray detector in common use in the national and homeland security arena is the scintillator detector. The scintillating materials in these detectors

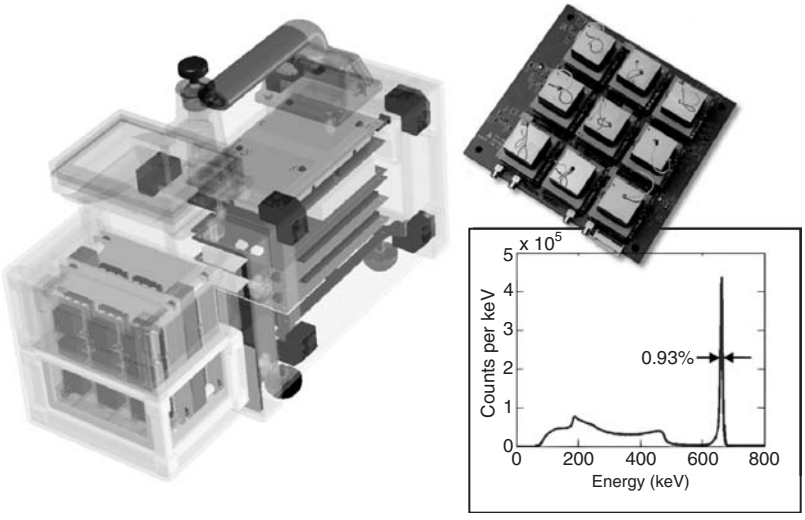



**FIGURE 1** Gamma-Tracker [8], a high efficiency, high resolution handheld radioisotope identifier with directional source indication based on 18 pixilated CZT detectors. Breakaway design drawing as well as insets of CZT detector array mounted on its front end electronics board, and a sample composite spectrum of $^{137}$Cs demonstrating ∼1% resolution at 662 keV are shown.

produce visible and near UV light photons through scintillation in an often complex cascade of events that result from the $\gamma$-ray ionization in the detector material. The most common medium energy resolution scintillator is the inorganic material thallium-doped sodium iodide (NaI(Tl)). This detector has been the mainstay of $\gamma$-ray detection and spectroscopy for laboratory and field measurement since its discovery in the 1940s. NaI(Tl) and its other doped variants have moderate energy resolution, high efficiency, operate at room temperature, and can be grown in volumes as large as thousands of cubic centimeters. Other notable scintillators utilized in security applications are the organic scintillators. There are many organic scintillator materials for $\gamma$-ray detection, but the most common for security applications is poly(vinyl toluene) (PVT) solidified in a polymer matrix. These so called *plastic* scintillators are widely used in large area detectors deployed for portal monitoring as they are relatively inexpensive and easy to manufacture on very large scales. They are of rather poor energy resolution, however, as a result of the predominance of Compton scattering events induced by incident $\gamma$ rays due to the low atomic number of PVT constituents. The energy resolution of these scintillators is not sufficient to uniquely identify specific radioisotopes in real world operations [9]. In these situations, the low energy resolving power may, at best, only be used to broadly classify radioactive sources as possibly containing threat materials.

Recent development progress has culminated in the commercialization of higher performing scintillation detectors such as those based on the inorganic crystal lanthanum tribromide ($LaBr_3$). They have detector characteristics similar to NaI(Tl) but with much better energy resolution [10]. An additional challenge unique to scintillators and one that continues to be the subject of vigorous investigation is the need to efficiently collect the visible or near-UV light produced by radiation energy deposition. This function is typically relegated to the Photo-Multiplier Tube (PMT), a vacuum tube devices that convert incident photons to an electrical signal. Improvements in the efficiency and robustness of PMTs, as well as improvements upon recently introduced photo-diode photon detectors will improve the overall performance of scintillator detectors.

In addition to detectors in the semiconductor and scintillator detector categories resides a class of calorimetric techniques that have recently achieved record [11] $\gamma$-ray energy spectroscopic performance. These detectors operate at superconducting transition temperatures (typically in the range of 0.1 K, below the liquid helium boiling point) and resolve $\gamma$-ray energy content by a very high precision temperature measurement of the heat deposited in a metal absorber utilizing a superconducting transition edge sensor (typically Cu/Mo). These bolometric techniques are achieving $\gamma$-ray energy resolution an order of magnitude better than the best HPGe. The most significant drawback is their inherently small size ($<1\,mm^3$) required to have effective thermal absorption and readout in reasonable time. This limits effective operation to low energy $\gamma$ rays and hard X rays ($<200$ keV), and for specialized long counting laboratory applications. Among the technical challenges being addressed in current R&D are increasing efficiency with multiplexed large arrays, ruggedization for potential field or mobile laboratory use, and applicability to $\alpha$ particle spectroscopy. Their ultimate application to homeland and national security missions is currently being evaluated.

In contrast to the atomic processes involved in the predominance of $\gamma$-ray interactions, indirect ionization of detector materials by neutrons results from nuclear scattering or absorption processes. These neutron-induced processes produce fast primary charged particles (usually protons, alpha particles, or other light ions) that then slow in the material and ultimately produce ionization. The net result is once again ionization of the detector

material. This allows similar detection techniques to be used as those described earlier for $\gamma$ rays albeit with different materials that have an affinity for neutrons.

Neutron detectors are typically divided into two distinct categories associated with the most likely interaction mechanism at a given range of incident neutron energy. In the low energy, or *thermal*, range (where neutrons are in ambient thermal equilibrium), detection usually requires nuclear absorption reactions. Absorption reaction based detectors contain materials with isotopes like $^{3}$He, $^{6}$Li, $^{10}$B, and $^{157}$Gd that have high neutron absorption probability. These reaction based neutron detectors preserve no neutron energy spectral information for incident thermal neutrons. In applications typical of national and homeland security, these detectors either operate as scintillators or semiconductors, having the same basic operation as described for $\gamma$ rays, or as gas ionization detectors. (The gas ionization detector operates by directly measuring the ionization products in the gas created by the neutron-induced reaction products.) The dominant thermal neutron detector in national and homeland security applications is the $^{3}$He gas ionization detector [7]. This detector is particularly favored for thermal neutron detection because it provides excellent discriminating ability between neutrons and $\gamma$ rays, being perhaps as much as $10^{5}$ times more sensitive to neutrons than to $\gamma$. In most operational situations, mixed fields of $\gamma$ rays and neutrons are encountered. Since confident detection of neutrons is often considered a stronger indicator of the presence of an SNM threat, it is important to have $\gamma$-ray discrimination as high as possible to avoid false positive detection.

Neutrons with energies typical of those emitted in nuclear decay, including fission in SNM, are initially of high neutron energy and are referred to as *fast neutrons*. Fast-neutron detectors can be built to exploit either nuclear absorption reactions or scattering. Common reaction based detectors for fast neutrons utilize absorption reactions in $^{3}$He or $^{6}$Li. The probability of these reactions occurring at fast-neutron energies is much lower than for thermal energies. Nevertheless, they have been exploited for fast-neutron detection. Fast-neutron detectors that exploit nuclear scattering, however, rely on the energetic recoil of the struck target nucleus to produce ionization in the detector medium. These detectors are commonly designed with high hydrogen content since the kinematics of the scattering collision favors energy transfer to a target proton [7]. These detectors are most usually scintillators and only measure the energy transferred in the elastic scattering collision. In general a fast neutron can undergo many such scattering events before it reaches thermal energy and is absorbed in a nuclear reaction. In practice, fast-neutron detection may also be accomplished by taking advantage of the energy loss from neutron scattering in hydrogen-rich materials (a process referred to as *moderation*) to reduce the energy of an incident fast neutron to thermal energies so that it can then be detected by a $^{3}$He based thermal neutron detector. This type of fast-neutron detector typically requires large masses of passive moderation material, typically polyethylene. In many operational settings, because of strict requirements on timing and/or additional energy content information, it is desirable to field direct fast-neutron detectors rather than those that moderate first before detecting.

Incident neutron energy spectrum of fast neutrons is, many times, an important quantity for national and homeland security applications since spectral details can reveal threat source characteristics and, perhaps, help distinguish among threat sources. Neutron spectroscopic techniques for thermal energy neutrons, on the other hand, are rather complex and not likely to provide additional information important in these applications. Spectroscopy for fast neutrons is typically achieved by a convolution technique whereby neutrons are moderated by varying amounts of hydrogenous material followed by detection

of the slowed neutron component, typically in a $^{3}$He or $^{6}$Li based detector. The relative populations of thermal neutrons in each moderation group allows the unfolding of a low energy resolution neutron spectra, devoid of fine spectral details yet representative of general spectral shapes that are often information rich. Fast-neutron spectroscopy may also be based on detector systems that record multiple scattering events in successive detector planes. Measuring event-wise energy deposition, interaction position, and time-of-flight between interactions allows for full kinematic reconstruction [12], as well as neutron source imaging as discussed in the section below. Detection challenges arising from inefficiencies in fast-neutron spectroscopy (since it requires multiple events or successive moderation) are somewhat mitigated in homeland and national security application by the very low neutron background rates. A notable exception is the increased neutron background found aboard large seagoing vessels produced by spallation interactions of cosmic rays with the large quantities of modest to high Z materials (especially iron) present. In these particular cases, neutron spectroscopic or temporal correlation information may provide a means to distinguish SNM threats from this background source.

Recent R&D in neutron detection has focused on identification of replacements for $^{3}$He gas ionization chambers, and the development of direct high energy neutron detectors. Gas ionization neutron detectors are not desirable for many operational scenarios. Alternatives such as intrinsic and convertor layer semiconductor neutron detectors [13] have been the focus of recent investigation. These alternatives, however, have thus far failed to achieve the same high detection efficiency and $\gamma$-ray discrimination of $^{3}$He detectors. Much of the current R&D for fast-neutron detectors is focused on the discovery and development of new organic scintillators [14] in either liquid or solid form, and in the development of faster and more sensitive neutron scatter spectrometer/cameras. The more in-depth exploitation of neutron correlated signatures from fission is a potentially productive area for further R&D as well.

## 3 RADIATION IMAGING

Radiation imaging is a technique that promises two potential benefits to homeland and national security missions. Imaging methods can reduce the contribution of background radiation to the observed signal, thereby raising the probability of detection by increasing the signal-to-noise (S/N) ratio in a narrow field of view, and by providing a visual image of the radiation source. Radiation imaging techniques have been and are continuing to be developed for both $\gamma$ rays and neutrons. For relatively low energy $\gamma$ rays, physical imagers are optimal. These imagers use physical optics to create images of $\gamma$ rays on position sensitive detectors and have been demonstrated [15] for stand-off detection of $\gamma$-emitting materials. The optics are made from high atomic number materials such as lead, and are ordered into patterns that occult a portion of the incident $\gamma$ flux, thereby producing a unique image at the detector plane. Techniques vary from the more complex coded aperture methods to the relatively simple pinhole camera. In practice, the exploitation of these techniques often results in massive detection systems because of the large amount of lead or other high Z shielding required, especially as the area of the detector increases in an effort to increase detection sensitivity. Systems of this type pose design challenges that trade detection efficiency for simplicity and portability. Pinhole cameras, being the simplest possible encoding, suffer the largest efficiency penalty of all physical

optics imagers since a sharp image requires a small aperture. On the other end of the scale, coded aperture data encoding allows the maximal quantity of photons to reach the active detector (up to 50% of the incident flux) at the expense of a more complicated image reconstruction process. Physical optics systems additionally suffer from reduced efficiency as $\gamma$-ray energy increases for fixed aperture thickness.

The Compton Imager, on the other hand, performs more efficiently at higher $\gamma$-ray energies. As the name implies, these systems exploit the Compton Scattering mechanism whereby partial energy loss from an incident $\gamma$ ray is measured in multiple detector volumes on successive scattering events. The technique does require multiple interactions in the detector, thus reducing the overall detection efficiently. However, much more imaging information is afforded per detected photon both because there is no coding (or aperture) penalty and because the sequence of scattering events from the same incident $\gamma$ ray provides nearly unique information regarding its incident direction. This technique has long been implemented in astrophysical imaging systems and is now beginning to be developed for national and homeland security applications in larger fixed, portable, and small handheld detectors [8] for direction finding in search and screening.

Neutron imaging techniques are functionally very similar to those applied in $\gamma$-ray imaging, though employing different detection materials as described above. In the case of thermal neutron imaging, physical methods such as coded aperture techniques work well. Materials with high thermal neutron absorption affinity (B, Li, Cd) usually comprise or are constituents of the aperture. In the case of high energy neutrons, scattering techniques analogous to Compton imaging are an area of current investigation and development. Figure 2 illustrates a recently developed instrument [12] for imaging fast neutrons ($\sim$1–10 MeV) referred to as a neutron double scatter camera. These techniques have recently demonstrated [12, 16] the additional capability to directly measure neutron energy spectra. The challenge with all imaging approaches is in justifying the penalty paid in loss of overall efficiency for encoding position information. Operational requirements must be carefully considered when selecting imaging techniques over other detection methods.

## 4 ACTIVE INTERROGATION

Although the passive detection technologies described above have proven quite effective in many situations and means of improving upon these continue through aggressive research and development campaigns, relying exclusively on passive means is likely to be ineffectual in some circumstances. Continually increasing requirements to detect ever smaller quantities of weakly emitting materials like HEU through material barriers and shielding raises detection and identification challenges beyond that practical of passive sensors. In these cases, only active stimulation of nuclear signatures can provide confident and timely detection, identification, and characterization.

Active interrogation refers to techniques that apply external sources of radiation, which induce reactions (usually nuclear) in SNM, thereby greatly improving detectability and/or reducing detection time. This improvement is possible because rates for induced reactions can be controlled through the intensity of the external source of radiation and are often many orders of magnitude greater than those of spontaneous decay. In this manner, active interrogation results in a greater rate of reaction product emission, a different variety of product particle, and/or unique energy spectral features of the reaction products, each of which can enhance our ability to detect.

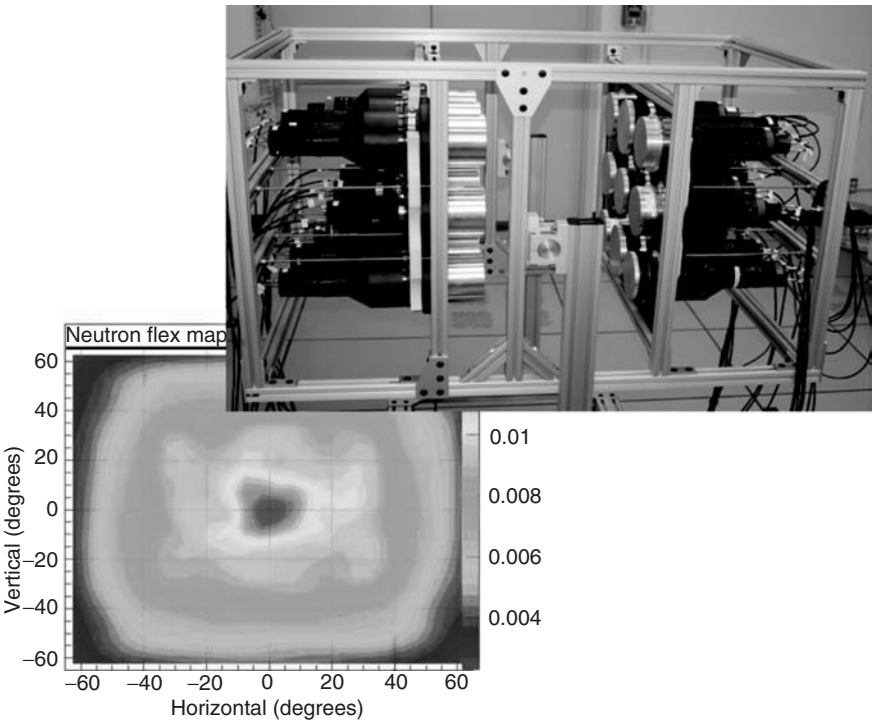



**FIGURE 2** Neutron scatter camera [12], a liquid scintillator based technique to witness fast-neutron scattering events in two successive interaction planes. Emission images and neutron energy spectra can be reconstructed from these data. The inset shows an image of a small $^{252}$Cf spontaneous fission neutron source imaged at $\sim$10 m through the steel hull of a sea vessel.

A wide variety of induced reactions is possible with fission, inelastic scattering, capture, and resonant absorption being the most prevalent. Only SNM fissions upon absorbing low energy neutrons, making thermal neutron-induced fission a unique signature. Unfortunately, low energy neutrons only weakly penetrate shielding material (especially low Z materials). Higher energy neutrons and $\gamma$ rays can be made to induce fission, however, with some loss of specificity since these particles (given sufficient energy) can eject neutrons from many other materials. Neutrons may also be captured or inelastically scattered by SNM resulting in the emission of characteristic $\gamma$ rays, though these reactions proceed at somewhat lower rates. Newly emerging on the active interrogation scene for SNM detection is resonant absorption and re-emission of characteristic $\gamma$ [17] referred to as *Nuclear Resonance Fluorescence* (NRF). Figure 3 depicts the experimental setup by which recent NRF signature measurements of HEU were recently conducted. This technique is in early stages of development and exploitation as a means of detection, yet shows great promise by virtue of the characteristic nature of emission and penetrability of energetic $\gamma$ in the range of 1–3 MeV for NRF in SNM [18]. Further exploitation of these and other signatures and detection modalities (like fission multiplicity and time correlation [19]) are ongoing subjects of investigation.

A wide array of sources is being developed to support active interrogation detection applications. Continual improvements and novel means are in high demand. Small accelerators, especially RF linacs, are the workhorses in most energetic photon interrogation

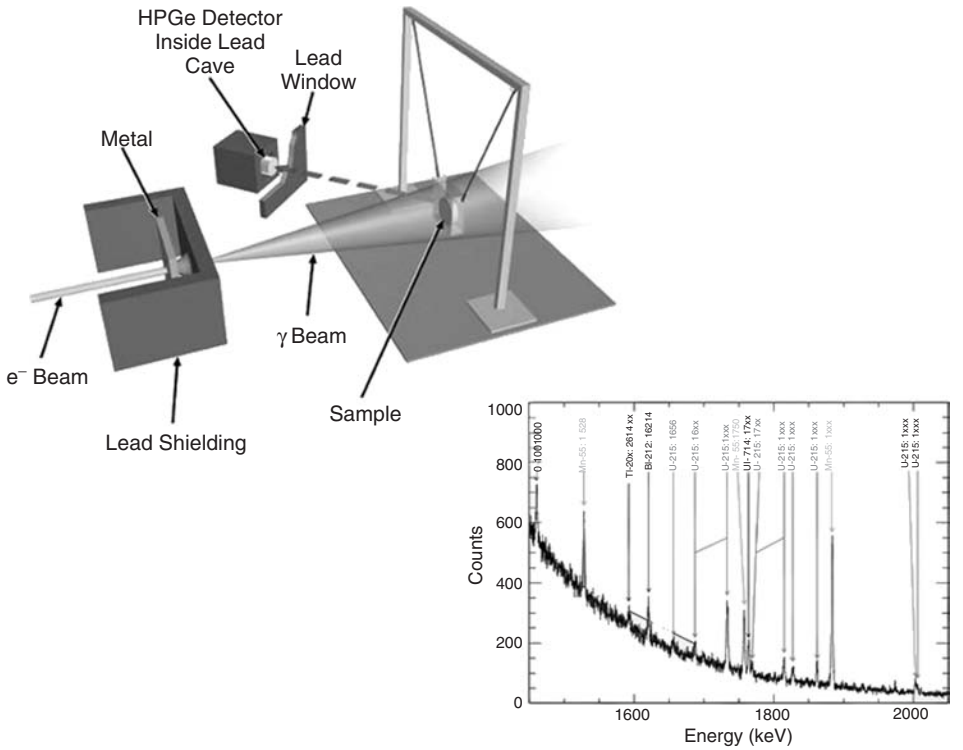



**FIGURE 3** Nuclear Resonance Fluorescence (NRF) [18] measurement setup. Inset $\gamma$ energy spectrum shows first ever direct measurements of $^{235}$U NRF lines in this region of interest (1450–2050 keV). Additional lines from background radiation and NRF in surrounding materials are also present.

schemes where accelerated electrons (usually to tens of MeV) are stopped on high Z targets to produce bremsstrahlung [20] radiation. Such sources are being pursued for both photo-fission and NRF interrogation. Bremsstrahlung beams, however, yield $\gamma$ energy distributions overwhelmingly dominated by low energy particles. Since the desired induced reactions require only those particles in the high energy tail, these sources produce much more radiation than necessary. This may result in more than necessary radiation exposure to operators and bystanders making these sources far from ideal. Narrow energy band sources are desired, which are either energy selectable or tunable for both photo-fission or NRF applications. $\gamma$ producing nuclear reaction based sources (e.g. p + $^{19}$F) and laser compton backscattering (LCB) sources [21] are being pursued. As compactness is a critical driver for many operations, laser wake field accelerators (LWFAs) are also being investigated as LCB drivers [22].

Fusion reaction (D–D or D–T) based high energy neutron sources are available commercially. Though some are compact, they suffer from lack of robustness and short lifetimes as well as modest output intensity. Addressing these issues, in addition to electronic collimation and high repetition rates and pulse shaping for pulsed sources, is the subject of substantial research investment [23]. Endoergic reaction based sources (e.g. p-Li) that produce moderate energy neutrons (~60 keV) are of interest for their modest penetrating ability while distinctly different in energy from the resultant fission neutrons

from SNM [24]. A portion of the development community is pursuing more exotic charged particle sources (especially protons and muons) for very long stand-off applications (up to kilometers). While practical applications may be far off, further development of source technologies and more complete understanding of beam particle interactions in air and target materials will surely advance state-of-the-art in active interrogation. Finally, detector development especially for the harsh environment, fast timing requirements, and particle discrimination requirements imposed by active interrogation applications is yet another very active investment area.

## 5 RADIATION DETECTION MATERIALS

Detecting particles of nuclear radiation relies on sensing the interaction of those particles with the material media of the detector. Since nuclear radiation is ionizing (either directly or indirectly), charged pairs are produced in such interactions and can be either drifted and directly collected in semiconductor detectors, or migrate to activator sites and produce scintillation light which can then be detected by a photo-detector (PMT or photo-diode) in scintillator detectors. Examples of both semiconductor and scintillator type detectors can be found in the solid, liquid, or gaseous states, though the bulk of contemporary research and development is focused on solid state detectors. Transportation regulation accommodation, avoidance of toxic and volatile material forms, and maximizing radiation stopping power are all strong motivators driving the technology in this direction.

Recent motivation to increase National and Homeland Security detection capability is beginning to provide impetus through more aggressive funding support for new radiation detection materials discovery, a research area that has been investment starved for decades [25]. Materials with long detection legacy like NaI (scintillator) and HPGe (semiconductor) continue to bear the brunt of the detection workload. Although well characterized and carefully outfitted for operational requirements, each has severe shortcomings. NaI is hydroscopic requiring enclosure and is sensitive to temperature fluctuations requiring gain control, but of more concern is its only modest ability to distinguish among radiation particles of differing energy, having resolving ability in the range of 6–10% (full width at half maximum in the photopeak). Although adequate for some purposes, for others this is insufficient discriminating ability. The search for better performing scintillator materials is ongoing. Recent progress on emerging materials like $LaBr_3$ [10] has been encouraging, though this material is not without its own peculiar problems especially fracture during growth. Still more recently $SrI_2$ and several candidates in the Elpasolite class have emerged as promising new scintillators.

Semiconductor materials are generally performing better with respect to energy resolution (HPGe resolution can be as low as ~0.25%) though these materials are not without their own shortcomings. HPGe, for example, must be cooled to liquid nitrogen temperatures before such performance can be realized, a serious maintenance burden for field operations. Candidate replacement materials have shown neither the performance nor the ability to be fabricated into detectors of comparable sizes. By far the most promising replacement for HPGe is CZT. Though not in widespread use, yet and still requiring additional improvement [26], promising new results from CZT are emerging. Less than 1% resolution at room temperature is consistently reported (Figure 1) with results as low as 0.7% not uncommon. Improvements continue and 0.5% resolution is expected imminently as a more thorough and mechanistic understanding of materials properties

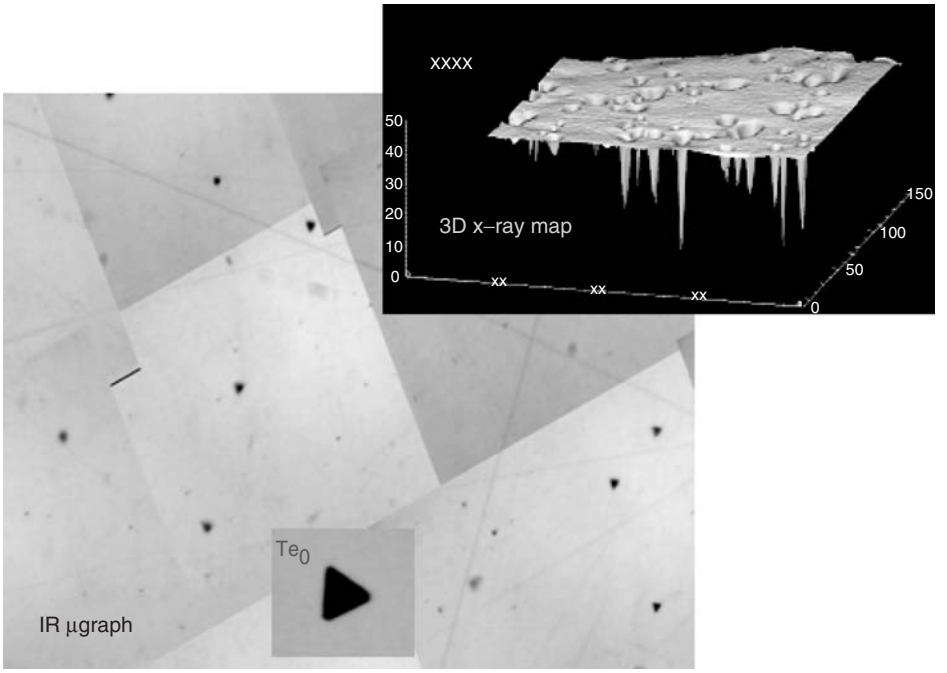



**FIGURE 4** IR transmission micrograph of a CZT single crystal showing presence of Te secondary phases. These material defects are well correlated with charge trapping as demonstrated by X-ray excitation from a 10 $\mu$m diameter beam line at the National Synchrotron Light Source (inset).

and charge transport develops. Figure 4 depicts recent microscopic examination in CZT where the appearance of Te secondary phases (as seen in IR micrograph) correlates well with reduction in charge collection as demonstrated by illumination with a 10 $\mu$m diameter X-ray beam line at the National Synchrotron Light Source (inset).

In addition to recent improvements made in the material properties, novel electronic readout provides a means to correct for material nonuniformities [27] so that better than intrinsic performance can be realized. The search for comparable or better performing materials that are easier and cheaper to grow in larger sizes continues. Recent indications suggest that nano-structured materials may hold promise as high performing detector materials or imbedded in a host matrix as scintillators or semiconductors [28].

There continues to be high demand for materials and structures to detect both fast and thermal neutrons. Lithium or boron doped (sometimes as nanoparticles) glasses and plastics are actively being pursued as efficient thermal neutron scintillator materials [29], while those materials either embedded or layered on Si devices are currently under investigation as thermal neutron semiconductors. The detection of fast neutrons is most often accomplished via liquid or plastic scintillators, with stilbene being considered the most effective for national and homeland security applications owing to the ability to readily distinguish among neutron and $\gamma$ interactions in the material. Having highly toxic starting materials, however, renders this material somewhat unattractive in providing a mass produced detection infrastructure. The search for new materials continues. Recently, salicylic acid derivatives have been investigated as promising replacements.

## 6 SYSTEM INTEGRATION

Radiation detection systems for homeland and national security require solutions that can meet the needs of the often harsh and complex operational environments. They must also be used effectively by a wide variety of users whose training and familiarity often varies considerably. The challenges associated with rapid transition of radiation detection technologies from the laboratory to these new venues requires the continued development and refinement of methods that result in high confidence operation. Areas of active research in automated isotope identification, low power computing, high efficiency cooling methods for detectors, improved mechanical properties of radiation detection materials, and imaging algorithms are a few specific examples. Algorithms for isotope identification in $\gamma$-ray spectra have been an area of particular emphasis in recent years. Expertise in $\gamma$ spectra analysis often requires years for even a highly technical individual to master, yet operational end users must rely on spectroscopic systems to routinely determine the composition of suspect items. The current state-of-the-art in this field necessarily focuses on both improved automated extraction of spectral features of interest and spectral deconvolution. Optimizing electronic components is yet another area of vigorous investigation and investment. As a general rule, the detection community attempts to utilize the latest in electronics technology by adapting it for use by custom integration. This is made apparent in the custom application of the latest communications hardware, custom ASICs, and field programmable gate arrays in radiation detection systems. On a final note, for deployed systems to be effective they must be optimized as systems rather than as stand-alone radiation sensors. Optimization necessarily includes test and evaluation specific to the ultimate system use, and the need for good systems engineering is sometimes overlooked in the push for better subsystem performance.

## 7 CLOSING REMARKS

In this short article we have described our understanding of the state-of-the-art in nuclear and radiological detection technologies. This is by no means a complete discussion, but should provide a reasonable introduction to the interested reader and new researcher. We have made every attempt to identify references that highlight contemporary work that has the most impact, from the leaders in their respective fields to provide a starting point for further investigation.

It was our further motivation to identify technical gaps or shortfalls wherever possible as a means of motivation. Many of these, including the development of new materials for higher performance radioisotope ID, compact intense sources for active interrogation with low unintended dose impact, and stand-off detection technologies rise to the level of *grand challenge*. For the eager researcher there is no shortage of opportunities to make significant impact to national and homeland security.

The technical disciplines described herein are rich and dynamic with many and diverse issues to be addressed. Indeed, RN detection technologies are interdisciplinary requiring expertise not only in radiation and detector physics, but also in microelectronics, shock and vibration isolation, thermal management, algorithms development, data reduction, and information management to name a few. The field has historically benefited from

related disciplines in nuclear and high energy physics, astrophysics, and weapons physics and is now leveraging clever solutions from the telecommunications, pharmaceutical, and biotechnology fields.

Support for research in all areas discussed in this article is provided across the federal government but development for security applications is concentrated within the Departments of Energy (DOE), Department of Defense (DoD), and Department of Homeland Security (DHS). The most directly relevant organizations within these departments are the Office of Nonproliferation Research and Development in the National Nuclear Security Administration of DOE, the Nuclear Technologies Directorate in the Defense Threat Reduction Agency of DoD, and the Transformational and Applied Research and Development Office in the Domestic Nuclear Detection Office of DHS. All three organizations support vigorous research and development programs conducting R&D in the national laboratories, universities, and industry.

## REFERENCES


1. Ferguson, C. and Potter, W. (2004). *The Four Faces of Nuclear Terrorism*, Center for Nonproliferation Studies, Monterey, CA.
2. Levi, M. (2007). *On Nuclear Terrorism*, Harvard University Press, Cambridge, MA.
3. Hecker, S. S. (2008). Preventing nuclear weapon proliferation as nuclear power expands. *MRS Bulletin* **33**, 340–342.
4. Byrd, R. C., Moss, J. M., Priedhorsky, W. C., Pura, C. A., Richter, G. W., Saeger, K. J., Scarlett, W. R., Scott, S. C., and Wagner, R. L. (2005). Nuclear detection to prevent or defeat clandestine nuclear attack. *IEEE Sensors J*. **5**(4), 593–609.
5. The Royal Society (2008). *Detecting Nuclear and Radiological Materials*, RS policy document 07/08. Available at http://royalsociety.org/displaypagedoc.asp?id=29187.
6. Stephens, D. L., Runkle, R. C., Carlson, D. K., Peurrung, A. J., Seifert, A., and Wyatt, C. (2005). Induced temporal signatures for point-source detection. *IEEE Trans. Nucl. Sci*. **52**(5), 1712–1715.
7. Knoll, G. F. (2000). *Radiation Detection and Measurements*, John Wiley & Sons, New York.
8. Myjak, M. J. and Seifert, C. E. (2008). Real-Time compton imaging for the GammaTracker handheld CdZnTe detector. *IEEE Trans. Nuc. Sci*. **55**(2), 769–777.
9. Ely, J., Kouzes, R. T., Schweppe, J. E., Siciliano, E. R., Strachan, D. M., and Weier, D. R. (2006). The use of energy windowing to discriminate SNM from NORM in radiation portal monitors. *Nucl. Instrum. Methods Phys. Res., Sect. A* **560**(2), 373–387.
10. Shah, K. S., Glodo, J., Klugerman, M., Moses, W. W., Derenzo, S. E., and Weber, M. J. (2003). $LaBr_3$:Ce scintillators for gamma-ray spectroscopy. *IEEE Trans. Nucl. Sci*. **50**(6), 2410–2413.
11. Horansky, R. D., Ullom, J. N., Beall, J. A., Doriese, W. B., Durican, W. D., Ferreira, L., Hilton, G. C., Irwin, K. D., Reintsema, C. D., Vale, L. R., Zink, B. L., Hoover, A., Rudy, C. R., Tournear, D. M., Vo, D. T., and Rabin, M. W. (2007). Superconducting absorbers for use in ultra-high resolution gamma-ray spectrometers based on low temperature microcalorimeter arrays. *Nucl. Instrum. Methods Phys. Res., Sect. A* **579**(1), 169–172.
12. Mascarenhas, N., Brennan, J., Krenz, K., Lund, J., Marleau, P., Rasmussen, J., Ryan, J., and Macri, J. (2006). Development of a neutron scatter camera for fission neutrons. *Nuclear Science Symposium Conference Record, 2006. IEEE*. 2006 Nov; San Diego, CA, 1, pp. 185–188.
13. Almaviva, S., Marinelli, M., Milani, E., Prestopino, G., Tucciarone, V. C., Verona-Rinati, G., Angelone, M., Lattanzi, D., Pillon, M., Montereali, R. M., and Vincenti, M. A. (2008).

Thermal and fast neutron detection in chemical vapor deposition single-crystal diamond detectors. *J. Appl. Phys*. **103**(5), 054501.

14. Budakovsky, S. V., Galunov, N. Z., Karavaeva, N. L., Kim, J. K., Kim, Y. K., Tarasenko, O. A., and Martynenko, E. V. (2007). New effective organic scintillators for fast neutron and short-range radiation detection. *IEEE Trans. Nucl. Sci*. **54**(6), 2734–2740.
15. Ziock, K. P., Collins, J. W., Fabris, L., Gallagher, S., Horn, B. K. P., Lanza, R. C., and Madden, N. W. (2006). Source-search sensitivity of a large-area, coded-aperture, gamma-ray imager. *IEEE Trans. Nucl. Sci*. **53**(3), 1614–1621.
16. Vanier, P. E., Forman, L., Dioszegi, I., Salwen, C., and Ghosh, V. J. (2007). Calibration and testing of a large-area fast-neutron directional detector. *Nuclear Science Symposium Conference Record, 2007. NSS '07. IEEE*. 2007 Nov; Honolulu, HI, 1, pp. 179–184.
17. Bertozzi, W., Korbly, S. E., Ledoux, R. J., and Park, W. (2007). Nuclear resonance fluorescence and effective Z determination applied to detection and imaging of special nuclear material, explosives, toxic substances and contraband. *Nucl. Instrum. Methods Phys. Res., Sect. B* **261**(1), 331–336.
18. Warren, G. A., Caggiano, J. A., Hensley, W. K., Lepel, E., Pratt, S., Bertozzi, W., Korbly, S. E., Ledoux, R. J., and Park, W. H. (2006). Nuclear Resonance Fluorescence of 235U. *IEEE Nuclear Science Symposium Conference Record*. 2006 Nov; San Diego, CA, 2(1), pp. 914–917.
19. Padovani, E., Clarke, S. D., and Pozzi, S. A. (2007). Feasibility of prompt correlated counting from photon interrogation of concealed nuclear materials. *Nucl. Instrum. Methods Phys. Res., Sect. A* **583**(2), 412–420.
20. Jones, J. L., Blackburn, B. W., Watson, S. M., Norman, D. R., and Hunt, A. W. (2007). High-energy photon interrogation for nonproliferation applications. *Nucl. Instrum. Methods Phys. Res., Sect. B* **261**(1), 326–330.
21. Hartemann, F. V., Brown, W. J., Gibson, D. J., Anderson, S. G., Tremaine, A. M., Springer, P. T., Wootton, A. J., Hartouni, E. P., and Barty, C. P. J. (2005). High-energy scaling of Compton scattering light sources. *Phys. Rev*. **8**(10), 100702.
22. Nakamura, K., Nagler, B., Toth, C., Geddes, C. G. R., Schroeder, C. B., Esarey, E., Leemans, W. P., Gonsalves, A. J., and Hooker, S. M. (2007). GeV electron beams from a centimeter-scale channel guided laser wakefield accelerator. *Phys. Plasmas* **14**(5), 056708.
23. Reijonen, J., Gicquel, F., Hahto, S. K., King, M., Lou, T. P., and Leung, K. N. (2005). D-D neutron generator development at LBNL. *Appl. Radiat. Isot*. **63**(5), 757–763.
24. Dietrich, D., Hagmann, C., Kerr, P., Nakae, L., Rowland, M., Snyderman, N., Stoeffl, W., and Hamm, R. (2005). A kinematically beamed, low energy pulsed neutron source for active interrogation. *Nucl. Instrum. Methods Phys. Res., Sect. B* **241**(1), 826–830.
25. Peurrung, A. J. (2008). Material science for nuclear detection. *Mater. Today* **11**(3), 50–54.
26. Bolotnikov, A. E., Camarda, G. S., Carini, G. A., Cui, Y., Li, L., and James, R. B. (2007). Cumulative effects of Te precipitates in CdZnTe radiation detectors. *Nucl. Instrum. Methods Phys. Res., Sect. A* **571**(3), 687–698.
27. He, Z., and Sturm, B. W. (2005). Characteristics of depth-sensing coplanar grid CdZnTe detectors. *Nucl. Instrum. Methods Phys. Res., Sect. A* **554**(1), 291–299.
28. McKigney, E. A., Del Sesto, R. E., Jacobsohn, L. G., Santi, P. A., Muenchausen, R. E., Ott, K. C., McCleskey, T. M., Bennett, B. L., Smith, J. F., and Cooke, D. W. (2007). Nanocomposite scintillators for radiation detection and nuclear spectroscopy. *Nucl. Instrum. Methods Phys. Res., Sect. A* **579**(1), 15–18.
29. Neal, J. S., Boatner, L. A., Spurrier, M., Szupryczynski, P., and Melcher, C. L. (2007). Cerium-doped mixed-alkali rare-earth double-phosphate scintillators for thermal neutron detection. *Nucl. Instrum. Methods Phys. Res., Sect. A* **579**(1), 19–22.

# KNOWLEDGE EXTRACTION FROM SURVEILLANCE SENSORS

RAMA CHELLAPPA, ASHOK VEERARAGHAVAN, AND ASWIN C. SANKARANARAYANAN
*Center for Automation Research and Department of Electrical and Computer Engineering, University of Maryland, College Park, Maryland*

## 1 INTRODUCTION

In the last decade, surveillance and monitoring has become critical for homeland security. With this increasing focus on surveillance of large public areas, a traditional human-centric surveillance system where a human operator watches a bank of cameras is largely being supported with automated surveillance suites. In a typical public area such as an airport or a train station there could be anywhere between 50 to a few hundred cameras deployed all over the area. It is almost impossible for human operators to keep a close watch on all of these cameras and continuously and robustly identify subjects and events of interest. Therefore, there is a greater need for automated analysis of the data obtained from multiple video cameras and other sensors that are distributed all around the area of interest.

Several current state-of-the-art surveillance systems work in aid of human operators. These surveillance systems have a host of sensors [visual, audio, infrared (IR) etc.] that are distributed in the area of interest. These sensors are in turn networked and connected to a central command center, where sophisticated algorithms for varied tasks such as person detection, tracking, and recognition; vehicle detection and classification; detection of restricted zone incursions, activity analysis; anomalous activity detection and so on, can be performed in real-time. One outcome of this automated analysis is to select a subset of the video cameras that are of interest so that these can then be monitored closely by human operators. This may significantly reduce the burden on the human operator. Moreover, when these sophisticated data mining techniques detect threats or anomalous behaviors they immediately alert the security personnel in the command center thereby reducing the time between an event and its detection.

We first discuss the various sensor modalities that are used in typical surveillance systems and discuss their advantages and disadvantages. We will then discuss in detail algorithmic paradigms for recovering important information from the data gathered by these sensors. Finally, we discuss the current challenges in fusion of information from a distributed web of sensors and discuss future trends.

## 2 SENSOR TYPES AND KNOWLEDGE EXTRACTION

There exist a wide range of sensors that find use in surveillance applications. These sensors are drawn from the families of line-of-sight and non-line-of-sight sensors. We

discuss them here in the order of increasing complexity of acquired data and the subsequent processing required for extracting the information of interest. In many cases, this correlates directly to the intrinsic capability of the sensor type.

### 2.1 Motion Sensors

Motion sensors register the presence/absence of humans in a small region by actively using laser to sense or passively noting the presence of IR to detect motion [1–3]. In this way, at each time instant, motion sensors report sparse information without much capability to characterize the identity of the target, and as a consequence disambiguate between multiple targets or the action performed by the target(s). However, a dense deployment of motion sensors along with sparse deployment of complementary sensors such as cameras can form a very powerful sensor suite. Motion sensors, typically consume much less power compared to a camera and it is easier to process the information that it generates. Further, it is possible to devise clever fusion strategies that allow for intelligent steering of cameras, so that the cameras' fields of view (FoVs) cover areas in which there is significant activity. Recently, deployments of such motion sensors have gained immense popularity. There are publicly available data sets which allow exploring such data [4].

### 2.2 Acoustic, Seismic, and Radar Sensors

Acoustic and seismic sensors detect pressure waves and record a profile of the time-varying strength of the wave. This information, especially its description in the time–frequency space encodes a rich description of target properties [5]. The amplitude of the signal is a function of the source power and the range of the source from the sensor. Fourier analysis of the sensed signal reveals the harmonic content of the source that could possibly be used for tracking and identification [6]. When an array of microphones is used, it is possible to estimate the direction of arrival (DoA) of the source [7]. The data collected using an array can then be used to compute a time delay between the signals received between a pair of microphones. This time delay is proportional to the difference of the distance between the source and the individual microphones. Given sufficient number of microphones (or equivalently, time-delays) it is possible to estimate a source location that could result in such time delay measurements. However, in the case of collocated microphone arrays, the narrow baseline only allows for the reliable estimation of the DoA of the source. Given multiple DoA estimates from different arrays, it is possible to estimate source location by triangulation. Acoustic microphones provide omnidirectional sensing at cheaper power costs, while losing the ability to robustly determine the identity of the target. Further, acoustic microphones do not scale well with the number of targets in a scene and have poorer sensing range than video cameras. Similar algorithms can be used for range-only tracking using radar sensors [8].

### 2.3 Visible and Infrared Imaging

Video sensors are among the most prominent sensors used for surveillance [9, 10]. Visual sensors allow for the estimation of target parameters such as its location in a world coordinate reference, its texture, motion, and specifics the nature of its interaction with

the scene and other targets. The information captured in the visual modality essentially allows for the extraction of significant amount of knowledge about the scene and events that occur in it. Further, the physics of image formation from the 3D world to the video provides constraints unique to the visual modality. These constraints are of immense use in well-conditioning of estimation algorithms that infer quantities of interest.

### 2.4 Multimodal Sensor Fusion

While video sensors provide a rich characterization of the scene, they suffer from a problems such as limited FoV, high operating costs in terms of power and computational complexity. In contrast, sensors such as motion detectors and acoustic microphones provide complementary capabilities that can be used in conjunction with visual sensors. As an example, motion sensors have been used to steer pan-tilt-zoom (PTZ) cameras to capture targets of interest [11]. This allows the PTZ cameras to be used only when there are targets in the scene and further, allows a large area to be sensed by the camera. In this sense, the two sensor types form a complementary pair that is useful for indoor surveillance. Acoustic microphone arrays provide similar support in the case of outdoor surveillance. Acoustic video fusion helps in providing omnidirectional sensing capabilities and providing robust tracking of objects even when one of the modality fails [12]. Similarly, acoustic-radar nodes provide position tracking for outdoor surveillance, wherein the DoA comes from the acoustic modality and the range information is provided by the radar [13].

## 3 SURVEILLANCE TASKS

A typical surveillance system must be capable of performing the following tasks—detection and tracking of humans and vehicles in the scene, person identification, vehicle classification, activity analysis, and anomalous activity detection.

### 3.1 Detection

The first and foremost task in typical surveillance systems is to detect objects of interest in the scene. Since these objects may have very different appearance characteristics it becomes extremely challenging to detect general objects. Hence, most surveillance systems resort to detection of moving objects. This is reasonable since in surveillance we are typically interested in humans and vehicles and their interaction with other humans and the environment. Motion-based object detection can be achieved both via passive sensors such as IR sensors or video cameras and via active sensors which are based on laser (similar to the ones used in elevator doors). Among these most surveillance systems use an intelligent mixture of passive IR sensors and video cameras [3, 4]. The advantage of using passive IR sensors is that they are very cheap to install, and they can therefore be densely distributed over the surveillance area. Moreover, these sensors provide just 1 bit of information, indicating the presence or absence of a human within its sensing range. Therefore analysis and integration of the information provided by a distributed web of these sensors is a rather simple task. However, these sensors do not provide any information about the appearance and therefore, the identity of the targets. This identity information is extremely important for several surveillance tasks. Therefore, these

motion detection sensors are usually used in conjunction with several PTZ cameras. These cameras can take the initial target detection output of these sensors and then zoom into the targets of interest thus enabling high resolution capture of target appearance so that other tasks such as recognition, classification, and action analysis may be performed [11, 14].

***3.1.1 Detection via Video Cameras.*** Background subtraction [15, 16] is the simplest and the most common computational algorithm that is used in order to detect moving objects from videos. The basic idea behind background subtraction is that an observed image is identical to the background model at all pixels that are static while the pixels that correspond to the moving object affect the appearance of those pixels that are on these moving objects. The background model may itself be a single static template (indoor single static camera with known scene environment) or a dynamic model (e.g. mixture of Gaussian) whose parameters are updated with time. In typical surveillance scenarios, the background model is dynamic, changes with the changing illumination conditions in the scene, and is updated on-the-fly. At each frame the background model is subtracted from the acquired video frame and the difference image indicates the regions in the image where there are potential moving objects (see Figure 1). Simple analysis of these pixels such as connected component analysis is performed in order to reliably detect objects of interest in the video.

## 3.2 Tracking

Once the targets of interest have been detected, the next task at hand is to track each of these targets using the multiple cameras surveying the scene [18]. Most algorithms maintain an appearance model for the detected targets, and use this appearance model in conjunction with a motion model for the target to estimate the target position at each individual camera. Such tracking can be achieved using deterministic approaches that solve an optimization problem [19] or using stochastic approaches that estimate the posterior distribution of the target location using Kalman filters [20] or more commonly particle filters [21, 22].

***3.2.1 Appearance Model Based Monocular Tracking.*** At each individual camera, the detector outputs a set of pixels that correspond to a single moving object. Using some simple cues such as the size and shape of the set of detected pixels a bounding box enclosing the entire object is then drawn. The color/intensity values denoting the appearance of

**FIGURE 1** In surveillance, it is common to use object motion for detection. In this example, we have available a target free image (a) of the scene constructed using the algorithm described in [17]. Given an image containing moving objects (b), we can compare the two to obtain possible target locations (c). The target free image models a static world and in this instance, the motion of the target forms an important cue for detection.

the object within this bounding box is then used in order to build/update the appearance model of the object. The simplest possible tracking algorithm is to naively search for bounding boxes with similar appearance in the next frame of the video. But such an approach will fail in several scenarios such as occlusions, change in illumination and pose of the targets. In order to account for these slow changes in the appearance of the target, most tracking algorithms build an on-line dynamic appearance model. For example, in [22], an on-line color appearance model is built using a mixture of Gaussian for each pixel within the object. The parameters of this dynamic appearance model are then updated using the current tracked output. In the case of the mixture of Gaussian model, the model parameters are comprised of the mixture weights and the mean and variances of each Gaussian. Moreover, in most cases some information about the motion characteristics of the object is also typically available. For example, in several surveillance scenarios, for tracking humans and vehicles it is reasonable to assume a simple constant velocity motion model. Both the motion model and the appearance model are used together in order to formulate a filtering problem in which the video sequence forms the observations. Traditional filtering methods such as a Kalman filter or more recent Monte Carlo methods such as a particle filter [21] are then used to recursively estimate the location and the appearance of the target in each subsequent frame of the video. Particle filtering [23] is an estimation technique that relies on approximating the posterior probability density (of the filtering problem) with a set of particles/samples and propagating these samples to recursively estimate the posterior density function. In particular, particle filtering techniques find applicability for a wide range of computer applications given the inherent nonlinearity in their formulations.

***3.2.2 Multicamera Tracking.*** In the case of multicamera networks, another important issue to address is the association of targets across camera views. In the case of cameras with overlapping fields of view, the geometric relationship between the fields of view of the cameras along with the appearance information of the targets may be used in order to perform target association across views [24] (see Figure 2). For cameras that have

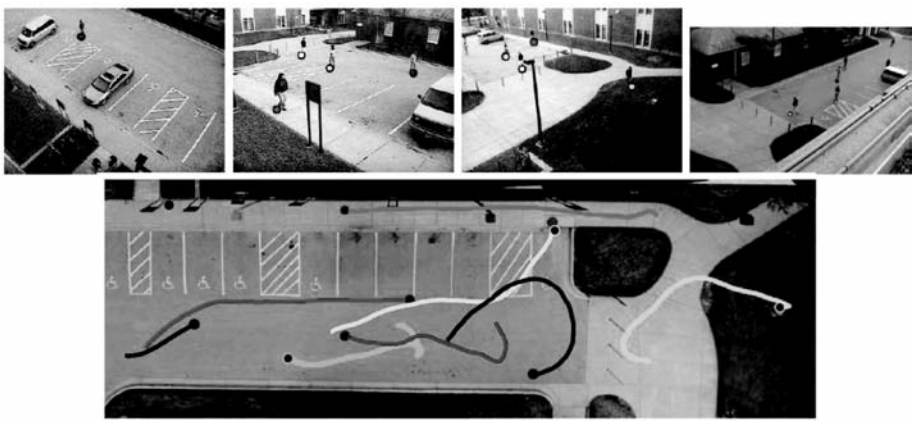


**FIGURE 2** Inputs form six cameras are used to track object locations on the ground plane using the algorithm described in [24]. (Top row) Shown are target locations on the respective image plane in four different cameras. (Bottom row) The collection of tracks overlaid on a top view of the world is also shown. Tracking using multiview data is robust to occlusions and low signal to noise rations (SNR).

nonoverlapping fields of view, target association must be achieved using either a 3D site model or by learning the relationship between patterns of entry and exit in the various camera views [25]. In several restricted surveillance scenarios, 3D site models may be available along with the location and the orientation of the cameras. If such 3D site models are available, then they can be used along with the camera parameters in order to reliably and accurately associate targets across camera views. We refer the interested reader to a recent survey of multicamera-based algorithms for details pertaining to target detection, tracking, and classification using multiple cameras [26].

### 3.3 Recognition and Classification

Having detected and tracked targets the next task is to recognize the objects that we have tracked. The simplest method for identifying human subjects is to use appearance models for the face and perform image and video-based face recognition. In far-field surveillance scenarios where the number of pixels on the target's face may be very small, other cues such as gait, which is related to the manner of walking may be used in order to identify people. In the simplest such scenario, this recognition may be performed using just the shape or the silhouettes of the objects being tracked. This will ensure that the target classification is robust to variations in lighting, color, clothing and so on, that will affect the color image significantly more than the binary silhouette. In calibrated multicamera settings, one may also fuse the 2D appearance models obtained at individual camera views in order to obtain a 3D texture mapped model and then perform recognition using these 3D models.

***3.3.1 2D Appearance Models for Recognition.*** For the sake of simplicity, let us assume that the objects of interest are faces, though the approach can be extended to generic objects. A simple 2D appearance template is first extracted and stored. This template is usually an image of the person's face under uniform illumination conditions. In [27], a particle filter is used to simultaneously estimate both the position of the target's face and the identity of the individual being tracked. The 2D appearance of the individual is modeled as a mixture of Gaussian and the parameters of the mixture density are estimated from the images in the gallery. The top row of Figure 3 shows the stored 2D appearance templates for the individuals in the gallery. In the bottom row are two images from a test sequence with the bounding box showing the location of the target's face. The image within the bounding box is matched with the stored 2D appearance models in the gallery in order to perform classification. Such a completely 2D-based recognition scheme suffers from limitations when the 3D pose of the face varies significantly. In order to tackle the pose problem effectively, multiple cameras along with 3D face models need to be used.

***3.3.2 Silhouettes: Gait-based Person Identification.*** Gait is defined as the style or manner of walking. Studies in psychophysics suggest that people can identify familiar individuals using just their gait. This has led to a number of automated vision-based algorithms that use gait as biometric. Gait as a biometric is nonintrusive, does not require cooperation from the subjects, and performs reliably at moderate to large distances from the subjects. Typical algorithms for gait-based identification first perform background

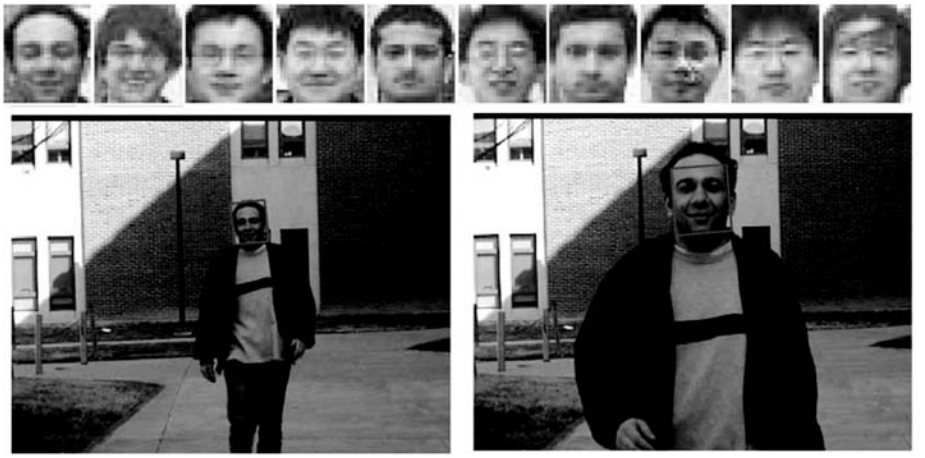


**FIGURE 3** (Top row) 2D appearance models for the individuals in the gallery. (Bottom Row) Two images from a video sequence in which a person is walking. The target's face is being tracked and the image within the bounding box of the tracked face is matched with the 2D appearance models in the gallery in order to perform recognition. (Image courtesy of [27]).

subtraction to obtain a binary image indicating the silhouette of the human. The first row in Figure 4 shows the tracked bounding box around the target in each frame of the video. Note that since the subject is moving, tracking needs to be performed before such a bounding box can be extracted. Background subtraction within the bounding box provides the binary image shown in the second row. The third row shows the shape of the extracted shape feature which is used in order to perform recognition. Note that the characteristics of the shape and identity of the individual and the subject's unique mannerisms during walking are captured in the sequence of shapes shown in the third row of Figure 4. Gait-based person identification differs from traditional biometrics in the sense that while traditional biometrics work on static features, gait as a biometric takes a sequence of deforming shapes in order to perform recognition. This means that dynamical models that capture both the shape and the kinematics of the feature need to be developed. Typical algorithms perform this shape sequence matching either using dynamic programming (dynamic time warping) or using state space methods (hidden Markov model (HMM)—[28, 29]) or by performing linear system identification (auto-regressive moving average (ARMA) model—[30]). In all these approaches the corresponding shape features or the model parameters for each of the subjects in the gallery is stored and is then used for comparison during the test/verification phase.

### 3.4 Event Analysis and Action Recognition

Event analysis in the context of surveillance systems can be broadly divided into those that model actions of single objects and those that handle multiobject interactions. In the case of single objects, we are interested in understanding the activity being performed by the objects. This is important in several scenarios so that vision-based surveillance systems may be able to understand and interpret the actions of humans within their field of view so

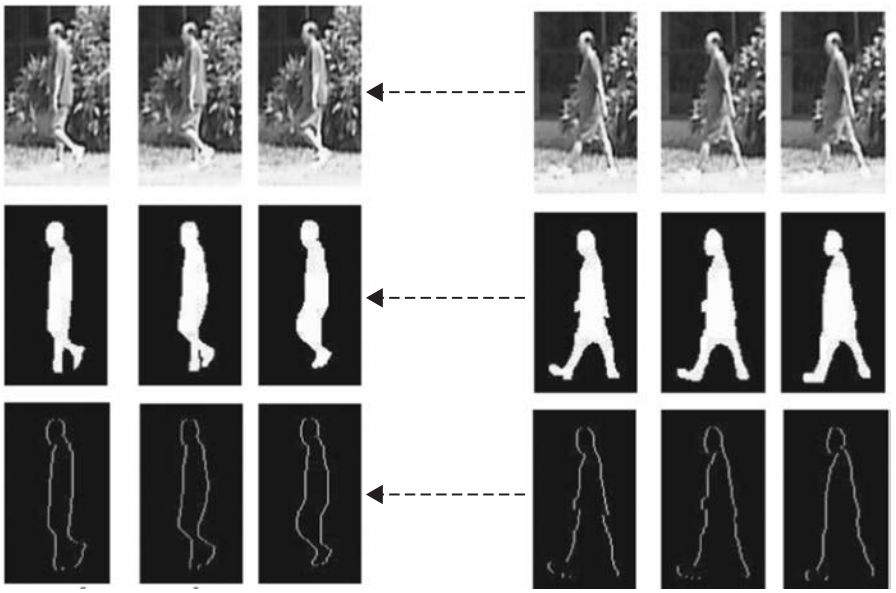


**FIGURE 4** (Top row) Image within the tracked bounding box as a subject is walking. (Middle row) Binary Background subtracted image sequence. (Bottom row) Extracted Shape Sequence containing the discriminative information for classification. (Image courtesy of [30]).

that they can effectively react to those actions. This kind of action recognition is usually performed in indoor surveillance when the number of pixels occupied by human subjects in the video is significantly large (of the order of $100 \times 100$ pixels). First, background subtraction is performed and a shape/silhouette feature vector [30] is computed. This shape representation is suitable to identify the activities while marginalizing nuisance parameters such as the identity of the object or view and illumination. Stochastic models such as HMMs [31] and linear dynamical systems [32] have been shown to be efficient in modeling activities. In these, the temporal dynamics of the activity are captured using state—space models, which form a generative model for the activity. Given a test activity, it is possible to evaluate the likelihood of the test sequence arising from the learnt model.

Modeling interactions between multiple objects are of immense importance in many outdoor and far-field surveillance scenarios. Consider a parking lot where we may be interested in interactions between humans and vehicles. Examples of such interactions include an individual exiting a building and driving a car, or an individual casing vehicles. Several other scenarios, such as abandoned vehicles and dropped objects also fit under this category. Such interactions can be modeled using context-free grammars [33, 34] (see Figure 5). Detection and tracking data are typically parsed by the rules describing the grammar and a likelihood of the particular sequence of tracking information conforming to the grammar is estimated. Other approaches rely on motion analysis of humans accompanying the abandoned objects.

In activity analysis, the challenges are in making algorithms robust to variations in pose, illumination, and identity. In this regard, the choice of feature vector chosen to describe objects is very important. Further, there is a need to bridge the gap between

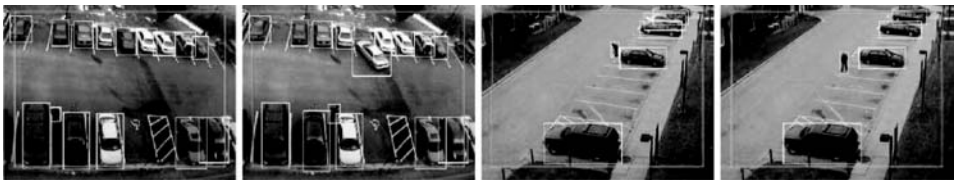


**FIGURE 5** Example frames from a detected casing incident in a parking lot [34]. The algorithm described in [34] was used to detect the casing incident.

the semantics of interactions described using grammars and the feature vectors used to identify individual actors and their activities.

## 4 CONCLUSIONS AND FUTURE WORK

In this article, we presented several issues related to the process of knowledge extraction from sensors for typical surveillance applications. Specifically, we discussed the relationship between sensor types and their sensing capabilities and stressed the importance of multimodal surveillance for practical systems. Further, we discussed the kind of information that is of typical interest to an end user and provided an overview of the algorithmic procedure that extracts such information.

There are several challenges and problems in information extraction from surveillance sensors especially in the context of distributed sensing and distributed computing. In particular, with the increasing use of unmanned air vehicles (UAVs) connected with static sensors using wireless networks, it is important to account for bandwidth and power constraints in the design. This is particularly important for robust information extraction as the connectivity of network depends on the lifetime of the individual nodes especially when inputs from multiple sensors are required. Therefore, a systematic and detailed study of both power and energy optimization versus algorithm performance is necessary. Recently, several research groups have started looking at this problem especially for visual sensor networks [35, 36].

Another key area of future research is in the visualization of the sensed information. The need to present surveillance information in a holistic framework to the end user is paramount in large scale sensor networks. With possibly hundreds of nodes, the correlations between events and information coming from the various parts of the network need to be presented in an intuitive way so that their semantics are easily perceived. We are currently building a test bed for novel visualization schemes in order to provide an end user the freedom in viewing the scene and the activities being performed from *arbitrary points of view*. The end user is presented with a virtual depiction of scene with synthetic virtual actors depicting the events of the scene. The information extraction using the sensors are used to locate, clothe, and for animating the actions of the virtual actors. One potential application of this technology is in scene monitoring where the security personnel can freely move around the scene without having to watch a fixed set of Closed Circuit Television (CCTV) screens (where the spatial coherence between views and the activities are lost). Further, this can be combined with

algorithms that alert the personnel when events of interest occur. Another area of potential use for such technology is in *privacy respecting* surveillance, wherein information that reveals the identity of the individual(s) is optionally suppressed by the visualization interface.

## REFERENCES


1. Aipperspach, R., Cohen, E., and Canny, J. (2006). Modeling human behavior from simple sensors in the home. *Lect. Notes Comput. Sc*. **3968**, 337.
2. Ivanov, Y. A., Wren, C. R., Sorokin, A., and Kaur, I. (2007). Visualizing the history of living spaces. *IEEE Transactions On Visualization and Computer Graphics* **13**(6) 1153–1160.
3. Wilson, D. H., and Atkeson, C. (2005). Simultaneous tracking and activity recognition (STAR) using many anonymous, binary sensors. In *The Third International Conference on Pervasive Computing*, Springer, Heidelberg, pp. 62–79.
4. Wren, C., Ivanov, Y., Leigh, D., and Westhues, J. (2007). *The MERL Motion Detector Dataset: 2007 Workshop on Massive Datasets*, Tech. Rep., Technical Report TR2007-069, Mitsubishi Electric Research Laboratories, Cambridge, MA. August.
5. Johnson, D. H., and Dudgeon, D. E. (1993). *Array Signal Processing*, Prentice-Hall, Englewood Cliffs, NJ.
6. Chen, V. C., and Ling, H. (2002). *Time-Frequency Transforms for Radar Imaging and Signal Analysis*, Artech House, Boston, MA.
7. Cevher, V., Velmurugan, R., and McClellan, J. H. (2006). Acoustic multi target tracking using direction-of-arrival batches. *IEEE Tran. Signal Processing*. **55**(6), 2810–2825.
8. Cevher, V., Velmurugan, R., and McClellan, J. H. (2006). A range-only multiple target particle filter tracker. *In Proc. IEEE Intl. Conf. Acoustics, Speech, and Signal Proc. ICASSP* **4** (14–19), IV.
9. Regazzoni, C. S., Fabri, G., and Vernazza, G. (1999). *Advanced Video-Based Surveillance Systems*, Kluwer Academic Publishers.
10. Remagnino, P., Jones, G. A., Paragios, N., and Regazzoni, C. S. (2001). *Video-Based Surveillance Systems: Computer Vision and Distributed Processing*, Kluwer Academic Publishers.
11. Wren, C. R., Erdem, U. M., and Azarbayejani, A. J. (2005). Automatic pan-tilt-zoom calibration in the presence of hybrid sensor networks. In *Proceedings of the Third ACM International Workshop on Video Surveillance & Sensor Networks*, ACM, New York, pp. 113–120.
12. Cevher, V., Sankaranarayanan, A. C., McClellan, J. H., and Chellappa, R. (2007). Target tracking using a joint acoustic video system. *IEEE Transactions on Multimedia* **9**(4), 715–727.
13. Cevher, V., Borkar, M., and McClellan, J. H. (2006). A joint radar-acoustic particle filter tracker with acoustic propagation delay compensation. *In Proc. 14th EUSIPCO*. Florence, Italy.
14. Hampapur, A., Brown, L., Cornell, J., Ekin, A., Haas, N., Lu, M., Merkl, H., Pankanti, S., and I. B. M. T. J. W. R. Center, Hawthorne, NY (2005). Smart video surveillance: exploring the concept of multiscale spatiotemporal tracking. *IEEE Signal Proc. Mag*. **22**(2), 38–51.
15. Piccardi, M. (2004). Background subtraction techniques: a review. *Systems, Man. and Cybernetics, IEEE International Conference on* **4**, 3099–3104.
16. Elgammal, A., Duraiswami, R., Harwood, D., and Davis, L. S. (2002). Background and foreground modeling using nonparametric kernel density estimation for visual surveillance. *P. IEEE* **90**(7), 1151–1163.

17. Joo, S., and Zheng, Q. (2005). A temporal variance-based moving target detector. *IEEE International Workshop on Performance Evaluation of Tracking and Surveillance (PETS)*. Breckenridge, Colorado, January.
18. Yilmaz, A., Javed, O., and Shah, M. (2006). Object tracking: a survey. *ACM Comput. Surv. (CSUR)* **38**(4).
19. Comaniciu, D., Ramesh, V., and Meer, P. (2000). Real-time tracking of non-rigid objects using mean-shift. *CVPR*, Hilton Head Island, South Carolina, **2**, 142–149.
20. Broida, T. J., Chandrashekhar, S., and Chellappa, R. (1990). Recursive techniques for the estimation of 3-d translation and rotation parameters from noisy image sequences. *IEEE Trans. Aerosp. Electron. Syst*. **AES 26**, 639–656.
21. Isard, M., and Blake, A. (1998). Icondensation: Unifying low-level and high-level tracking in a stochastic framework. *European Conference on Computer Vision* **1**, 767–781.
22. Zhou, S. K., Chellappa, R., and Moghaddam, B. (2004). Visual tracking and recognition using appearance-adaptive models in particle filters. *IEEE T. Image Process*. **11**, 1434–1456.
23. Doucet, A., de Freitas, N., and Gordon, N. (2001). An introduction to sequential Monte Carlo methods. *Sequential Monte Carlo Methods in Practice*, Springer, pp. 4–11.
24. Sankaranarayanan, A. C., and Chellappa, R. (2008). Optimal multi-view fusion of object locations. *IEEE Workshop on Motion and Video Computing (WMVC)*. Copper Mountain, CO, pp. 1–8.
25. Makris, D., Ellis, T., and Black, J. (2004). Bridging the gaps between cameras. *IEEE Conference on Computer Vision and Pattern Recognition*, Washington, DC, **2**, pp. 1–8.
26. Sankaranarayanan, A. C., Veeraraghavan, A., and Chellappa, R. (2008). Object detection, tracking and recognition using multiple smart cameras. *P. IEEE* **96**(10), 1606–1624.
27. Zhou, S., Krueger, V., and Chellappa, R. (2003). Probabilistic recognition of human faces from video. *Comput. Vis. Image Underst*. **91**, 214–245.
28. Kale, A., Rajagopalan, A. N., Sundaresan, A., Cuntoor, N., Roy Cowdhury, A., Krueger, V., and Chellappa, R. (2004). Identification of humans using gait. *IEEE T. Image Process*. **13**, 1163–1173.
29. Liu, Z., and Sarkar, S. (2006). Improved gait recognition by gait dynamics normalization. *IEEE Trans. Pattern Anal. Mach. Intell*. **28**, 863–876.
30. Veeraraghavan, A., Roy-Chowdhury, A. K., and Chellappa, R. (2005). Matching shape sequences in video with applications in human movement analysis. *IEEE Trans. Pattern Anal. Mach. Intell*. **27**, 1896–1909.
31. Rabiner, L. R. (1989). A tutorial on hidden Markov models and selected applications inspeech recognition. *P. IEEE* **77**(2), 257–286.
32. Turaga, P. K., Veeraraghavan, A., and Chellappa, R. (2007). From videos to verbs: mining videos for activities using a cascade of dynamical systems. *In IEEE Computer Vision and Pattern Recognition, 2007*. Minneapolis, MN, pp. 1–8.
33. Moore, D., and Essa, I. (2001). Recognizing multitasked activities from video using stochastic context-free grammar. *Workshop on Models versus Exemplars in Computer Vision*. Kauai, HI.
34. Joo, S. W., and Chellappa, R. (2006). Recognition of multi-object events using attribute grammars. *IEEE International Conference on Image Processing*. Atlanta, GA, pp. 2897–2900.
35. Shen, C., Plishker, W., Bhattacharyya, S. S., and Goldsman, N. (2007). An energy-driven design methodology for distributing dsp applications across wireless sensor networks. *IEEE Real-Time Systems Symposium*. Tucson, Arizona, December.
36. Schlessman, J., and Wolf, W. (2004). Leakage power considerations for processor array-based vision systems. *Workshop on Synthesis And System Integration of Mixed Information Technologies*. Kanazawa, Japan.

# RADAR AND LiDAR PERIMETER PROTECTION SENSORS

FRANK W. GRIFFIN

*Sandia National Laboratories, NWS DoD Program Design & Implementation, Albuquerque, New Mexico*

RICK HURLEY

*Sandia National Laboratories, RF and Optics Microsystem Applications, Albuquerque, New Mexico*

DAN KELLER

*Sandia National Laboratories, Strategic Business Enterprise Services, Albuquerque, New Mexico*

## 1 INTRODUCTION

With the goal of improving the adversary interdiction time line, ground-based radar and light detection and ranging (LiDAR) technologies offer options for intrusion detection and situational awareness, beyond facility perimeters. However, failure to understand and address the variables that affect successful employment of these technologies can result in costly installation of an inappropriate technology for the given security application. Far too often, security system designers work backwards by allowing advertised performance or cost to determine technology selection rather than the objectives and requirements of the security application.

Sandia National Laboratories (SNL) conducts evaluations of extended detection technologies for US government customers and their specific applications. On the basis of this experience, the authors assert that installation mistakes can be avoided using an approach that first assesses and defines the objectives of the application (what the application must detect, where, and for what reason), and then matches an appropriate technology to meet these objectives. This process is not always linear and may require an iterative approach.

The unique operating environment (terrain, weather, etc.) also plays a key role in appropriate technology selection. Other variables include system-specific capabilities and limitations, user-defined settings, and how a given technology is installed and employed.

## 2 TECHNOLOGY OVERVIEW

The following is an advanced discussion of radar and LiDAR operational methods and design variables. Each technology's operational methods have inherent strengths and limitations, and some systems employ or combine more than one operational method.

For information regarding specific systems, the reader is encouraged to contact product vendors. Reference herein to any specific commercial product, process, or service by

trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by SNL, Lockheed Martin, the US government, any agency thereof, or any of their contractors or subcontractors.

### 2.1 Light Detection and Ranging Technology (LiDAR)

LiDAR systems are active infrared technologies that use the near infrared (NIR) portion of the electromagnetic spectrum (750–3000 nm) for transmission of energy to illuminate targets. For target identification and tracking, target position and velocity changes are noted between each scan of the area against the known background. Because of the short wavelength of NIR energy, these systems are very sensitive to detecting small scene changes; however, increased sensitivity also tends to produce a relatively high nuisance alarm rate (NAR) from alarms attributed to animals and other nuisance alarm sources (a high NAR, which is the number of nuisance alarms averaged over a specified time period, may lead to operator overload and decrease confidence in the effectiveness of the system). Issues with these systems include laser safety concerns, short detection ranges for available systems (150–250 m maximum), and performance limitations in poor visibility or foggy conditions.

### 2.2 Radar Technology

Tactically deployable radar systems have been in use since the 1970s, and were originally designed to allow an operator to "listen" for troop or vehicle movement within an area of interest [1, 2]. Depending on the radar's horizontal and vertical beam width and the distance to the target, a large area several kilometers away may be monitored. Operating in the X-band (8.5–10.68 GHz) or Ku-band (12–18 GHz), these systems use a pulse repetition rate of several kilohertz. The frequency shift of return signals due to the Doppler effect is analyzed for target detection and identification [3]. These systems were not originally designed to operate continuously from a permanent position, but only as needed for the given tactical situation. Today, interest in using these systems for static security applications has gained momentum due to technology advances.

***2.2.1 Pulsed-Doppler Scanning Radar.*** For basic pulsed-Doppler radar systems, target range is calculated from the time it takes an emitted signal pulse to travel from the radar emitter, bounce off the target, and then return to the system. A Doppler shift occurs when a transmitted carrier frequency bounces off a moving target. This shift is a measure of relative radial velocity and direction, and is used to distinguish a moving target from stationary objects [3]. For early ground-based radars, this information was presented as audible signal changes, and system effectiveness was dependent on the skill and training of the operator.

Today, many pulsed-Doppler systems employ a graphical user interface to display target information and use lower power or pulse compression (less power over a longer pulse duration), improved processing and filtering techniques, variations of modulation methods, and various antenna configurations to improve performance.

The primary advantage of a pulsed-Doppler system is the ability to identify and isolate target movement in an area with relatively high energy returns from background clutter. A disadvantage is that a high NAR is often generated by reflections from rainfall and vegetation moving in the wind, thus creating multiple signal returns (Fig. 1).

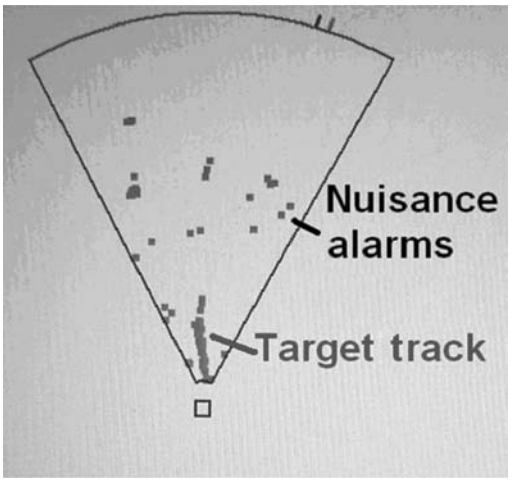



**FIGURE 1** Display from pulsed-Doppler radar: reflections from moving vegetation as nuisance alarms.

***2.2.2 Frequency Modulated Continuous Wave Scanning Radar.*** Advancements in computer processing speed, low cost techniques for generating linear frequency sweeps, and improved filtering have led to development of ground-based versions of frequency modulated continuous wave (FMCW) systems. Used for years by aircrafts, FMCW radars generally employ simultaneously operating transmitter and receiver antennas [3] and operate in the Ku or the Ka (27–40 GHz) frequency band.

There are significant differences between FMCW short-range and long-range systems. Long-range systems use Doppler discrimination to identify moving targets; short-range systems use high resolution range bin cell sizes (e.g. 0.5 m) and track target movement across multiple range bins to determine direction and velocity. By using higher resolution range bins, short-range systems use background clutter and an adaptive threshold to account for environmental changes occurring over time. This allows for filtering of energy received from stationary nuisance alarm sources.

***2.2.3 Moving Target Indication (MTI) versus Pulse Doppler.*** Moving target indication (MTI) radars are based on the same principles as pulsed-Doppler systems. The difference is that an MTI system typically operates with an ambiguous Doppler measurement and unambiguous range measurement. This means that the system has a blind speed where detection will not occur and does not address second-time-around echoes from far targets. Pulsed-Doppler systems have no blind speed, but do experience range ambiguities and limitations [3].

***2.2.4 Electronic Scanning or Phased Array Radar.*** For an electronic scanning or phased array radar, the system scans by electronically varying the electrical current phase across the antenna aperture [3]. These systems have scan area limitations. Depending on the system, scan angle is usually limited to less than $90^{\circ}$. This problem can be offset by using multiple antennas to cover large areas of interest. Electronic scanning offers a potential maintenance cost savings (no moving parts requiring periodic replacement), but emerging systems require additional design work to improve processing and scanning capabilities.

## 2.3 Design Variables

Modern radar and LiDAR systems vary considerably in design and operational characteristics. Variables include, but are not limited to, the number and size of range bin cells, horizontal and vertical beam width, and scan angle and rate.

***2.3.1 Range Bin Cells and Resolution Cell Size.*** All radars use range and angular range bins for processing. In pulsed-Doppler systems, these cells are used to integrate (average) multiple returns from a single target to minimize the effects of noise, improve the probability of detection, and reduce nuisance alarms [3]. For long-range pulsed-Doppler systems, these range bins can be 50–100 m in length, and the strongest signal can be processed to approximate the range from the radar to the target within that cell.

For FMCW radars, smaller resolution cell sizes offer higher fidelity for target detection, but reduce the maximum detection distance of the radar. In many cases, when vendors offer multiple ranges for FMCW radar, they are increasing the cell size to effectively double the range capability of the system. While this adds distance, it reduces radar sensitivity because the cell size is now larger and more energy is returned from the background within that cell (i.e. a higher clutter level).

***2.3.2 Horizontal and Vertical Beam Width.*** For radars, a narrow vertical beam width is desirable for a system that tracks targets several kilometers away (e.g. $3^\circ$ or less), but this limits effectiveness at ranges less than 1 km if there are undulations in the terrain. Generally, a larger vertical beam width will cover variations in terrain easier than a narrow beam width. The downside is that target location is generally reported as two-dimensional information (e.g. latitude and longitude), and target elevation information relative to the system is usually not provided.

Typically, the horizontal beam width determines the angular resolution and angular cell size of the radar. When a system averages returns from the environment to establish a background clutter level, the width of the angular cell size will have a significant impact on the amount of energy received from background clutter in that cell. For pulsed-Doppler systems, horizontal beam width also determines how many times an object will be interrogated during a single scan.

***2.3.3 Scan Angle, Scan Rate, and Processing Time.*** The scan angle, scan rate, and processing time required for a system to identify a target are important variables for system selection. Long-range systems typically have a longer scan rate than short-range systems. Problems arise if the selected system scan rate is slower than the time it would take a target to traverse the area the radar is expected to cover. For example, consider a system with a fixed scan angle of $360^\circ$, a 15-s scan rate, and a target acquisition parameter that requires three consecutive target interrogations, or "hits," before generating an alarm. For this system, processing time is greater than 45 s, and a fast-moving target (such as a vehicle) may travel a considerable distance before being detected.

***2.3.4 User Interface and Clutter Maps.*** Most modern systems employ clutter or background return maps presented through the user interface. Essential during system operation, clutter maps also allow the security engineer to easily identify areas of concern, as illustrated in Figure 2, which shows an area containing a known reflection source (a fence) as presented by two different radar systems' user interfaces. Using the clutter map as a reference, the security system engineer can make adjustments to the system or the installation configuration to mitigate application-specific concerns.

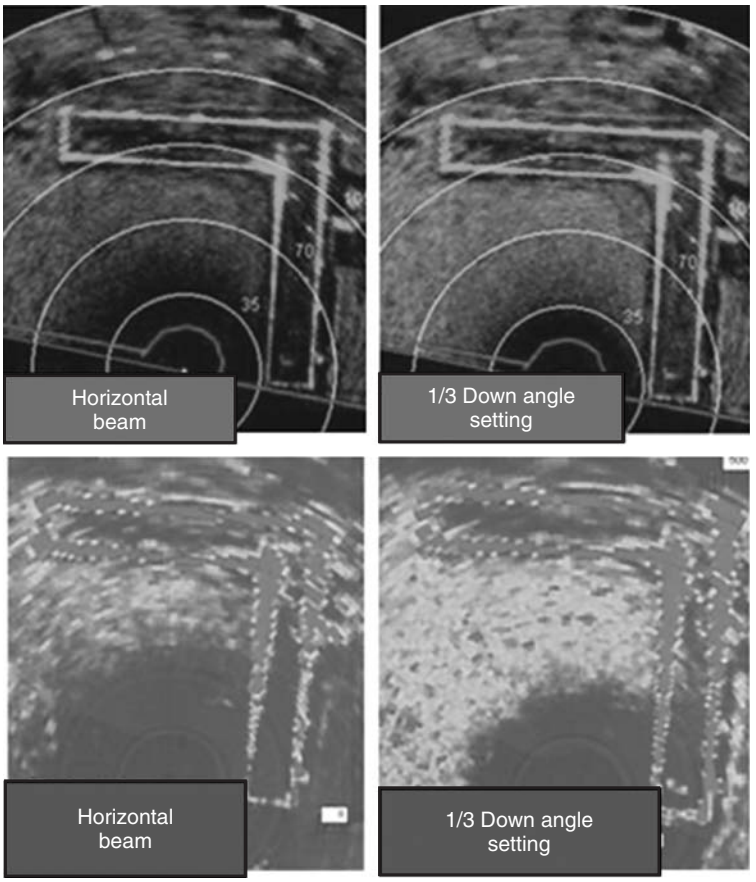



**FIGURE 2** Clutter map and increased clutter due to angle of incidence variation for two radar systems.

### 2.4 Operational and Performance Variables

When selecting a radar or LiDAR system, the security system designer should also understand and address technology and system-specific operational and performance variables.

***2.4.1 Clutter.*** Obstructions produce high clutter returns and reduce the operator's ability to distinguish target returns relative to the obstruction (Fig. 3). These returns are scene-dependant (i.e. dependant on the angle and geometry of the obstructions within the scene). Changing weather conditions, terrain undulations, and the presence of tall vegetation also cause clutter problems.

For short-range LiDAR systems (150–250 m), clutter sources are generally less of a problem than for radar systems because emitted (light) energy does not behave in the same way as radiated (radio frequency) energy, to background clutter. For LiDAR systems, the problem posed by a high clutter environment is shadowing from line-of-sight obstructions.

Redundancy (multiple radars overlapping the same area of observation) or use of other detection technologies may be needed within an application to mitigate high clutter concerns.

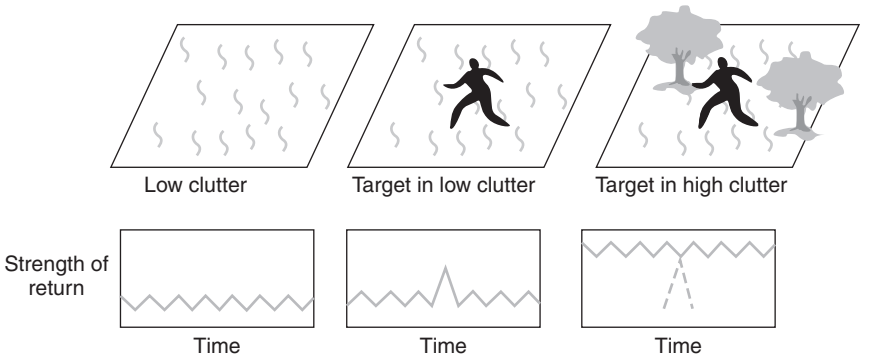



**FIGURE 3** Target in low and high clutter resolution cells.

***2.4.2 Dead Spot.*** Because of their operating characteristics and beam width, radar and LiDAR systems are surrounded by an area of no detection (a dead spot) that varies in range and area, dependent on the radar system. If installation height is increased, the area of the dead spot will also increase. The size of the dead spot can be reduced by adjusting the radar's angle of incidence; however, testing has shown that this reduces far-range performance and increases near-range returns, which may lead to receiver saturation (high clutter). Theoretically, LiDAR systems do not have the same saturation issue as radar systems, but this has not been verified through SNL testing.

***2.4.3 Environmental Effects.*** Rain, snow, and fog can increase clutter within a resolution cell and attenuate the transmitted signal at its operating frequency, diminishing effective radar range. The effects of precipitation are less significant for lower operational frequencies. However, most lower-frequency radars are pulsed-Doppler systems that have a greater sensitivity to nuisance alarms from rainfall, due to the movement and density of the rain. (Circular polarization of a pulsed-Doppler system has been advertised to help minimize returns received from rainfall, but this has not been verified by SNL). Figure 4 provides an example of target returns received during testing from a relatively light but fast-moving rainstorm.

LiDAR systems have issues relating to dispersion and reflection of light energy due to precipitation. Fog creates a diffuse reflectance and can be the source of nuisance alarms (Fig. 5).

FMCW systems that use adaptive threshold processing have been demonstrated to function without generating nuisance alarms in light and medium rainstorms (heavy downpour effects have not been evaluated by SNL), as illustrated in Figure 6 which shows an increase in background clutter but not in nuisance alarms. However, rain degrades the detection capability through a decrease in the maximum detection distance.

While many systems provide manual rain filters or can be configured to minimize rain effects, the security system designer should note that the more an operator is required to make system adjustments, the higher the chance that the system will be adjusted incorrectly or not be readjusted when conditions return to normal.

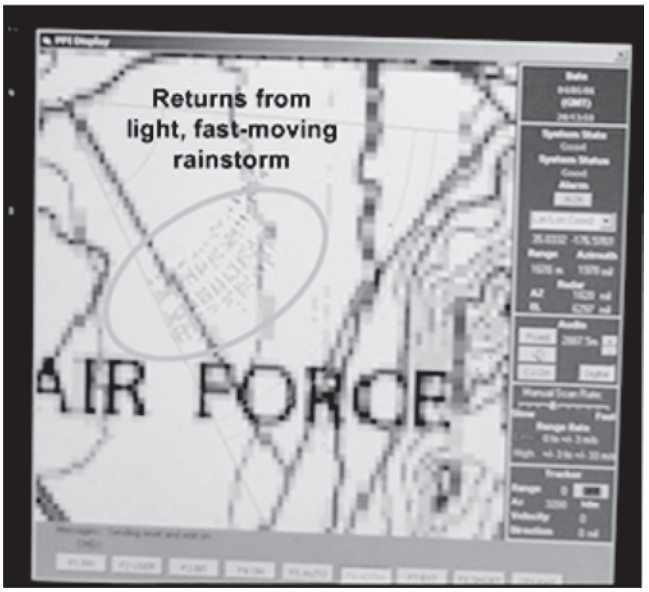



**FIGURE 4** Operator display (rainstorm) with pulsed-Doppler system.

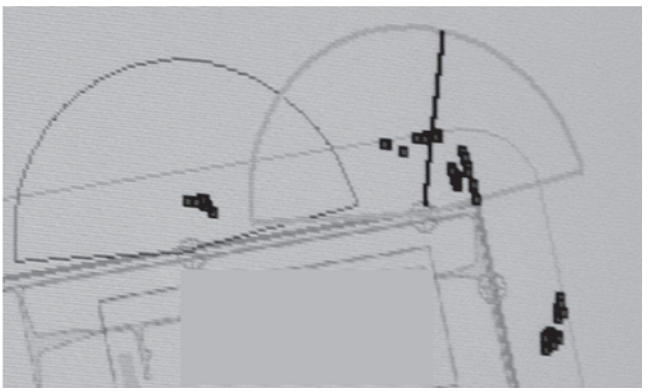


**FIGURE 5** Fog generated nuisance alarms for LiDAR system—example application.

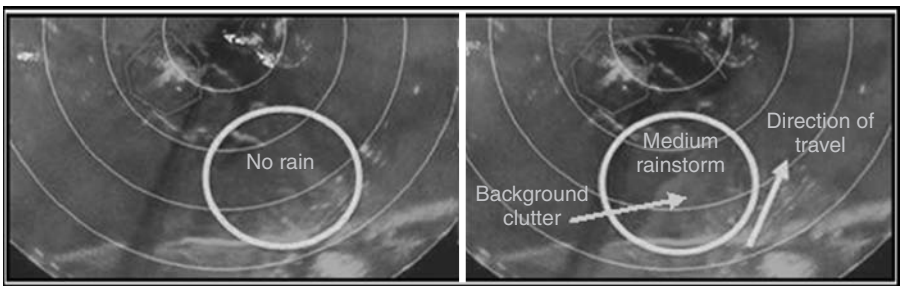



**FIGURE 6** Rainstorm affecting background clutter level for FMCW radar.

## 3 DEFINE AND CHARACTERIZE THE SECURITY APPLICATION

Radar and LiDAR technologies appear to offer a cost-effective alternative to the traditional perimeter security applications. In some circles, the concept of using these technologies to maintain a "virtual fence" has taken root. Because of the unique issues encountered by radar and LiDAR applications, the authors assert that these systems should be employed and characterized as situational awareness or extended detection *enhancements* to traditional perimeter security systems, not as a replacement.

Further, technology selection and installation considerations generally applied to most perimeter detection applications cannot be as easily applied to extended detection applications. What works well for one application (technology selection and installation configuration) may not work for another application with different objectives, environmental conditions, and operational use variables. To match the best technology to a given application, the security system designer must first characterize the application.

### 3.1 Application Objectives

At the highest level, the application objective consists of what is to be detected, where, and for what reason. For traditional perimeter security systems, the objective is usually to detect a target as it crosses a defined line of demarcation (perimeter), to provide alarm assessment (often using video cameras), and to delay the target long enough for an appropriate response [2]. Target intent is easily determined (e.g. someone climbing the perimeter fence is not supposed to be there).

Defining objectives for an extended detection application is more involved. There is not always a defined line of demarcation, and some targets detected within the area of interest may be authorized to be there, such as traffic on a roadway. Alarm assessment is more difficult at extended ranges (as is determining intent), and initiating a response beyond a perimeter may not be practical.

To define application objectives, the security system designer must first determine what target types represent the primary concern for the site (such as personnel on foot or fast-moving vehicles, etc.) to select the technology best suited to detect these target types for the given area of interest. Target types are generally identified through site-specific threat analyses and historical precedence.

### 3.2 Application Requirements

Application requirements define how the application must perform to achieve its objectives against the defined target set.

***3.2.1 Quantifying Performance.*** To quantify performance, security systems are evaluated using performance metrics to verify compliance with established performance requirements. Metrics include such performance thresholds as a minimum NAR and probability of detection, which is a measure of system effectiveness based on target sensing, assessment, and alarm communication probabilities. Because of differing system and environmental variables, radar and LiDAR systems will generally have a higher NAR and lower probability of detection than is acceptable for perimeter sensors, and the security system designer and system effectiveness analyst should understand that detection probability will decrease and the NAR may increase as detection range increases.

***3.2.2 Target Tracking and Target Intent.*** For long-range applications, it may be impractical to initiate an immediate response at the point of detection because target intent may be difficult to determine; therefore, accurately tracking target movement is as important as detecting the target. For example, a target moving rapidly toward a facility or line of demarcation may warrant a more heightened state of alert than a nonthreatening target passing through the area.

***3.2.3 Operational Mode.*** Does the application require the system to remain in continual operation, or will it be turned on only as needed for enhanced situational awareness? Systems operating continually will likely require more frequent maintenance and repair than those operated less frequently, so a system's mean time between failure (MTBF) rate, operational mode, and the availability and cost of spare components should be factored into its selection. For example, electronic scanning systems have fewer movable parts, which may translate into lower maintenance costs for these systems.

***3.2.4 Area of Interest and Range.*** Radar and LiDAR systems are line-of-sight technologies that work best for applications relatively clear of objects and terrain undulations that create areas of shadowing within the area of interest. The authors recommend characterizing the potential area of interest using three-dimensional terrain modeling to identify these areas of concern. This assists with determining system placement location for maximum coverage. Other measures may include raising the installation height of the system, deploying more than one system, or employing additional sensor technologies.

The security system designer should not simply accept the advertised maximum range of a technology to define the range of the application. Generally, the farther the range, the more difficult it is to assess the target due to distance and more line-of-sight obstructions. Effective range may also decrease for some systems during inclement weather. For short-range applications, it is also a mistake to assume that a system designed to detect at longer ranges will exhibit the same performance at shorter ranges.

## 4 TECHNOLOGY SELECTION

### 4.1 Systems Approach and Additional Deployment Considerations

For technology selection, the security system designer, using a systems approach, must address deployment considerations and adopt methods for dealing with alarm assessment issues, the effects of excessive numbers of actual and nuisance alarms, and must implement an effective Concept of Operations plan. The selected product must also be appropriately installed to take full advantage of its positive strengths while minimizing the negative effects of its limitations.

***4.1.1 Installation Height and Antenna Tilt Angle.*** Radar installation height and antenna tilt angle are key factors affecting the signal-to-clutter ratio. Background energy (clutter) increases with a system's angle of incidence. Increasing installation height reduces shadowing effects from obstructions; however, increased height decreases sensing and tracking performance since the clutter return is higher due to an increased angle of incidence with the environment.

Radar and LiDAR systems should be mounted as low as possible, dependent on intervening obstructions within the application. Figure 2 illustrates the changes seen on

clutter maps caused by changing the angle of incidence. When energy returns from the ground are strong (dark areas), sensitivity is decreased for detecting new targets because there is already a significant amount of energy returning in those range and angular cells.

***4.1.2 Assessment of Alarms and Tracks.*** For the standard perimeter, fixed cameras provide assessment of both legitimate targets and nuisance alarm sources. In general, the operational environment for perimeter security systems is well maintained, is usually clear of line-of-sight obstructions, and is well illuminated at night [2].

The extended detection environment, however, is full of visual obstructions that may limit effective assessment of alarms, and may require assessment under low or no-light conditions. Distance is also an important factor, as the probability of (correct) assessment of alarms decreases as detection distance increases.

If visual assessment is a requirement, the desired effective range of a radar or LiDAR system should be matched to an equally effective assessment system. An ineffective assessment system may decrease or cancel out the interdiction time line advantage afforded by an effective detection system.

***4.1.3 Nuisance Alarms and Actual Alarms.*** Even if a system has been tested and the results indicate a low NAR, it is important to understand that those values will increase with each system added to the design, and as a function of desired detection range. The capability to detect targets at the maximum range of the system is not always the most effective use of radar and LiDAR technologies, particularly if monitoring a large area of interest becomes unmanageable due to a high NAR.

Most radar and LiDAR systems have the ability to mask off areas of noninterest. Masking features could be employed during periods of high traffic along known pathways. In this application, it is recommended to define a line of detection and designate routes for restricted passage of authorized personnel within the detection envelope. Without these measures, system effectiveness is decreased during peak traffic periods.

***4.1.4 Technology Integration.*** The security system designer must also address how the radar or LiDAR system will integrate with the existing site physical security system. Factors to consider are alarm message communications using eXtensible Markup Language (XML) protocols, visual assessment technologies (if used), and communications links.

In the authors' opinion, a site's perimeter security system alarm console should not be linked with radar/LiDAR operator interfaces as the radar/LiDAR operator may deal with nuisance alarms and actual alarms at a rate much higher than a perimeter security system operator. Combining the two functions may result in a reduction in effectiveness for the site's security system as a whole.

***4.1.5 Life Cycle Costs.*** These include initial installation, maintenance, and costs for repairs and replacement parts throughout the operational life of the system. Variables affecting costs include system MTBF (and time to repair), availability of spare parts, and how the system is employed (i.e. continual versus occasional operation). Not considering long-term costs can lead to long periods of down time due to unforeseen maintenance costs.

***4.1.6 Response—Concept of Operations.*** Concept of Operations for a realistic response is critical to the effectiveness of a radar or LiDAR application. There are several issues to be addressed, such as:

- definition of what situations to respond to and what level of response is appropriate for each situation;
- identification of a challenge line or challenge distance(s) from the facility;
- determination of a response location or range (i.e. where the target must be challenged).

## 4.2 System Selection

In general, when reviewing potential radar or LiDAR systems for a given application, it is important to consider the following:

- *Existing integration capabilities (XML protocols, assessment technologies, etc.).* Does the system integrate easily with the selected system platform and/or assessment system?
- *Range and angular resolution requirements.* At what range are you trying to detect a target and why—can the response force effectively use the information given for a target several kilometers away? How important is it to accurately know the target's location, and is it sufficient to accurately slue or position an integrated assessment system?
- *Scan angle limitations.* Is the system installed on a fence directly adjacent to the area of interest? (Installation may require a scan angle of $180^\circ$ or $270^\circ$.)
- *Scan rate limitations.* Is the system scanning at the correct speed to pick up its intended target in time to support timely response? (If a system is overlooking an area of interest from a distance of 1 km away, a slow scan speed may be acceptable for the smaller field of view relative to the system; however, a system with a shorter range may require 1 rps, for example.)
- *Processing delays, limitations, or strengths (system alarm criteria, level of filtering, tracking capabilities, etc.).* Do filtering techniques impede or slow down the alarm reporting time line? Does the system require a large number of operator adjustments?
- *Tested or advertised MTBF, cost of system, cost of maintenance.* All are equally important for calculating life cycle costs.
- *Down time associated with repairs and support.* Is the manufacturer or one of their subsidiaries located in your country? What effects will customs considerations have on emergency repairs, and how does this affect security?
- *System-specific limitations.* Can system limitations be compensated for by other security measures? All sensor technologies have inherent limitations that may be exploited, requiring other measures to compensate for these limitations.

## 4.3 Testing

One important point that should be adopted from this article is the need for on-site performance testing. For this, a concise but comprehensive test plan must be developed to address application-specific security compliance requirements. This test plan

should also include tests designed to identify and define technology strengths and limitations while operating within the unique operational environment. Testing should be designed to ensure the system is installed and calibrated to provide optimal performance.

Radar and LiDAR systems should also be tested during degraded environmental conditions to ensure adequate performance. Security system designers should not rely solely on advertised performance specifications provided by product vendors as these metrics are usually collected under "best-case" evaluation conditions.

## 5 TECHNOLOGY ADVANCEMENTS AND CURRENT ISSUES

With an increased interest in radar and LiDAR technology, increased funding is being allocated to improve and further develop these products. Below is a brief description of some recent improvements, as well as areas that still require attention.

### 5.1 Signal Processing Changes

Improvements in signal processing allow design engineers to further filter or process the information returned to the system. This is seen in tracking algorithms that take multiple target returns and look for target speed, direction, signal strength, and general characteristics to provide the operator with a single labeled track of a target as opposed to a group of individual dots on the user interface. By establishing target tracks, software developers can then create sensor fusion engines that process returns from multiple units to show a single target on a user interface. As more platforms begin to offer this capability, the focus may change to improved tracking using integrated assessment and surveillance video systems that will consider target elevation.

### 5.2 Elevation Tracking and Multipoint Calibration for Integrated Assessment Systems

Most ground-based radar and LiDAR systems only provide two-dimensional location data for targets detected within their vertical and horizontal beam pattern. Although these data are useful for sluing a camera system to the proper latitude/longitude coordinates, there is a need for collection and interpretation of elevation data for proper vertical orientation of the camera system. This becomes more apparent as the range from the radar to the target increases (few environments are perfectly level).

Inclusion of a three-dimensional mapping capability into the control software would improve tracking capabilities for integrated assessment systems. Another possible solution would be to allow the operator to create an initial multipoint calibration for the camera, allowing the camera to slue to fixed points at different elevations. The elevation values for camera travel would be linearly interpreted between elevation points. Thus, the more points included in the calibration, the more accurately the camera would follow the terrain, as illustrated in Figure 7.

### 5.3 Integration Issues and Needs

Radar systems for most installations within the United States deal with everyday high traffic areas and with segregating potential target movement from normal traffic (assessment

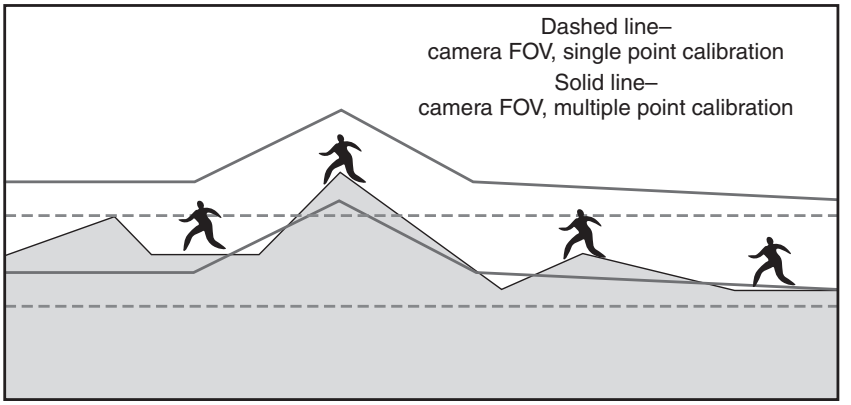



**FIGURE 7** Camera multiple point versus single point calibration.

and intent). The human operator may experience complacency over time, and a system that returns too many nuisance alarms for the operator to manage creates operator overload, degrading the effectiveness of the system.

Ideally, security system designers should work toward developing a nearly autonomous system that alerts the operator only when a "real target" is identified. This is a challenging task, and may introduce other security concerns with regards to vulnerabilities. Therefore, making the system more accurate and usable should be a primary design focus. When an alarm or target track is displayed for an operator, accurate assessment (i.e. camera tracking with sufficient imaging resolution) is a must.

### 5.4 Identification of Friends and Foes

For many applications, site personnel are authorized within an area of interest. Having a means to identify these individuals would assist system operators with distinguishing between authorized and unauthorized targets (friend or foe). What is needed is a means to identify authorized individuals directly on the radar or LiDAR user interface, and some effort has been made toward realizing this capability.

## 6 SUMMARY OF MAIN POINTS

In summary, the following are the main points security system designers should take from this overview:

- Failure to address radar or LiDAR system design, performance, operational, and installation variables can lead to costly installation of an inappropriate technology for a given security application.
- Successful employment of radar or LiDAR technologies first requires characterization of the security application in order to effectively match an appropriate technology to meet application objectives.
- Cost and advertised performance (e.g. advertised detection range) should not drive technology selection or define application objectives.

- Radar and LiDAR technologies should be employed as situational awareness or extended detection enhancements to traditional facility security systems, not as a replacement.
- On-site performance testing under all environmental conditions is crucial to ensuring optimal performance.

## REFERENCES

1. Tryniski, M. (2004). *AN/PPS-5D Radar Overview Presentation*. Syracuse Research Corporation, North Syracuse, NY.
2. Garcia, M. L. (2008). *The Design and Evaluation of Physical Protection Systems*, 2nd ed. Butterworth-Heinemann.
3. Skolnik, M. I. (1980). *Introduction to Radar Systems*. McGraw-Hill Book Company, New York, NY.

# DESIGN CONSIDERATIONS IN DEVELOPMENT AND APPLICATION OF CHEMICAL AND BIOLOGICAL AGENT DETECTORS

DONNA C. SHANDLE

*Nuclear, Chemical, and Biological Contamination Avoidance, Aberdeen Proving Ground, Maryland*

## 1 BACKGROUND

This study will address the differences and similarities in requirements that drive design features and product development of a handheld chemical vapor detector and a man-portable, vehicle-mounted standoff chemical detector for use by the uniformed services, and what changes or additional design/test work is required to ensure that the systems meet the needs of a Homeland Security application. It is apparent that the missions of the uniformed services likely differ in some respects from those of Homeland Security. However, the application of many systems developed for the services to that of Homeland Security involves minor, if any, adjustments resulting in significant capability for this governmental department. The issues to be answered relate to where and how the systems would be employed. Once these questions are addressed, immediate progress toward providing capability can occur.

### 1.1 How Requirements are Derived

It is worth noting that the Department of Defense follows a disciplined requirements development process coupled with standard systems engineering processes. From the definition of the customer's use concept, a developer derives performance specifications. Categories and related questions to be answered include, but are not limited to the following:

1. Intended users
   - Who will operate the system? This question drives human factors requirements such as size, weight, ease of maintenance, modular design, use of common parts, and location and size of any switches, knobs, buttons, or indicators on the system.
2. Operational environment
   - Under what climatic conditions will the system be used? Specifically, what are the temperature extremes for operation as well as for storage?
   - What are the relative humidity conditions in which the system must operate?
   - Must the system operate in rain, high wind conditions, and maritime atmospheres?
   - What are the intended environments for system operation? This question addresses interferents that may be naturally occurring or specific to an area of operation such as one where there is a heavy concentration of volatiles, for example. These environments affect the ability of the system to detect the target materials of interest. This question also addresses the safety aspects of the system and its operating conditions.
   - Will the system be used in a stationary or mobile scenario?
3. Operational use cases
   - What is the purpose of the detector in the mission? That is, what protection is the system required to provide?
   - What materials must the system detect, at what concentrations, and what is the required response time at each concentration? If the detector is used by personnel in protective clothing, the minimum level of detection may differ from that if the operator were wearing protective clothing/masks, for example.
4. Mandated integration/interfaces
   - With what other systems must this detector interface or communicate?
   - What other systems will be operating in close proximity to this detector?
5. Transport and storage
   - How will the system be transported to the area where it will be employed? This question is significant since it determines the maximum weight of the system as well as the means of carry/transport.
   - Will it be transported by vehicle, can it include a carrying case, what straps or attachments are needed, or is it carried by one or multiple persons?
6. Size/weight/power
   - What is the mission duration? This question establishes requirements that impact selection of power sources (battery or line), definition of scheduled maintenance

cycles, reliability, all logistics aspects such as types and locations of repair facilities, spare parts provisioning, and the need for specialized maintainer skills, as examples.

7. Cost
   - What is the target cost for the system on initial purchase?
   - What is the sustainment cost over the life cycle of the system?
   - What is the anticipated density for issue to users?

## 1.2 Comparison of Homeland Security—Specific Requirements to those of Uniformed Services

1. Intended user
   - The users of the systems for a Homeland Security mission are likely to have a higher level of technical knowledge/understanding regarding detectors.
   - The Homeland Security users could likely accommodate less-detailed training and premission operational trials.
2. Operational environment and use cases
   - That the mission of Homeland Security is within the continental United States reduces the extreme environments in which vapor detector systems must be stored and operated.
   - The lower detection limits are considered comparable for both missions. However, it is likely that the interferents in the environments may differ particularly if the Homeland Security mission extends into industrial settings where vapor atmospheres are prevalent, thus presenting a significant challenge to detect and differentiate between chemical warfare agents, toxic industrial compounds, and nonhazardous industrial compounds. This is specifically important if the materials of interest are in lower concentrations than the vapor interferents in the atmosphere.
   - Maintenance requirements for the Homeland Security scenarios differ in nature from the needs of the uniformed services and can be assumed to be more easily accommodated using local maintenance facilities vice having the systems repaired or maintained in the field by the operator of the detector.
3. Size/weight/power/integration/interfaces
   - Although the Homeland Security scenarios will entail outdoor, stand-alone missions, there is also the high likelihood that some mission scenarios will employ detector systems with sources other than battery power. For example, in an airport security scenario, detectors could easily be installed using house power, thereby eliminating a large logistics burden, which translates into cost avoidance per operating hour. Likewise, detector systems that are installed versus carried, lessen the concern for power since these can be hard-wired using commercial power in lieu of batteries that have a specific life.
   - The size requirements for both unformed services and Homeland Security are considered comparable, particularly for the counterterrorism missions where mobility and portability are of primary importance. For point detectors in

particular, small, lightweight, and easy to operate are essential characteristics for both customer bases.

4. Cost
   - The structure and facilities available to the Homeland Security teams also reduce the design features that provide for ruggedness and hardness in detector systems.
   - Owing to the complexity of some of the technologies in the current detectors, particularly passive infrared technology and the detection components within these systems, operator maintenance is not feasible; therefore a skilled maintenance facility is essential in the case of both the uniformed services and Homeland Security.

## 2 DESIGN CONSIDERATIONS

The design of a chemical vapor detector revolves around the technology employed that addresses the required performance. In the case of vapor detectors, the technology must address the characteristics of the chemical agent vapor that make them distinguishable from other nonthreat vapors in the atmosphere. The molecular structure of the materials of interest, the pattern of chemical bonds present in the substance, or unique spectra of the vapor are examples of characteristics that technologies can target. There are two mature technologies that have been incorporated into current chemical vapor detectors that each detect and identify agent vapors using different technologies, which impact the design considerations of each system. The first technology, ion mobility spectrometry, is utilized in vapor detectors classified for use as "point", since the detection is made within several inches to a foot of the agent, while passive infrared detection is incorporated in standoff detectors, for the purpose of enabling detection without exposure to the agent itself. Both of these technologies and systems are applicable to Homeland Security and counterterrorism missions.

### 2.1 Ion Mobility Spectrometry in Point Chemical Vapor Detectors

Ion mobility spectrometry technology is applied in agent vapor detectors to measure time of flight of ions of the materials of interest. The application of this technology requires that a vapor be ingested into the opening of the detector and pass through an ionizing process. The ions then drift down a tube owing to the force created by an applied voltage. The speed with which the ions travel are a fixed characteristic for each material at a given voltage. The arrival of the ions at the end of the drift tube creates a spectrum suitable for analysis through detection algorithms [1]. Detection of a material of interest is made when the result of the application of a set of algorithms to the spectrum of each material meets predetermined criteria. The technology lends itself to packaging into a small, lightweight, handheld device and boasts added benefits of low power consumption and minimal maintenance. Advances in the technology have successfully eliminated the radioactive ionizing source, thereby increasing the safety of the user and the maintainer, while reducing the environmental considerations upon disposal of the system at the end of its useful life. This improvement also reduces the ownership and accountability burden imposed by radioactive source licensure [2].

The incorporation of ion mobility spectrometry technology into a new detector has enabled the Department of Defense to generate test data that demonstrates detection

performance that meets system requirements for the Joint Chemical Agent Detector, a handheld, point detection system for use by the uniformed services [3]. As stated above, the advancement of the Joint Chemical Agent Detector over existing detection systems that employ ion mobility spectrometry is that it accomplished the ionization by a source other than a radioactive one. This favorable feature enhances the safety aspects of use, handling, and maintenance and impacts the design considerations as evidenced by the system's modularity, the reduced power allocation, and the overall cube of the final package [4]. The Department of Defense has also shown that this technology lends itself to detection of additional materials, such as toxic industrial chemicals, upon development of the appropriate algorithms and detection windows [5].

### 2.2 Passive Infrared Detection in Standoff Vapor Detection Systems

Development of a standoff detector for chemical agent vapor has effectively employed passive infrared technology to detect a vapor cloud at ranges of at least half a kilometer from the detector [6]. The application of this technology in a battlefield scenario assumes that the target material appears as a cloud with sufficient dimensions to create a change in the optical signature, due to a small temperature difference from the background, of the order of a few degrees, when viewed through the system optics after spectra were analyzed through the algorithm. Therefore, use of this technology incorporated a sophisticated optics package that presented design challenges such as packaging the scanner, its cooling system, maintaining module pressurization, and measuring signal-to-noise ratios. The output from the optics is a signal distinguishable from the background at sufficient amplitude to produce a spectrum that is then processed through algorithms to discriminate between a scene of nonagent-containing atmosphere and one that includes a cloud with the features of a threat agent. The packaging of the modules that contain the optics and associated coolers, elements for system orientation, and computer for signal processing must be optimized to meet system requirements of environmental conditions for on-the-move operations, weight, and power considerations. The determination of probability of detection at a given range is directly related to the optics of the system. The successful operation of the system depends on maximizing the opportunities for the detector to view the cloud of interest. More opportunities are a function of the size of the field of view and field of regard, which are optics design parameters. The relationship is that the smaller the field of regard, the higher the number of opportunities for the optics to view the cloud within a given time. Additionally, the smaller the instantaneous field of view, the greater the signal-to-noise ratio, which enables better resolution, and thus more accurate detections as well as enabling an increased range at which a cloud can be detected. An additional requirement for the Joint Service Lightweight Standoff Chemical Agent Detector was that the system detect in a $360^\circ$ arc across an elevation range of $-3$ to $+20^\circ$ while on the move [6]. Its predecessor, the M21 Remote Standoff Chemical Agent Alarm, provided standoff detection at seven distinct snapshots at the horizon across a $60^\circ$ arc from a stationary position. This additional requirement for on-the-move operations presented an algorithm challenge in that there needed to be a reference to the "before" scene in order to make the determination of the temperature differential due to the presence of an additional atmospheric feature. The requirement for on-the-move detection eliminated the use of the background subtraction algorithm that was employed in the M21 [7]. The development of an analytical technique for the spectra in light of the sizable data sets generated by the Joint Service Lightweight

Standoff Chemical Agent Detector was perhaps the biggest challenge for the developers. Improving detection sensitivity required trade-offs with false alarm rates; therefore, the algorithm designers conducted many iterations of algorithm adjustments to optimize the parameters that affected the probability of detection and false alarm rate.

### 2.3 General Design Considerations for Agent Detectors

Today's detection systems are more complex than the prior generation of detectors, but in spite of the increased complexity of current technologies, there is an even stronger requirement for a high degree of simplicity in the user interface. Thus, equipment designers tackle the challenge of presentation of comprehensible information on a small system display. The degree and detail of information, time available to act once information is received, and questions that must be answered by the information presented are all specific to the mission of the customer, whether it is Homeland Security or the uniformed services. Additionally, the level of user training and education impacts the grade level that the designer uses to ensure the user's total comprehension of the information. As an example, the requirements for the Joint Chemical Agent Detector are stated in terms of the product of concentration and time. Ion mobility spectrometry provides information regarding concentration of a given agent. However, a given concentration of a nerve agent produces a much different biological response than an equal concentration of a vesicant [8]. Thus, if the display were to show a response strictly based on concentration detected, the user would need knowledge of agent toxicity in order to understand the significance of the system display. To overcome this issue, the designer related the relative hazard of each agent to the detected concentration and displayed that data in terms of a bar response [4]. As the bar response incorporated agent-specific toxicity values in the algorithm, the display output was normalized, enabling the user to understand his/her level of danger no matter which agent was detected.

### 2.4 Design Trade-Off Process

Because users defining system requirements often ask for performance that exceeds the current state of the art, equipment designers conduct a trade-off analysis during the design and systems engineering phase of the effort. In that analysis, they document the capabilities of the technology based on work accomplished during the research phase of the effort. When a basic technology in research is proposed as a candidate to answer a requirement, the capability of the candidate technology is often reduced when applied in a nonlaboratory environment. The engineering work that continues during the development of the technology into a usable piece of hardware considers the hardness, ruggedness, human interface, and environmental conditions in which the system must operate. The incorporation of these factors into the development results in the necessity for trade-off studies to prioritize the requirements, assign a risk of meeting required levels of performance, and perform an optimization study that presents an estimate of the best performance that the system could achieve [9]. The use of a science-based system model provides an effective, cost-saving tool to exercise critical system parameters during the optimization process.

As an example, the physical characteristics of the optics incorporated in standoff detection systems influenced the range and probability of detection of the Joint Service Lightweight Standoff Chemical Agent Detector. The users desired maximum probability of detection and range of detection with minimum false alarms. There were at least

two parameters that were nonnegotiable in the early prototype systems, these being the window material and the field of view dimensions. These were fixed based on the required area of interrogation (originally 360°s horizontally and −10 to +50° vertically) and the time to detect. The designer traded off the probability of detection at a given range to maintain an acceptable false alarm rate. The design parameters that impacted detection performance pertained to the optics characteristics—field of regard and instantaneous field of view—since these directly resulted in the signal-to-noise ratio that was processed into spectra for analysis and time to detect. Additional tradeoffs were made in resolution of the wave numbers as well as in the algorithms. The analysis of test data from field trials enabled the designers to estimate and then optimize the relationship of field of view, field of regard, and signal-to-noise ratios on the range and detection probability of the system to simulant clouds [10]. The analysis also identified the impact on increase in false alarm rates should the algorithms be altered [10].

### 2.5 Application of Existing Chemical Vapor Detectors to Homeland Security Mission

To provide flexibility to the user in a uniformed services or Homeland Security mission, a solution that consists of a suite of systems best addresses detection levels between submiosis and large, overwhelming concentrations. In the Homeland Security mission, the desire to detect materials ranges from precursors to the actual finished product. To date, there is no single technology that has the capability to detect across this wide range. Therefore, the development of packages of detection equipment for use in these scenarios must consider a suite of detectors that employ several technologies and offer a wide variety of functions. The toolbox of detection equipment may also utilize commercially available products, which in combination can provide an extensive capability for the teams. The Department of Defense has successfully leveraged commercial products in both an as-purchased configuration as well as with some modification to meet more specific requirements. The Joint Chemical Agent Detector is an example of a commercially available system that the Department of Defense, in conjunction with the manufacturer, conducted system modifications to meet service-unique requirements [4].

## 3 DEFINING SYSTEM PERFORMANCE

This study opened with a discussion of the need to determine system requirements. Once defined, there must be a process to determine actual system performance against the requirements. Without performing an evaluation with actual test data, any system that is fielded carries a level of risk of having lesser capability than required or being inappropriate for the intended mission. Therefore, the step in the development that closely follows requirements definition is the development of the performance evaluation strategy.

### 3.1 System Evaluation

The process for conducting a system analysis is initiated with a review of the threat against which there is no defense. The Science and Technology community offers a candidate technology that forms the foundation for systems development. This community also identifies the critical parameters that make the technology effective against the threat, and having performed a sensitivity analysis, suggests a required range of measurements for

each parameter. This information forms the basis for the statistical design of experiments, to include accuracy and precision of each measurement that the Science and Technology community establishes in concert with the development community to ensure proper application and evaluation of the technology. In addition to reliability and confidence in terms of numbers and repetitions of trials, the design of experiments also considers the questions identified in the Section 1, so that all tests address the full gamut of conditions to which a system will be exposed in its life cycle to include disposal. To be efficient in providing equipment to the users, the evaluation strategy for any given system must be documented ideally before design and hardware build is initiated. If the evaluation strategy is developed based on the requirements and is finalized before the hardware is readied for testing, the parties who are developing the strategy do so without preconceived ideas of what the hardware will be or its performance characteristics. Likewise, when the developer understands how the system will be evaluated, he/she will be able to focus on the performance traits that are of highest priority to the user. This enables a situation whereby the provider offers a solution that most closely meets the customer's needs. The Department of Defense application of these concepts is illustrated in Figure 1.

To adequately evaluate a detection system, one must establish a series of tests that generate data to answer the questions that are pertinent to the use and purpose of the system. For example, the questions posed in Section 1.1 ask "how and to what degree will this equipment protect the intended audience?" The two modes of use for the held Joint Chemical Agent Detector are monitor and survey [4]. Each mode has a different purpose, which creates different test conditions and requirements. In a monitor mode, the employment concept is for use in a preexposure/preattack clean environment; therefore, the system must provide an alert at first indication of the presence of a chemical agent. In the survey mode, the assumption is that the attack has occurred, and the user is surveying to define areas of contamination as well as checking for any possible contamination after decontamination operations. These two conditions present different levels of acceptable performance.

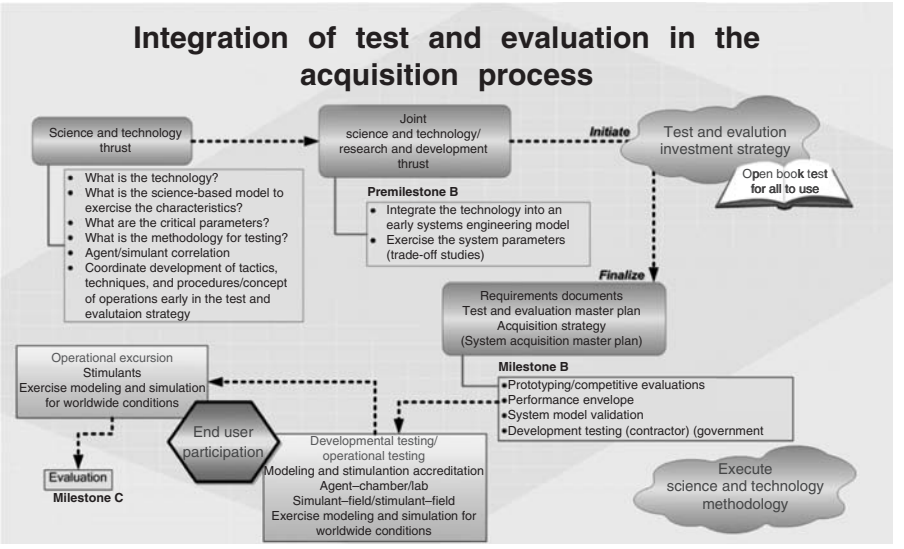



**FIGURE 1** Test process development.

The Joint Chemical Agent Detector testing for detection of agent in the monitor mode required the introduction of an agent stream that replicated a concentration profile representing the onset through full development of an agent vapor cloud. To determine whether the detection performance was acceptable, the data collected during the test trials included concentration as a function of time, time for the system to detect, concentration at which a detection occurs, temperature and relative humidity of the agent stream, temperature and relative humidity of the system under test, occurrence of any false alarms, and detection and identification of the agent by the system under test as depicted by its display [11]. In some cases, actual spectra were collected during agent trials to provide information regarding the accuracy of the drift tube functioning [12]. This data was essential to understand how the system was performing and if its performance would provide utility for the user. Additionally, in the monitor mode, the time to alarm when exposed to agent vapor must allow the user sufficient time to alert others to don protective gear or initiate collective protection in vehicles or facilities. Therefore, the product of the concentration level at detection and the time to alarm is an indication of the dose that a user would experience. This factor and the toxicity of the detected substance translate into a relative hazard level to the user as discussed above. Similarly, in the survey mode, the Joint Chemical Agent Detector is used in both postattack and post-decontamination scenarios to determine if the equipment is contaminated, and once decontaminated, if the decontamination process was sufficient to declare the equipment safe for use by personnel in an unprotected posture. These evaluation questions were answered from an agent performance data set [5] with two sampling intervals that represented the mission scenarios. The efficiency of the design of experiments generated a data set that could determine the degree to which the system enabled the user to meet both missions of detect and alert to protect as well as sort for and validate after the decontamination process.

When the Joint Chemical Agent Detector is used in its intended environment, and since it is a handheld device, the designer paid strict attention to the human factor aspects. The Joint Chemical Agent Detector was required to operate in "basic" operational environmental [3] conditions, which translated to a minimum temperature of $-25^{\circ}$F [13]. The human factors implication of this requirement meant that the size of the system operator could range from the 5th percentile female to 95th percentile male. Additionally, since the range of operations included arctic conditions, operators would be wearing arctic mittens, which increase the size of the gloved hands while decreasing dexterity. Design considerations included the location and separation of switches and buttons as well as the size and readability of the display. These considerations influenced the operation of the instrument where size, weight, and ease of use were traded in favor of optimized performance.

### 3.2 Parametric Determination

When designing a test program for a given technology, it is essential to understand what parameters of the technology have the greatest influence on whether the technology performs appropriately. These are then the parameters that must be tested thoroughly and with greater accuracy and precision, than a parameter that may be relevant to the overall system performance, such as weight or cube, but which has little impact on whether the applied science will be effective.

The Science and Technology community typically proposes a candidate technology as the foundation for a development program. It also identifies the key parameters of

the technology and the scientific explanation of how the technology addresses the threat characteristics. When a new technology is introduced or applied in a new use concept, the need to develop an appropriate test methodology arises. It is essential to test and collect data for a technology in a scenario appropriate to the application for which it will be used. In ion mobility spectrometry, the mobility peaks of samples, be they chemical agent vapors or naturally occurring vapors such as water, are affected by the environmental conditions of temperature, humidity, and pressure. Since all the peaks shift an equal amount under the same environmental conditions, the impact of the environmental conditions can be neutralized if a reference reactant ion peak is incorporated in the design. Alternatively, the design of a system that did not require a reference reactant ion peak would have required internally controlled temperature, humidity, and pressure to ensure that the system saw the absolute mobility of the sample in the drift tube under all environmental conditions. This design would have added serious size, weight, and power demands, which were unacceptable to the user, because, in the Joint Chemical Agent Detector, the minimum size and weight requirements were extremely high priority to the user. Therefore, developing a methodology to determine the applicability of the ion mobility spectrometry technology for use in the Joint Chemical Agent Detector by measuring the ion peak of a substance without reference to a reactant ion peak is of no value in determining what material is present. Similarly, in an evaluation strategy, measuring the weight of a system to five significant decimal places when the impact of this precision has no bearing on the effectiveness of the ion mobility spectrometry is irrelevant and wasteful in terms of value to the overall system assessment. Determining the correct parameter to measure, establishing the relevant accuracy and precision of the measurement, identifying appropriate instrumentation to attain the required measures, and designing an experiment, which captures the use conditions of the system, form the basis of the methodology development effort. The final result must be a data set that defines the performance of the system void of experimental artifacts. The Department of Defense's approach to test process development is pictured in Figure 2.

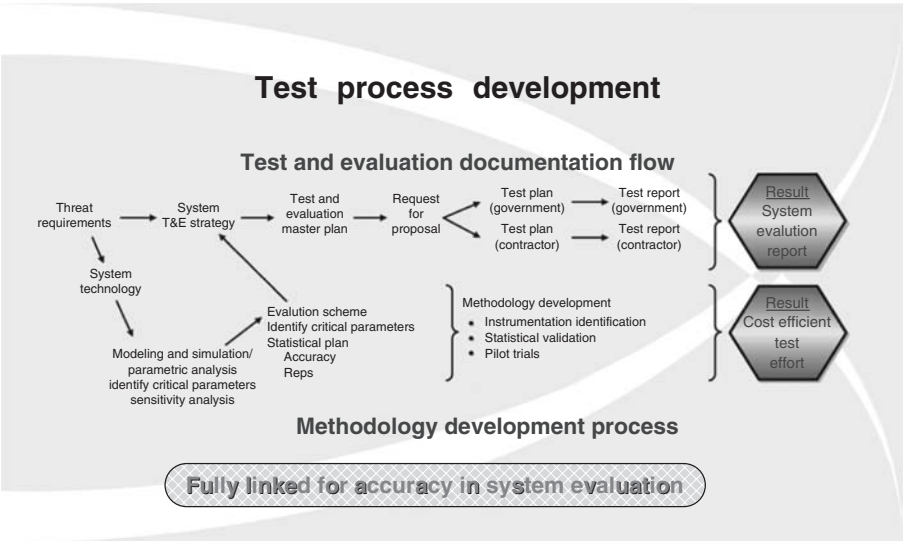



**FIGURE 2** Integration of test and evaluation in the acquisition process.

### 3.3 Use of Modeling and Simulation as an Element of the Evaluation Strategy

The systems engineering approach to development includes requirements development, parametric determination, design of experiments, trade-off analysis, modeling and simulation, and experimentation. In the development of detectors for chemical agent vapors, the incorporation of modeling and simulation has played an important role. In all developments, the evaluators require data regarding performance against live agents. The single most important difference between detector developments with ion mobility spectrometry technology and passive infrared technology was the ability to conduct qualification tests that represented the actual mode of employment. For the small handheld point detector such as the Joint Chemical Agent Detector, tests were conducted in a chamber in which the systems were exposed to an agent environment as they would experience in the open air [14]. Responses were directly related to statements of performance. The evaluation of the Joint Service Lightweight Standoff Agent Detector precluded testing in the system's intended environment due to the prohibition of use of agent in the open environment [15]. Therefore, the evaluation strategy determined performance through a series of chamber tests with a live agent that had a truncated path length from the instrument to the target material, similarly truncated path length chamber tests with simulants, field-tests with simulants, and a physics-based model that predicted performance based on the test data and scientific first principles [16]. The development and evaluation community made performance statements based on a strategy consisting of empirical data and modeling results. The models were verified and validated by independent sources and then accredited by the organization using the models to perform the system evaluation. The process of model development, verification, and validation is a standardized, documented procedure used in industry as well as the federal government [17]. The advantages of using modeling include creating the ability to gain system knowledge when testing is unavailable, as well as asset conservation.

## 4 SUMMARY AND CONCLUSIONS

The development of chemical warfare agent vapor detectors by the Department of Defense has been focused on the use scenarios specific to the uniformed services. Using a systems engineering approach, hardware developers respond to the user's requirements, which describe the need for the systems based on new or increased capability, to protect against known or changing threats. The identification of the critical parameters of a given technology by the Science and Technology community aids in developing an appropriate evaluation strategy that must include the design of experiments, development of new methodology, use of modeling and simulation, as well as acquisition of empirical data. Developing the evaluation strategy before any hardware is offered for test presents the most unbiased and unconstrained opportunity for the community to define and prioritize the data requirements.

Use of modeling and simulation in the qualification of systems was essential in the acceptance of a system for which outdoor testing with prohibited materials was not permitted. The development of a physics-based system model was a foundation block for the modeling and simulation effort for the standoff detection system that demonstrated the performance of the system against the threat materials. In the development of agent detector systems, challenges against actual threat material are essential to assure confidence in the system. Data exists for currently available systems that demonstrate effective

chemical agent vapor detection performance by both ion mobility spectrometry point and passive infrared standoff systems [16]. The application of this equipment to Homeland Security scenarios requires early analysis of employment concepts to determine similarities in use to enable leveraging of performance data and development of maintenance concepts and facilities to support the Homeland Security mission. The demonstrated performance of the Joint Chemical Agent Detector, a point detector, and the Joint Lightweight Standoff Chemical Agent Detector, a standoff detector, against chemical warfare agents in the challenging environments typical of military applications is a prime example of the opportunity to leverage Department of Defense development to a Department of Homeland Security application. That the use concepts and environments of the Department of Homeland Security are less harsh ensure favorable performance while enhancing commonality and standardization of equipment across federal agencies.

## REFERENCES


1. Eiceman, G. A., and Karpas, Z. (2005). *Ion Mobility Spectrometry*, 2nd ed., CRC Press, Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300, Boca Raton, FL, 33487-2742, pp. 3–5.
2. Title 10 Code of Federal Regulations Part 20, Standards for Protection Against Radiation. (2007).
3. Capability Production Document for Joint Chemical Agent Detector (JCAD). (2008). *Increment: I, ACAT III, Validation Authority: Joint Requirements Office Committee (JROC), Milestone Decision Authority: Joint Program Executive Officer for Chemical and Biological Defense, Designation: JROC Interest prepared for Milestone (MS) C Decision*, Version 11.
4. Performance Specification Detector, Joint Chemical Agent (JCAD). (2008). *Increment 1, EA-D-10009, Prepared for: JPM, NBC Contamination Avoidance, SFAE-CBD-NBC, Aberdeen Proving Ground, MD 21010-5424*, Submitted by Kim-Tuyen Le, Chairman, Configuration Control Board, JCAD Team.
5. System Evaluation Report for Joint Chemical Agent Detector (JCAD) Increment 1. (2008). *Assessment produced by U.S. Army Evaluation Center*.
6. Joint Service Lightweight Standoff Chemical Agent Detector (JSLSCAD) Capability Production Document (CPD) Milestone C. (2005). *Increment 1, Acquisition Category (ACAT) III, version 1.*
7. Lyons, R. C., and Milchling, S. S. (1997). *ERDEC Technical Report TR-346, XM21 Remote Sensing Chemical Agent Alarm (RSCAAL) Risk Reduction Program*.
8. USACHPPM. (2008). *Health-based Chemical Vapor Concentration Levels for Future Systems Acquisition and Development*, USACHPPM Technical Report No. 64-FF-0722-07, U.S. Army Center for Health Promotion and Preventative Medicine.
9. Tauras, D. G., and Kichula, J. (1995). *Contributor, "Conduct Systems Engineering Trade Studies Process", Rev 3*, Defense Acquisition University.
10. Flanagan, M. J., and Hammond, B. (2006). *Final Technical Report for the Joint Service Lightweight Standoff Chemical Agent Detector Engineering and Manufacturing Development Program, prepared by General Dynamics Armament and Technical Products, Charlotte, N.C. under Contract No DAAM01-97-C-0030*.
11. Joint Chemical Agent Detector (JCAD) ACAT II (with OSD T&E oversight) Test and Evaluation Master Plan (TEMP) Increment 1 Supporting Multi-Service Operational Test and Evaluations, and Full Rate Production, Version 2.2, 13 June 2007, submitted by Kyle T. Burke, COL USA, Joint Project Manager NBC Contamination Avoidance, approved by Charles, E. McQueary, Ph.D., Director, Operational Test and Evaluation, 10 August 2007.

12. TRIMSCAN. (2009). *Time Retentive Ion Mobility Scan Analysis (TRIMSCAN) Manual/User's Guide 8X/699-399 Issue AJ (Version 0.5)*. Smiths Detection Limited, Watford.
13. Department of Defense Test Method Standard. (2008). *MIL-STD 810G, Environmental Engineering Considerations and Laboratory Tests*, 31 Oct 2008.
14. Detailed Test Plan for the Production Qualification Test (PQT) for the Chemical Warfare Detection and Identification Testing for the Joint Chemical Agent Detector (JCAD) Increment 1 Gate 2, Test Project No 2006-DT-DPG-JCADX-C8866, WDTC Document No. WDTC-TP-05-135, December 2005, prepared by Louis Anderson, R. James Berry, Brad Rowland, and George Law, West Desert Test Center, U.S. Army Dugway Proving Ground, Dugway, UT 84022-5000.
15. *US Code Title 50:War and National Defense-50 USC 1512 Sec 1512*, January 2003.
16. Larsen, E. C., Bankman, I. N., Lazarevich, A. K., and Rogala, E. W. (2006). *The Johns Hopkins University Applied Physics Laboratory, Young, Randy S., Althenbaugh, Ryan, Reherman, Jason, Joint Project Manager Nuclear Biological Chemical Contamination Avoidance, "Verification and Validation (V&V) Report for the Joint Service Lightweight Standoff Chemical Agent Detector (JSLSCAD) Increment 1 Model and Simulation (M&S).*
17. Testing and Evaluation of Standoff Chemical Agent Detectors. Committee on Test and Evaluation of Standoff Chemical Agent Detctors, Board on Chemical Sciences and Technology, Division on Earth and Life Science, National Research Council of National Academies. (2003). *"Testing and Evaluation of Standoff Chemical Agent Detectors" report by the National Academy of Sciences (NAS) Committee on Testing and Evaluation of Standoff Chemical Detectors.* The National Academies Press, Washington, D.C., www.nap.edu.

# SENSING DISPERSAL OF CHEMICAL AND BIOLOGICAL AGENTS IN URBAN ENVIRONMENTS

Angela M. Ervin, Anne E. Hultgren, Edward P. Rhyne, and Keith B. Ward
*Department of Homeland Security Science and Technology Directorate, Washington, D.C.*

## 1 RATIONALE FOR CHEMICAL AND BIOLOGICAL SENSORS IN URBAN ENVIRONMENTS

The urban environment consists of a variety of unique venues, including large indoor and outdoor gathering spaces, office and residential buildings, and regional and national transportation systems, all containing large populations to be protected. The potentially

devastating effects of the release of a chemical or biological agent in an urban environment, including massive loss of life and property, have been documented in several recent reports [1–4]. The Department of Homeland Security (DHS) has the task of protecting these urban environments against the threat of a chemical or biological agent attack from international or domestic terrorists, natural disasters, and industrial accidents [5–7]. DHS Science and Technology (S&T) Directorate is addressing this challenge by developing appropriate detection technologies, performing assessment and impact studies, as well as validating decontamination and restoration procedures and protocols to ensure that we are prepared to respond to and mitigate the damage from such a chemical or biological attack or accident.

A DHS preparedness plan to counter chemical and biological threats begins with deploying an extensive system of chemical and biological sensors throughout the urban environment to provide early warning of an attack or accident [8, 9]. There are significant challenges with deploying sensors in an urban environment, such as operating in a densely populated civilian population where interpretation and response to a sensor alert must be understood and managed in a dynamic environment, operating in the presence of sensor interferent materials, and operating in the midst of legitimate activities which involve near neighbor or simulant materials. All of these challenges can degrade sensor performance by creating false positive or false negative detections. DHS S&T is also sensitive to the commercial market drivers which demand that the technology solutions are low cost to purchase and maintain as the operation of these sensors will be an additional burden on facility operations. There are systems currently in place to provide detection and response to a chemical or biological incident; however there are still significant shortcomings with these technologies. The current first responder tools are plagued with false alarms and difficultly in interpretation of the results, while the installed systems have long detection times and are prohibitively expensive for general deployments. The technologies and sensor network architectures to fulfill the DHS preparedness plan and improve upon current sensors are described in detail in this article.

## 2 CHEMICAL AND BIOLOGICAL DETECTION ARCHITECTURE

The chemical agent detection architecture concept for homeland security considers the very different requirements for response to an indoor attack versus the response to an outdoor attack. Indoor protection of high-asset buildings and facilities (e.g. subway stations, airports, etc.) are oriented toward a “detect-to-warn” scenario. In this scenario, autonomous sensors with a rapid response time are widely deployed in the indoor environment. These rapid sensors will issue an alert of an attack in time to allow effective countermeasures (e.g. shutting down or redirection of heating, ventilation and air conditioning (HVAC) units) to contain the threat and reduce exposure to the building occupants. This protection architecture will save the greatest number of lives via sufficient warning time, and also provide critical information to first responders prior to entering the scene of an incident. The response plan to an outdoor attack constitutes a “detect-to-protect” scenario, which are aimed at providing first responders information to quickly assess the type and extent of the chemical release and the type of protective protection equipment (PPE) to don. The lightweight, portable nature of the devices under development for

outdoor environments makes them very mobile, and hence can be used to track chemical agent plumes, either by hand or secured to a fire truck or response vehicle, to assist emergency personnel in determining evacuation areas and decontamination procedures when necessary. The detection of low vapor pressure chemical threat compounds (e.g. $<10^{-4}$ Torr) is of special concern for homeland security because of their persistence and long-term contamination in the environment. Although chemical attacks are not likely to cause the widespread casualties that could be observed in the case of a biological attack, chemicals are easier to obtain and package for dissemination amongst a large crowd of people (e.g. the 1995 release of Sarin in the Tokyo subway) and thus continue to represent a serious threat to homeland security.

The goal of the biological agent detection architecture concept for homeland security protection of urban areas is to enable the rapid detection of the presence of disease causing agents in advance of the presentation of medical symptoms in the population. The architecture must also take into consideration the diversity of biological threat agents as well as the variety of release scenarios for the protection of both indoor and outdoor environments. This goal is accomplished through the wide deployment of three classes of biological agent detection sensors, supported by the national network of public health laboratories. Two of these classes are low confidence sensors intended for use in indoor environments. These sensors would initiate low consequence responses, such as shutting down or redirecting HVAC units, closing portions of buildings, and initiating analysis from the high confidence detection sensors. The third class of sensor is a high confidence sensor intended for use in a "detect-to-treat" mode, which would initiate high consequence responses, such as the quarantine of people, evacuation and restriction of affected areas, and the distribution of medical countermeasures. In order to maximize the benefit from national investment in these high confidence biological detectors, the locations for their permanent installation are determined through studies to protect the maximum percentage of the US population as well as the occupants and visitors of high-profile indoor spaces.

Lastly, the feasibility of an integrated architecture to include the detection of chemical, biological, radiological, nuclear, and explosive (CBRNE) threats within regional areas is being evaluated. This architecture would enable state and city agencies and private facilities to rapidly share information and decisions made in detection, crisis management, and response. By providing a complete view of an incident, the decision support needed for an effective response in the event of an attack will be available and easily transferable among the relevant agencies.

### 2.1 Low Consequence Sensor Performance Requirements

A low consequence sensor is one that initiates an action that is invisible to the general public as a result of an alert from the sensor. In the chemical detection arena, two projects fall into this category. Both projects are developing portable technologies for use by first responders to help with the assessment and characterization of an incident. The goal of the Lightweight Autonomous Chemical Agent Identification System (LACIS) Project is to develop an autonomous, hand-portable detection system with the ability to detect and identify a broad range of chemical agents. Table 1 lists the detailed performance metrics for this project. The lower limit of detection (LOD) and response time of detectors

**TABLE 1 DHS S&T Performance Goals for Low- and High Consequence Chemical Sensors**

| | Low Consequence | | High Consequence |
|---|---|---|---|
| Parameter | LACIS | LVPCD | ARFCAM |
| Agents detected | 17 chemical hazards: chemical warfare blood, vesicant, nerve, choking, and blister agents; TICs | Persistent chemical compounds (vapor pressures $10^{-4}$ Torr) on a variety of surfaces | 17 chemical hazards: chemical warfare blood, vesicant, nerve, choking, and blister agents; TICs |
| Response time | 2 min (IDLH and LOD) | 2 min | 1 min (IDLH); 15 min (PEL) |
| False negative rate | 0.1% | 1% | 5% |
| False positive rate | 1% | 1% | 1 per yr |
| Unit size | 0.5 cu ft; 5.0 lbs | 20 kg | |
| Unit acquisition cost | $2000 (quantities of 1000) | TBD | $1000 (quantities of 10,000) |
| Maintenance interval | 6 mo | 1 h battery life | 6 mo |
| Environmental conditions | 10–60°C and 0–90% RH | 0–40°C and 0–90% RH | 10–60°C and 0–90% RH |
| Communications | Wireless | TBD | Building network |
| Operations | Handheld | 3 m standoff, man portable | Installed, continuous and automated |

IDLH, immediate danger to life and health; LOD, limit of detection; PEL, permissible exposure level; TBD, to be determined; TIC, toxic industrial chemical; RH, relative humidity.

developed in LACIS will provide first responders with a tool to determine areas having dangerous chemical concentration levels and to determine if protective garments will be required for their activities. The second chemical detector technology that is considered a part of the low consequence scenario is the Low Vapor Pressure Chemical Detector System (LVPCDS) Project. The goal of this project is to develop and field-test a system focused on detecting and identifying toxic, low vapor pressure chemicals without contacting the contaminated surface. The LVPCDS performance metrics are also included in Table 1. Detectors developed in the LVPCDS Project will provide emergency personnel with a capability to detect and identify persistent chemical threats *in situ*, thereby eliminating the need for surface sampling (via swipes or swabs) and subsequent laboratory analysis.

The low consequence biological detection sensors are being developed for long-term unattended operation in indoor environments through a sensor network system. The performance requirements for these sensors assume that a high concentration release occurs in an indoor environment, and therefore the sensors will be exposed to a large amount of the biological agent due to the containment of the agent within the space. For operational use in occupied buildings, the sensor network must be affordable and have an overall false positive rate of once per many years depending on the operational requirements of the facility. In addition, the maximum benefit from these sensors will be in providing the earliest possible warning, less than 20 min after the release, to building occupants of an attack. This warning will limit the number of people who enter a potentially contaminated area and reduce the spread of the contaminant into other areas by shutting

**TABLE 2 DHS S&T Performance Goals for Low and High Consequence Biological Sensors**

| | Low Consequence | | High Consequence |
|---|---|---|---|
| Parameter | Triggers | Confirmers | BAND |
| Agents detected | Biological vs. Nonbiological Discrimination | 20 agents: CDC A&Blist | 20 agents: CDC A&B list |
| Limit of detection | 1000 CFU/L air (spores) 5 ng (toxin) | 100 CFU/L air (spores) 0.5 ng (toxin) | 100 organism/collection (spores, cells and viruses) 10 ng (toxin) |
| Response time | 2 min | 15 min | 3 h sample, 1 h analysis |
| False positive rate | 1 per wk | 0.001% | 0.00001% |
| Unit size | 2 cu ft | 5 cu ft | Modest packaging |
| Unit acquisition cost | $1000–10,000 (quantities of 1000) | $50,000 (quantities of 1000) | $25,000 (quantities of 1000) |
| Yearly O&M cost | $50–2000/sensor | $5000/sensor | $10,000/instrument |
| Maintenance interval | 1 mo | 1 mo | 1 mo |
| Sample archive | None | 1 mo (nonviable) | 5 d |
| Environmental conditions | Indoor | Indoor | Indoor and outdoor |
| Communications | Building network | Building network | Wireless |
| Operations | Installed in building environment | Installed in building environment | Installed, continuous and automated |

CDC A&B, Centers for Disease Control A&B agent list; O&M, operation and maintenance; CFU/L air, colony forming unit per liter of air.

down or redirecting building airflows. To meet these aggressive sensor network requirements, two classes of sensors (triggers and confirmers) are under development in the DHS Detect-to-Warn Project as components of an overall sensor network. The detailed performance requirements for the triggers and confirmers are listed in Table 2. Trigger sensors continuously test the environment for an increase in respirable biological material, above levels either anticipated or typically observed. Trigger sensors can accomplish this nonspecific biological detection within 1 min, although they are expected to have a high false positive rate due to naturally occurring biological materials in the environment. Once this elevation of biological material is detected, a confirmation sensor is initiated to automatically collect a sample and determine if the material is a biological threat. The confirmation sensors are very specific to biological threat materials, have automated sample collection, purification, and proessing ability, and also perform very rapid detection assays to meet the 10–20 min network detection goal. This triggered confirmer architecture lowers the false positive rate of the overall detection network to meet the stringent requirements of facility owners, since the confirmer sensors are run only a fraction of the time.

### 2.2 High Consequence Sensor Performance Requirements

A high consequence sensor is one that initiates an action that would be obvious and inconvenient to the public (e.g. building evacuation) from an alert by the sensor. In

the chemical detection arena, the indoor facility chemical threat monitor project, the Autonomous Rapid Facility Chemical Agent Monitor (ARFCAM) Project is focused on high consequence detection. The ARFCAM Project goal is to develop a monitor to detect chemical threats in closed or partially enclosed facilities. The performance specifications for this project are shown in Table 1. This rapid and ultrasensitive detection capability will provide facility protection against both intentional releases and slow leaks of dangerous chemical materials.

In the biological detection arena, the Bioagent Autonomous Networked Detector (BAND) Project is focused on development of the high consequence detection systems. Deployed outdoors in an urban area in a "detect-to-treat" mode, these detection systems are anticipated to continuously sample the air, extract aerosol particulates, and analyze them at least once every three hours, providing an integrated detection of any airborne bioagent released within the preceding 3 h window. The DHS S&T performance goals of the BAND systems are given in Table 2. The key aspect of these systems is that they provide high confidence results to the public health community, which can be utilized as part of their decision process in response to a biological threat. To ensure that the BAND systems are delivering high confidence results, multiple agencies and the public health community have developed inclusivity (representative samples of potential pathogens) and exclusivity (background materials and near-neighbors) panels to use in testing the efficacy of the systems prior to their operational use. The tests of the sensors using these panels, as well as other system level tests such as long-term field tests, are designed to illustrate the system performance and establish that the BAND systems, or any other developmental systems, meet the minimum performance standards to be considered valid by the public health community.

In addition, two projects executed by DHS S&T are implementing integrated architectures to include the detection of CBRNE threats within high-profile regional areas. The Integrated CBRNE (iCBRNE) Project goal is to develop and deploy citywide detection, alert, and emergency response communication systems using mature technologies and tools. This would enable a network of city agencies to rapidly share critical information to make informed decisions with respect to detection, crisis management, and response. The Regional Technology Integration Initiative (RTII) Project intends to provide a complete networked chemical, biological, and explosive (CBE) sensor system in a model facility, using mature and validated detectors. In addition, the RTII Project will assist with training and conducting local exercises with the facility and first responder community on the operation and response to the CBE sensor network. This model CBE protection system will serve as an example for how to deploy an effective protection system for similar facilities throughout the country. In executing these two architecture focused projects, DHS S&T is facilitating the successful transition of these new technology solutions to the public and private community as well as offer a venue for testing and transition to commercial-off-the-shelf (COTS) of other DHS S&T developed sensors.

## 3 CHEMICAL AND BIOLOGICAL SENSOR TECHNICAL APPROACH

This section contains a description of the technologies currently under development to address the need for chemical and biological detection sensors for homeland defense. Note that neither the discussion nor the ordering of the technologies indicates a DHS S&T preference.

### 3.1 Low Consequence Chemical Sensor Technologies

The current technology development for low consequence chemical sensors in the LACIS Project is focused on three different analytical approaches described in this section. The first approach is a microelectromechanical system (MEMS)-based platform using an array of semiconducting metal oxide (SMO) materials to detect and identify a select series of chemical analytes. The SMOs are processed in such a way so as to induce control of target analyte reactions with a given sensing material imparting partial differential selectivity that, when coupled with signal processing and pattern recognition algorithms, affords detection and identification of chemical analytes with consistent accuracy and reproducibility [10].

The second approach is based on a hybridization of ion mobility spectrometry (IMS) and a polymer nanocomposite array (NCA). The IMS engine is based on the DoD-developed lightweight chemical detector (LCD) [11]. In IMS, gas-phase ions are separated by difference in mobility of the ions under the influence of an electric field gradient [12]. The IMS technology is a mature analytical approach with fundamental studies dating back to the 1950s. IMS parameters include high-speed analysis, portability, high reliability, and low cost. The NCA is a resistance-based detection modality where the interaction of a chemical analyte with a selective polymer matrix disturbs the inherent conductivity and the resulting change in resistance can be related to concentration of the analyte. The combination of the NCA and IMS data streams and processing with appropriate data fusion algorithms increases the detection space of this handheld chemical detection device.

The third approach under investigation in the LACIS Project is based on the laboratory gold-standard, mass spectrometry (MS). During a typical MS analysis, gas-phase ions are produced and undergo fragmentation via electron impact ionization [13]. These fragmented ions are then separated according to their mass-to-charge ratio ($m/z$) and their abundance. Due to the presence of multiple fragmented species, information rich spectra are obtained which can then be compared to a spectral library for identification. The technological challenges for these "detect-to-protect" devices are being able to detect a much broader range of chemical analytes than current COTS items with minimal (to no) false alarms, particularly false negative responses, in a rugged, form-fit low cost ($<$\$2000) package.

The current technology development for low vapor pressure chemical hazards in the LVPCDS Project is based on a technology known as laser interrogation of surface agents (LISA). The LISA platform is based on UV–Raman spectroscopy, and leverages Department of Defense (DoD) investments. UV–Raman spectroscopy uses ultraviolet (UV) light (typically 200–300 nm) to interrogate samples, which results in spectra with enhanced signal intensities versus longer wavelength Raman spectroscopy and thus improved signal to noise [14]. The current LISA technology in the man-portable configuration has several weaknesses, foremost being the high acquisition cost. Other technological challenges include high fluorescence on certain backgrounds and high shot noise, a short scan range ($<$3 m), and a small spot size for detection leading to long scan times to cover larger areas.

### 3.2 Low Consequence Biological Sensor Technologies

The current technology development for low consequence biological sensors focuses on triggers (1–3 min detection) and rapid confirmers (6–15 min detection). To meet the time

goals for trigger detection of biological aerosols, the "detect-to-warn" sensor development has focused on optical techniques that offer very rapid, often single-particle detection schemes. However, these optical techniques have limited discrimination capability and are prone to false alarms from naturally occurring biological and nonbiological materials in the environment. The most mature optical detection technique is based on detection of the three amino acids that have fluorescent properties in the UV region (tyrosine, tryptophan, and phenylalanine [15]). These fluorescent properties are measured by the sensors to detect the presence of aerosol particles with similar excitation and emission properties as those of the amino acids, indicating the presence of particles of potential biological origin [16, 17]. Additional optical techniques are being investigated to exploit characteristics of biological materials in other spectral regions, such as infrared detection [18], surface-enhanced Raman spectroscopy [19], laser-induced breakdown spectroscopy [20], and spark-induced breakdown spectroscopy [21]. Finally, another trigger sensor technique is to add a biologically specific optical tag to collected aerosol particles to enhance the detection of DNA or protein containing biological material from nonbiological environmental interferents [22]. These developmental trigger techniques are currently in the evaluation process of the performance characteristics of the technology to ensure confidence in the deployment of the sensors, and the engineering analysis for adequate fieldability of the resulting sensor designs.

"Detect-to-warn" confirmer sensors will provide a more specific analysis of collected material for rapid field presumptive identification. The indoor deployment of these sensors assumes a relatively high concentration of biological material to allow for the rapid detection timeline necessary for early warning of a biological attack. The confirmation sensor development has focused on moving standard laboratory techniques into autonomous, rapid, field deployable devices. Improvements have been made in the engineering of real-time polymerase chain reaction (rt-PCR) devices to reduce the temperature ramping times through reduction in the volume of the PCR reaction and shuttling of the reaction between fixed temperature zones. These improvements have resulted in devices capable of 6–8 min complete rt-PCR reactions using laboratory standard reagents [23, 24]. Advances in the design and production of microfluidic devices have utility in the creation of high-surface area antibody or nucleic acid structures with small analysis volumes, and for rapid mixing and binding of reagents leading to rapid detection assays [25]. Another emerging detection technology exploits cell-based sensing, where the response of simple living systems to the environment is monitored to rapidly detect the presence of biological agents [26]. Finally, new MS techniques are also under development to incorporate sample preparation and protein detection in cluttered environmental samples on automated MS platforms [27]. These confirmer technologies face several significant challenges before they will be transitioned to operation, including engineering for completely unattended operation and maintenance by facility personnel, and validation testing to demonstrate specificity and false positive characteristics of the sensors.

### 3.3 High Consequence Chemical Sensor Technologies

The current technology development for high consequence chemical sensors in the ARFCAM Project is focused on three different analytical approaches described in this

section. The first approach is based on IMS. As described in Section 3.1, gas-phase ions are separated by difference in mobility of the ions under the influence of an electric field gradient [12]. IMS parameters include high-speed analysis, portability, high reliability, and low cost.

The second approach is a coupling of the IMS with a miniature gas chromatograph (GC). In GC, constituents within a complex gas sample can be separated by sweeping the sample into a column with an inert gas (in this application the inert gas is ambient air). The chemical constituents that make up the gas sample interact with a stationary phase, which either fills or coats the column at different rates depending on their chemical or physical properties. Hence, the sample constituents will exit the end of the column into the IMS in a sequential manner and undergo further separation and detection. By placing the GC on the front end of the IMS, the GC acts to "pre-filter" the gas sample to increase selectivity of the IMS detection.

The third approach is a coupling of the IMS with differential mobility spectrometry (DMS). As is the GC in the GC–IMS approach, the DMS is positioned as a pre-filter to the IMS. The DMS technology was discovered in the former Soviet Union and is proving to be a very promising technology [12, 28]. DMS separates ionized compounds based on their differential mobilities that are a function of their charge, mass, and cross-sectional area. By applying both an RF and DC field to the DMS sensor, the sensor selects a chosen ion or collection of ions, which are then swept into the IMS for further separation and detection. The technological challenges for these "detect-to-warn" systems are being able to detect a much broader range of chemical analytes than current facility monitor systems, having minimal false alarms, particularly false positive responses, and being configurable and interoperable with current facility security measures, all at a low cost (~$10,000).

### 3.4 High Consequence Biological Sensor Technologies

During the BAND Project, several technologies have been investigated for both toxin and nucleic acid detection to meet the aggressive goal of identifying 20 agents in one system. To meet the BAND requirements, each system must be able to detect several diverse classes of agents, including toxins, viruses (RNA and DNA), and bacteria, within the analysis cycle time and at the LOD. The toxin detection methodologies exploit specific antibody reactions with various detection methodologies. The detection methods range from immuno-PCR [29] to traditional sandwich assays on beads or on long DNA constructs.

The nucleic acid detection methodologies employ both amplifying techniques and nonamplifying techniques. Each of these methodologies present opportunities for robust nucleic acid detection; however, they also face important challenges for creating a system that is capable of autonomous operation in extreme environments for 30 d without maintenance. The amplifying techniques utilize traditional PCR with various signal transduction methods, including microarrays, fluorescent probes, and padlock probes [30] with molecular beacons [31]. The amplifying technologies have the challenge of reducing reagent use and maintaining reagent activity for the month long maintenance cycles, as well as enabling high-multiplexed capability to identify 20 or more threat agents simultaneously. The nonamplifying technology under investigation in the BAND Project, direct linear analysis (DLA), creates a unique bar code of large DNA molecules [32]. By using long

fragments of DNA and nonspecific fluorescent tags, DLA utilizes a universal reagent set reducing operating costs while maintaining the high confident identification. DLA has the challenge that each DNA fragment of the appropriate length is investigated to determine the content of the sample, and therefore throughput challenges exist with this technique.

## 4 FUTURE TECHNOLOGY NEEDS AND IMPROVEMENTS

Although much progress has been made in the area of detection of chemical warfare agents, toxic industrial chemical vapors, and known pathogenic biological agents, there is still considerable room for improvement. These improvements are necessary for all of the chemical and biological detection technologies to allow for confident and widespread use of these sensors. Further reduction of false alarms is of key importance because decisions on whether to perform low-regret actions (such as shutting off or redirecting HVAC units) versus high-regret actions (such as evacuating buildings) will need to be made by facility operators based on the output from these sensor systems. The financial loss from evacuating a building after a false alarm can be very costly, so it is critical that the results from the sensors be extremely reliable. The continued reduction in sensor cost, while maintaining desired performance, is a major consideration for all potential customers of these technologies. These cost reductions will be essential so that more buildings, transit systems, and emergency personnel can afford the protection these sensors will provide. Finally, for both chemical and biological detection sensors, interoperability with existing incident commander procedures and protocols is an important future goal and should be considered early on in the technology development phase.

Major challenges facing chemical detection sensors include decreasing detection speed, while increasing the sensitivity and reliability of the sensors. One single technology will most likely not be able to detect such a broad range of threats, hence the future will likely see the integration of multiple sensors with data fusion functionality. Specific improvements for the portable chemical sensors will be continued reduction in sensor weight and size, as well as increased single battery operation time. These improvements are critical to meet the operational requirements of emergency responders.

For biological confirmation sensors, a major challenge for future development will be in moving beyond the paradigm of sensing specific biological agents to sensing the fundamental elements of what causes illness. Also desired in future sensors is the ability to keep field collected organisms viable for further investigation such as antibiotic susceptibility, and the ability to quantify the amount of organisms that are collected. A portable biological detection sensor will allow emergency personnel to add another layer of detection capability to their protective architecture. Finally, continued improvements in the long-term stability of reagents, the reduction in reagents needed for detection assays, and automated sample preparation platforms are required to make the distributed deployment of these sensors practical.

Looking beyond the next few years, the rapidly advancing field of nanotechnology is expected to positively impact the detection technology community. Highly sensitive and selective sensors are expected to result from the ongoing research that is exploiting the unusual surface area and thereby the increased reactivity and catalytic properties of nanomaterials. Additionally, improved fabrication processes are revealing reproducible and low cost production of these novel materials.

Significant progress has been made in the past few years in moving laboratory detection techniques into the first generation of fieldable chemical and biological sensors. More work remains to be done to engineer sensor solutions to address the challenges and needs of the diverse set of operators and users of these sensors in the urban environment. Protection of the urban infrastructure and population against a release of a chemical or biological threat will be realized as these sensors are widely deployed and operated.

## REFERENCES


1. Danzig, R. (2003). *Catastrophic Bioterrorism—What is to be done?* Center for Technology and National Security Policy, Washington, DC.
2. Romano, J. A. Jr., Lukey, B. J., and Salem, H. (Eds.) (2008). *Chemical Warfare Agents: Chemistry, Pharmacology, Toxicology, and Therapeutics*, 2nd ed., CRC Press, Boca Raton, FL.
3. Tucker, J. B. (2006). *War of Nerves*, Pantheon Books, NY.
4. Langford, R. E. (2004). *Introduction to Weapons of Mass Destruction*, John Wiley & Sons, Inc., Hoboken, NJ.
5. Bush, G. W. (2002). *National Strategy to Combat Weapons of Mass Destruction. National Security Presidential Directive 17/Homeland Security Presidential Directive 4*, Office of the Press Secretary, Washington, DC.
6. Bush, G. W. (2004). *Biodefense for the 21st Century. National Security Presidential Directive 33/Homeland Security Presidential Directive 10*, Office of the Press Secretary, Washington, DC.
7. Bush, G. W. (2007). *Homeland Security Presidential Directive 22* (*classified*).
8. Vitko, J. Jr., Franz, D. R., Alper, M., Biggins, P. D. E., Brandt, L. D., Bruckner-Lea, C., Burge, H. A., Ediger, R., Hollis, M. A., Laughlin, L. L., Mariella Jr, R. P., McFarland, A. R., and Schaudies, R. P. (2004). *Sensor Systems for Biological Agent Attacks: Protecting Buildings and Military Bases*, National Academies Press, Washington, DC.
9. Franz, D. R., Johnson, N. L., Bahnfleth, W. P., Bruckner-Lea, C., Buchsbaum, S. P., Friedlander, S. K., Hamlet, M., Knoop, S. L., Maier, A., Schaudies, R. P., Sextro, R. G., Stetzenbach, L. D., Thomas-Mobley, L. M., and Walt, D. R. (2007). *Protecting Building Occupants and Operations from Biological and Chemical Airborne Threats: A Framework for Decision Making*, National Academies Press, Washington, DC.
10. Derringer, T. *Unpublished Results from DHS S&T Phase II Independent Testing & Evaluation*, Battelle Memorial Institute, Columbus, OH (contract HSHQDC-06-F-00025).
11. Press Release (2007). *Smiths Detection Awarded Initial Contract to Supply M4 JCAD, the US Military's New generation Chemical Agent Detector*, 24 July 07, http://www.smiths-group.com/press_release_details.aspx?releaseID=264.
12. Eiceman, G. A., and Karpas, Z. (2005). *Ion Mobility Spectrometry*, 2nd ed., Taylor & Francis Ground, Boca Raton, FL.
13. de Hoffmann, E., and Stroobant, V. (2007). *Mass Spectrometry: Principles and Applications*, 3rd ed., John Wiley & Sons, Ltd, West Sussex.
14. Skoog, D., Holler, F. J., and Nieman, T. (1998). *Principles of Instrumental Analysis*, 5th ed., Brooks/Cole, United States.
15. Teale, F. W. J., and Weber, G. (1957). Ultraviolet fluorescence of the aromatic amino acids. *Biochem. J*. **65**(3), 476–482.

16. Kierdaszuk, B., Gryczynski, I., Modrak-Wojcik, A., Bzowska, A., Shugas, D., and Lakowicz, J. R. (1995). Fluorescence of tyrosine and tryptophan in proteins using one- and two-photon excitation. *Photochem. Photobiol*. **61**(4), 319–324.

17. Jeys, T. H., Herzog, W. D., Hybl, J. D., Czerwinski, R. N., and Sanchez, A. (2007). Advanced trigger development. *Linc. Lab. J*. **17**(1), 29–62.

18. Stuart, B. H., and Ando, D. J. (Eds.) (1997). *Biological Application of Infrared Spectroscopy*, John Wiley & Sons, West Sussex.

19. Jarvis, R. M., and Goodacre, R. (2004). Discrimination of bacteria using surface-enhanced Raman spectroscopy. *Anal. Chem*. **76**(1), 40–47.

20. Panne, U., and Hahn, D. (2006). Analysis of aerosols by LIBS. In *Laser Induced Breakdown Spectroscopy*, A. W. Miziolek, V. Palleschi, and I. Schechter, Eds. Cambridge University Press, Cambridge, pp 194–254.

21. Hunter, A. J. B., and Piper, L. G. (2006). Spark-induced breakdown spectroscopy: a description of an electrically generated LIBS-like process for elemental analysis of airborne particulates and solid samples. In *Laser Induced Breakdown Spectroscopy*, A. W. Miziolek, V. Palleschi, and I. Schechter, Eds. Cambridge University Press, Cambridge, pp. 585–614.

22. Reichardt, T. A., Bisson, S. E., Crocker, R., and Kulp, T. J. (2008). Analysis of flow-cytometer scattering and fluorescence data to identify particle mixtures (conference proceedings paper). In *Optics and Photonics in Global Homeland Security IV (Proceedings Volume 6945)*, C. S. Halvorson, D. Lehrfeld, and T. T. Saito, Eds. SPIE Publications, France.

23. Neuzil, P., Zhang, C., Pipper, J., Oh, S., and Zhou, L. (2006). Ultra fast miniaturized real-time PCR: 40 cycles in less than six min. *Nucleic Acids Res*. **34**(11):e77 (9 pages).

24. Kopp, M. U., de Mello, A. J., and Manz, A. (1998). Chemical amplification: continuous-flow PCR on a chip. *Science* **280**(5366), 1046–1048.

25. Northrup, M. A. (2004). Microfluidics: a few good tricks. *Nat. Mater*. **3**(5), 282–283.

26. Rider, T. H., Petrovick, M. S., Nargi, F. E., Harper, J. D., Schwoebel, E. D., Mathews, R. H., Blanchard, D. J., Bortolin, L. T., Young, A. M., Chen, J., and Hollis, M. A. (2003). A B cell-based sensor for rapid identification of pathogens. *Science* **301**(5630), 213–215.

27. Bunger, M. K., Cargile, B. J., Ngunjiri, A., Bundy, J. L., and Stephenson, J. L. Jr. (2008). Automated proteomics of E. coli via top-down electron-transfer dissociation mass spectrometry. *Anal Chem*. **80**(5), 1459–1467.

28. Buryakov, I. A., Krylov, E. B., Makas, A. L., Nazarov, E. G., Pervukhin, V. V., and Rasulev, K. (1991). Separation of ions according to mobility in strong AC electric fields. *Sov. Tech. Phys. Lett*. **17**(6), 446–447.

29. Sano, Takeshi., and Smith, Cassandra. L. (1992). Cantor, Immuno-PCR: very sensitive antigen detection by means of specific antibody-DNA conjugates. *Science* **258**, 120–122.

30. Marras, S. A. E., Kramer, F. R., and Tyagi, S. Genotyping single nucleotide polymorphisms with molecular beacons. In *Genotyping Single Nucleotide Polymorphisms: Methods and Protocols*, P. Y. Kwok, Ed. The Humana Press, Totowa, NJ, Vol. 212, pp. 111–128.

31. Hardenbol, P., Baner, J., Jain, M., Nilsson, M., NAmsaraev, E. A., Karlin-Neumann, G. A., Fakhrai-Rad, H., Ranoghi, M., Willis, T. D., Landegren, U., and Davis, R. W. (2003). Multiplexed genotyping with sequence-tagged molecular inversion probes. *Nat. Biotechnol*. **21**(6), 673–678.

32. Chan, E. Y., Goncalves, N. M., Haeusler, R. A., Hatch, A. J., Larson, J. W., Maletta, A. M., Yantz, G. R., Carstea, E. D., Fuchs, M., Wong, G. G., Gullans, S. T., and Gilmanshin, R. (2004). DNA mapping using microfluidic stretching and single—molecule detection of fluorescent site-specific tags. *Genome Res*. **14**, 1137–1146.

# SENSING RELEASES OF HIGHLY TOXIC AND EXTREMELY TOXIC COMPOUNDS

D. ANTHONY GRAY
*Syracuse Research Corporation, North Syracuse, New York*

## 1 INTRODUCTION

Chemical terrorism (i.e. using or threatening to use chemicals as weapons of terror) is a serious threat in modern society, which is likely to continue for many years. The level of the concern about this threat can be seen in many of the articles in this volume, and the explosion of information on the subject is available in scholarly documents, journal articles, Internet (e.g. [1, 2]), symposia, and short courses dedicated to the subject. In addition, the currency of at least one aspect of this threat was underscored when Iraqi insurgents successfully dispersed chlorine for the first time by exploding an improvised explosive device (IED)/chlorine tank combination in early 2007 as a means of dispersing an industrial chemical agent (see [3, 4]). Because of the magnitude of the threat both to civilians and military personnel and the potential consequences, it is incumbent on both governments and industry to prepare for such an event to the extent possible.

One of the ways to prepare for chemical terrorism events is to develop sensors capable of identifying and quantifying the chemical in use so that when an event occurs, it can be rapidly and accurately identified and its effects can be mitigated. A second way to prepare is to identify a list of candidate chemicals that have toxicological and physicochemical properties that are consistent with use as a chemical agent (e.g. a chemical that is both toxic and dispersible). Both of these activities are important to preparing for such an event for a number of reasons including the two major ones important to this discussion. Firstly, there are more than 100,000 chemicals currently in commerce, many of which have low toxicities, limited availabilities, or physical properties that are not consistent with those needed to be a serious threat to public health. It is therefore both impractical and imprudent to develop the large array of expensive sensors that would be needed to support the capability of identifying and quantifying all commercial chemicals and especially for those having a low likelihood of being considered as candidates for terrorist activity. Secondly, because there are so many commercially available chemicals that cannot be selectively identified with current sensor technology, there is a high likelihood that the identity of the toxic industrial chemical used in a chemical attack will be unknown to responders and health care providers throughout at least much of the initial portion of the event. This lack of information, however, may both lead to additional exposures to, for example, emergency responders, others at the scene, and health care providers at hospitals treating the victims (especially if the chemical has few or no organoleptic warning properties) and hamper or prevent delivery of life saving procedures to the exposed population.

For example, methyl sulfate has few warning properties at lethal concentrations and causes delayed pulmonary edema so that immediate symptoms may not be present in the exposed population. However, when symptoms appear 8–12 h after exposure, victims presenting respiratory distress may quickly overwhelm the capacity of the health care system to provide the needed respirators. This potentially could lead to significant loss of life that might be prevented if respirators were widely available. However, if the chemical substance were known at the outset of the event, valuable time would be gained to locate additional respirators that might be made available to the affected community from relatively distant points. This article is therefore devoted to describing a methodology for identifying potential chemical threat agents, identifying a set of toxic industrial chemicals that fit the criteria, and describing example sensor availabilities for selected highly and extremely toxic chemicals.

Any discussion of the type presented below, which lists a set of highly toxic industrial chemicals that could be used in a terrorist event and thereby potentially aiding terrorists, is not complete without a discussion of the propriety making such a list public. The types of issues associated with this article therefore parallel those discussed by Phillip A. Sharp in his editorial on the conduct of responsible science and the prudence of publishing the DNA sequence and reconstruction of the 1918 Spanish influenza virus [5]. His conclusion and that of a committee of the US National Academies charged with considering these issues were that the publication was the correct action on the basis of both national security and public health. While the consequences of publishing the DNA sequence and reconstruction of the 1918 influenza virus, which killed an estimated 50 million people worldwide, are much higher than a list of highly toxic industrial chemicals (release of a reconstructed version of this virus could potentially result in many deaths and therefore justified review at the national level), these same issues are relevant for publishing a list of highly toxic chemicals. It is the sincere hope of the author that the information in this article will spur new and innovative technologies including advances in the sensor development and manufacturing community, advances in the development of medical countermeasures that can be used to better treat victims, and advances in the development of replacement chemicals that will eliminate the need for the production of commercial quantities of these toxic chemicals. It is therefore the goal of this article that the information contained in it will result in greater security and safety for the people of all countries that suffer from a terrorist threat.

Finally, the list presented here is designed to be neither an exhaustive list of all possible threat agents nor a compilation of chemicals developed from highly authoritative and critically reviewed information sources (as is the case with, for example, the National Advisory Committee for Acute Exposure Guideline Levels for Hazardous Substances). Rather it is designed to be an initial survey of industrial chemical threat agents that can be used as a starting point for further discussion and development.

## 2 IDENTIFICATION OF EXTREMELY AND HIGHLY TOXIC CHEMICALS AND IMPACT TO SENSOR DEVELOPMENT

The US and other governments, in both recognition and response to the need described above, have sought to identify a set of toxic industrial chemicals that if used by terrorists

would cause significant harm (see, for example, Hauschild and Bratt [6] and Federal Register Vol. 72 17687–17745 [2007]), although no list specifically dedicated to extreme toxicity could be found in the available literature. In addition to identifying candidate threat chemicals, many of these efforts have also sought to quantify and prioritize the threats so that, for example, research and development work can be directed to those chemicals that will likely cause the highest impact if used. The criteria used to identify and prioritize these chemicals include acute lethality, availability, flammability, and reactivity and acknowledge that many factors will influence the degree of harm an event inflicts. A terrorist event involving industrial chemicals, of course, could take many forms including, for example, attacks on the infrastructure of a chemical manufacturing or storage facility (and thereby releasing toxic chemicals to the surrounding area), attacks on the chemical transportation system (e.g. destroying a rail tank car or cars carrying toxic industrial chemicals in a populated area), or attacks on the structures in populated or sensitive areas (e.g. a chemical release in a shopping mall, office building, or military installation). Factors that will influence the magnitude of the effect of these types of scenarios include the exact location of the attack (e.g. a major densely populated city vs. a smaller less densely populated area), weather (e.g. temperature, wind speed and direction, and precipitation), time of day and year (e.g. a mall at the height of the Christmas shopping season), dispersal method, and chemical used. While specific scenarios vary, it is clear that, if well executed, a terrorist attack using a highly toxic industrial chemical or chemicals can result in loss of life, significant injury, and potentially substantial economic harm. Other preparedness activities, such as determining the likely health and environmental effects from chemical releases/exposures, developing medical countermeasures, and developing and implementing training for the medical and emergency community to respond adequately to an event, are also important activities that must be undertaken before we can adequately respond to an event.

The first step in identifying a set of highly toxic chemicals is to determine what constitutes an extremely or highly toxic industrial chemical. As with previous efforts, the list of chemicals presented below is based on an assessment of acute lethality information by the inhalation and dermal routes and reported as an $LC_{50}$ or $LD_{50}$ (i.e. the air concentration or dose to the skin, respectively, that causes 50% of the population of test animals to die). The inhalation and dermal routes were considered to be the most important routes of exposure during a terrorist event involving industrial chemicals (oral exposure was considered to be less important) because the scenarios considered most relevant for toxic industrial chemicals involve dispersal of the chemical in the air in a building or at an event. During these releases, people will be exposed by both breathing the air that contains the chemical and potentially by touching surfaces contaminated with the chemical. Acute toxicity was considered to be the most relevant and most available measure since the types of events considered most likely for industrial chemicals are short-term events. In addition, lethality was considered to be the most relevant measure of acute toxicity because this endpoint will likely be a major purpose of a terrorist event and compilations of acute lethality are available (see below for further discussion). Although dated, one of the most commonly used (and thereby accepted) metrics for categorizing chemicals into acute lethality classes is that compiled by Hodge and Sterner [7, 8] and Hine and Jacobsen [9], and are summarized in Table 1. Chemicals under consideration

**TABLE 1 Acute Toxicity Classes**

| Toxicity Rating | Commonly Used Term | Routes of Administration: Oral $LD_{50}$ (Single Dose to Rats) (mg/kg) | Inhalation $LC_{50}$ (4-h Exposure to Rats) ppm[a] | Dermal $LD_{50}$ (Single Dose to Rabbit Skin) (mg/kg) |
|---|---|---|---|---|
| 1 | Extremely toxic | $\leq 1$ | $<10$ | $\leq 5$ |
| 2 | Highly toxic | 1–50 | 10–100 | 5–43 |
| 3 | Moderately toxic | 50–500 | 100–1000 | 44–340 |
| 4 | Slightly toxic | 500–5000 | 1000–10,000 | 350–2810 |
| 5 | Practically non-toxic | 5000–15,000 | 10,000–100,000 | 2820–22,590 |
| 6 | Relatively harmless | $\geq 15{,}000$ | $>100{,}000$ | $\geq 22{,}600$ |

[a]Neither Hodge and Sterner [8] nor Hine and Jacobsen [9] use the term "$LC_{50}$" to describe the criteria for inhalation toxicity, rather, they use "vapor exposure mortality of 2/6–4/6 rats" as the measure. This has been interpreted to be equivalent to $LC_{50}$ for the purposes of this discussion.

here, therefore, have either inhalation $LC_{50}$s that are less than or equal to 100 ppm for a 4-h exposure to rats or dermal $LD_{50}$s less than or equal to 43 mg/kg for exposure to rabbits.

Acute lethality is not the only measure of acute toxicity or necessarily the only one that should be considered when identifying chemicals of concern for use in a terrorist event. Rather, other endpoints may be equally important or at least significant in determining the final outcome of an event. For example, a moderately toxic chemical that is a lachrymator may cause the same effects as a highly toxic chemical that is not a lachrymator, and those exposed to the lachrymator cannot escape because of blurred vision and experience longer exposure times. Similarly, chemicals with lower toxicities, but without organoleptic warning properties such as smell or taste, may also have the same outcome if used in an event since air concentrations will go undetected by the exposed population and exposure concentrations and durations can be higher and longer, respectively. Other endpoints will also determine the outcome of an event and include, for example, long-term effects from short-term exposures (e.g. effects to a developing fetus and neurological effects) and delayed toxicity (e.g. pulmonary edema). Although metrics other than lethality, therefore, can be used to identify a set of candidate chemicals, they are typically much more difficult to consistently ascribe, have small data sets, or require significant assessment of the data (involving professional judgment) before conclusions can be made about toxicity and applied to a set of chemicals.

After determining the metrics for identifying extremely and highly toxic chemicals, sources of the needed information were located. One of the most comprehensive (albeit not exhaustive or peer reviewed) compilations of acute lethality information is contained within the Registry of Toxic Effects of Chemical Substances RTECS, available from Elsevier MDL; much of the acute lethality information in RTECS is

also available on the ChemIDplus, an advanced website maintained by the National Library of Medicine NLM, http://chem.sis.nlm.nih.gov/chemidplus/). Information from RTECS was supplemented with acute toxicity information from the Syracuse Research Corporation implementation of the Toxic Substances Control Act Test Submissions TSCATS database, which contains unpublished data submitted by the chemical industry to the Environmental Protection Agency (EPA) under Toxic Substances Control Act (TSCA) and provides abstracts with endpoint data for some of the submissions in the database (see http://www.syrres.com/‖esc/‖tscats.htm). There were approximately 7100 lethality records in the combined data sets for inhalation and dermal exposure, but only slightly more than 4200 records had information for the selected species.

The list was further edited by (i) removing those chemicals with inexact $LD_{50}$ or $LC_{50}$ values (e.g. an $LD_{50}$ value identified as "$>10$ mg/kg" was removed because it does not exactly identify a level), (ii) removing chemicals marketed as variable mixtures (e.g. ligroine), and then (iii) selecting only those that were commercially available. Commercial availability was determined by identifying a set of over 50,000 chemicals that are in EPA's Inventory Update Rule(IUR—this source lists organic chemicals produced or imported into the United States in volumes greater than or equal to 10,000 lb/year), the Directory of Chemical Producers (worldwide) published by SRI Consulting, or identified as commercially available on the ChemChannels website (http://www.chemchannels.com). Inclusion on one of these lists was considered to be sufficient to mean that the chemical was readily available and could be purchased somewhere in the world without significant difficulty.

Finally, units were converted when necessary to ensure that the comparisons with the selection criteria were consistent. In both RTECS and TSCATS, the units for inhalation $LC_{50}$ values can be reported either in terms of parts (e.g. ppm or ppb) or mass per unit volume (e.g. mg/m$^3$). The units for dermal $LD_{50}$ values can also be expressed in terms of either mass or volume per unit body mass (e.g. milligram per kilogram body mass or microliter per kilogram body mass). Inhalation $LC_{50}$ units in terms of mass per volume were converted to ppm then adjusted to a 4-h exposure assuming linearity (Haber's rule). Whenever converting from units of mass per volume, care was taken to ensure that the theoretical saturation concentration in ppm (i.e. [vapor pressure in mmHg/760 mmHg] $\times$ $10^6$) was at least equal to the calculated $LC_{50}$ in ppm. The needed vapor pressures for this calculation were obtained from Syracuse Research Corporation's PHYSPROP database, if available, or estimated using the EPISuite estimation programs (see http://www.epa.gov/opptintr/exposure/pubs/episuite.htm). If the $LC_{50}$ was reported in ppm or ppb, it was assumed that the reported concentration was achieved as a vapor independent of the calculated saturation concentration. Since animal exposures to aerosol concentrations in terms of mass per unit volume cannot be expressed in terms of ppm, this process eliminates those chemicals with vapor pressures too low to achieve a vapor concentration equal to their experimental $LC_{50}$ (the selection criteria assume vapor exposures). Dermal $LD_{50}$ values in terms of volume per unit body mass were converted to milligram per kilogram units assuming a density of 1 g/ml, thus the maximum dermal $LD_{50}$ value consistent with the highly toxic criteria in Table 1 would be 0.043 ml/kg or 43 $\mu$l/kg. The final set of chemicals matching the criteria included 126 and 31 chemicals that matched the inhalation (Table 2) and dermal criteria (Table 3, respectively. Tables 2 and 3 also contain

**TABLE 2 Industrial Chemicals Extremely or Highly Toxic by the Inhalation Route of Exposure**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LC_{50}$ (ppm) | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 1752-30-3 | AL2338000 | Acetone thiosemicarbazide | $C_4H_9N_3S$ | 131.22 | 6.71 | Tremor | Convulsions or effect on seizure threshold | Changes in the structure or function of the salivary glands |
| 107-02-8 | AS9660000 | Acrolein | $C_3H_4O$ | 56.07 | 7.85 | | | |
| 2937-50-0 | LV7168000 | Allyl chloroformate | $C_4H_5ClO_2$ | 120.54 | 6.57 | Dyspnea (labored breathing) | | |
| 26842-43-3 | SF1435000 | 2-Amino-2,4-dimethyl pentanenitrile | $C_7H_{14}N_2$ | 126.23 | 25 | Changes relating to olfaction other than a deviated or ulcerated nasal septum, change of the olfactory nerve, or change in the sense of smell | Somnolence or a generally depressed activity level | Tremor |
| 19355-69-2 | UD5155000 | 2-Aminoisobutyronitrile | $C_4H_8N_2$ | 84.14 | 27.8 | Changes relating to olfaction other than a deviated or ulcerated nasal septum, change of the olfactory nerve, or change in the sense of smell | Somnolence or a generally depressed activity level | |
| 7647-18-9 | CA1722000 | Antimony pentachloride | $Cl_5Sb$ | 299 | 29.4 | | | |
| 7784-42-1 | CC9968000 | Arsine | $AsH_3$ | 77.95 | 5.1 | | | |
| 98-87-3 | CW9716000 | Benzal chloride | $C_7H_6Cl_2$ | 161.03 | 30.5 | Changes in recordings from specific areas of the brain and/or membranous coverings | Excitement | Respiratory depression |
| 100-44-7 | XW9324000 | Benzyl chloride | $C_7H_7Cl$ | 126.59 | 75 | Respiratory depression | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 111-44-4 | KX1708000 | Bis(2-chloroethyl)ether | $C_4H_8Cl_2O$ | 143.02 | 56.4 | | | |
| 542-88-1 | KX1750000 | Bis(chloromethyl)ether | $C_2H_4Cl_2O$ | 114.96 | 12.3 | Chronic pulmonary edema (excess fluid accumulation and retention over time) | Hemorrhage (copious bleeding) | |
| 1461-23-0 | WR3458000 | Bromotributyltin | $C_{12}H_{27}SnBr$ | 369.99 | 0.859 | Somnolence or a generally depressed activity level | Structural or functional change in the trachea or bronchi | Hemorrhage (copious bleeding) |
| 78-94-4 | EX4312000 | 3-Buten-2-one | $C_4H_6O$ | 70.1 | 2.44 | | | |
| 4262-43-5 | CD1127000 | *t*-Butylarsine | $C_4H_{11}As$ | 134.07 | 73.5 | Unspecified liver changes | Unspecified changes in the kidneys, ureter, and/or bladder | Unspecified hair changes |
| 75-87-6 | FW7714000 | Chloral | $C_2HCl_3O$ | 147.38 | 73 | Ptosis (drooping of the eyelid) | Somnolence or a generally depressed activity level | Dyspnea (labored breathing) |
| 7782-50-5 | FX8204000 | Chlorine | $Cl_2$ | 70.9 | 73.3 | | | |
| 7790-91-2 | FX8372000 | Chlorine fluoride | $ClF_3$ | 92.45 | 74.8 | | | |
| 13637-63-3 | FX8386000 | Chlorine pentafluoride | $ClF_5$ | 30.45 | 30.5 | Lachrymation (excessive tearing) | Changes in the structure or function of the salivary glands | Corneal damage |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LC_{50}$ (ppm) | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 107-20-0 | AB4928000 | Chloroacetaldehyde | $C_2H_3ClO$ | 78.5 | 50.6 | BP elevation not originating from effects on the autonomic nervous system | Respiratory obstruction | Unspecified respiratory changes |
| 79-11-8 | AH6664000 | Chloroacetic acid | $C_2H_3ClO_2$ | 94.5 | 46.6 | | | |
| 78-95-5 | UG8134000 | Chloroacetone | $C_3H_5ClO$ | 92.53 | 65.5 | Somnolence or a generally depressed activity level | Ataxia (incoordination) | Unspecified hair changes |
| 2315-36-8 | AC3934000 | 2-Chloro-*N*,*N*-diethyl acetamide | $C_6H_{12}ClNO$ | 149.64 | 51.5 | Excitement | Muscle weakness | Unspecified respiratory changes |
| 1622-32-8 | KT2954000 | 2-Chloroethanesulfonyl chloride | $C_2H_4Cl_2O_2S$ | 163.02 | 63 | | | |
| 107-07-3 | KU7910000 | 2-Chloroethanol | $C_2H_5ClO$ | 80.52 | 88.1 | Somnolence or a generally depressed activity level | Dyspnea (labored breathing) | |
| 107-27-7 | PA7966000 | Chloroethyl mercury | $C_2H_5ClHg$ | 265.11 | 63.5 | | | |
| 107-30-2 | KX3066000 | Chloromethyl methyl ether | $C_2H_5ClO$ | 80.52 | 96.3 | Chronic pulmonary edema (excess fluid accumulation and retention over time) | Hemorrhage (copious bleeding) | |
| 106-48-9 | SM5446000 | *p*-Chlorophenol | $C_6H_5ClO$ | 128.56 | 2.09 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 104-12-1 | NZ5348000 | 4-Chlorophenyl isocyanate | $C_7H_4ClNO$ | 153.57 | 18 | Changes relating to olfaction other than a deviated or ulcerated nasal septum, change of the olfactory nerve, or change in the sense of smell | Dyspnea (labored breathing) | Unspecified gastrointestinal changes |
| 2909-38-8 | NZ5334000 | 3-Chlorophenyl isocyanate | $C_7H_4ClNO$ | 153.57 | 6.69 | Somnolence or a generally depressed activity level | Cyanosis (bluish or purplish cast to skin and mucous membranes due to lack of oxygen | Respiratory stimulation |
| 76-06-2 | PD3906000 | Chloropicrin | $CCl_3NO_2$ | 164.37 | 14.4 | Unspecified respiratory changes | | |
| 26447-14-3 | UD4312000 | Cresyl glycidyl ether | $C_{10}H_{12}O_2$ | 164.22 | 42 | Somnolence or a generally depressed activity level | Excitement | Muscle weakness |
| 4170-30-3 | HB4606000 | Crotonaldehyde | $C_4H_6O$ | 70.1 | 34.9 | | | |
| 460-19-5 | HD6146000 | Cyanogen | $C_2N_2$ | 52.04 | 87.5 | Respiratory obstruction | Lachrymation (excessive tearing) | Somnolence or a generally depressed activity level |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LC_{50}$ (ppm) | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 675-14-9 | YC3052000 | Cyanuric fluoride | $C_3F_3N_3$ | 135.06 | 3.1 | Excitement | Chronic pulmonary edema (excess fluid accumulation and retention over time) | Dyspnea (labored breathing) |
| 17702-41-9 | HP5880000 | Decaborane | $B_{10}H_{14}$ | 122.24 | 46 | Convulsions or effect on seizure threshold | Unspecified liver changes | Unspecified changes in the kidneys, ureter, and/or bladder |
| 56-18-8 | KC1302000 | 3,3′-Diaminodipropyl-amine | $C_6H_{17}N_3$ | 131.26 | 5.59 | Dyspnea (labored breathing) | Cyanosis (bluish or purplish cast to skin and mucous membranes due to lack of oxygen | Unspecified hair changes |
| 105-83-9 | KC1316000 | 3,3′-Diamino-*N*-methyl dipropylamine | $C_7H_{19}N_3$ | 145.29 | 11.8 | Acute pulmonary edema (rapid onset of excess fluid accumulation in the lungs) | Dyspnea (labored breathing) | Unspecified hair changes |
| 19287-45-7 | IB2688000 | Diborane | $B_2H_6$ | 27.68 | 40 | | | |
| 534-07-6 | UG8862000 | 1,3-Dichloroacetone | $C_3H_4Cl_2O$ | 126.97 | 2.79 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 110-57-6 | EW9534000 | *trans*-1,4-Dichloro-2-butene | $C_4H_6Cl_2$ | 125 | 86 | Lachrymation (excessive tearing) | Unspecified respiratory changes | Changes in the structure or function of the salivary glands |
| 79-35-6 | LD6370000 | 1,1-Dichloro-2,2-difluoroethylene | $C_2Cl_2F_2$ | 132.92 | 92.9 | Somnolence or a generally depressed activity level | Unspecified liver changes | Unspecified changes in the kidneys, ureter, and/or bladder |
| 22591-21-5 | EW3934000 | 1,1-Dichloro-3,3-dimethyl-2-butanone | $C_6H_{10}Cl_2O$ | 169.06 | 93 | Unspecified changes associated with the eye | Unspecified respiratory changes | |
| 62-73-7 | TB3360000 | Dichlorvos | $C_4H_7Cl_2O_4P$ | 220.98 | 1.66 | Lachrymation (excessive tearing) | Tremor | Changes in the structure or function of the salivary glands |
| 1464-53-5 | EU5824000 | 1,2 : 3,4-Diepoxybutane | $C_4H_6O_2$ | 86.1 | 90 | | | |
| 2524-04-1 | TB8148000 | Diethyl phosphorochloridothionate | $C_4H_{10}ClO_2PS$ | 188.62 | 20 | | | |
| 627-44-1 | PA8694000 | Diethylmercury | $C_4H_{10}Hg$ | 258.73 | 24.4 | Excitement | Ataxia (incoordination) | Dyspnea (labored breathing) |
| 627-54-3 | KT2996000 | Diethyltelluride | $C_4H_{10}Te$ | 185.74 | 3.16 | | | |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LC_{50}$ (ppm) | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 28178-42-9 | CV6664000 | 2,6-Diisopropylphenyl isocyanate | $C_{13}H_{17}NO$ | 203.31 | 5.65 | | | |
| 624-92-0 | KE2380000 | Dimethyl disulfide | $C_2H_6S_2$ | 94.2 | 2.06 | | | |
| 2524-03-0 | TB8176000 | Dimethyl phosphorochloridothionate | $C_2H_6ClO_2PS$ | 160.56 | 51.8 | | | |
| 77-78-1 | WX4466000 | Dimethyl sulfate | $C_2H_6O_4S$ | 126.14 | 8.72 | Dyspnea (labored breathing) | Cyanosis (bluish or purplish cast to skin and mucous membranes due to lack of oxygen | Hemorrhage (copious bleeding) |
| 2867-47-2 | PC0994000 | 2-(Dimethylamino)ethyl methacrylate | $C_8H_{15}NO_2$ | 157.24 | 96.4 | | | |
| 2439-35-2 | AT2044000 | 2-(Dimethylamino)ethyl acrylate | $C_7H_{13}NO_2$ | 143.21 | 11.3 | Ptosis (drooping of the eyelid) | Somnolence or a generally depressed activity level | Dyspnea (labored breathing) |
| 24424-99-5 | ID4235000 | Di-*t*-butyldicarbonate | $C_{10}H_{18}O_5$ | 218.28 | 11.2 | Unspecified changes associated with the eye | Dyspnea (labored breathing) | Weight loss or decreased weight gain |
| 106-91-2 | PC1022000 | 2,3-Epoxypropyl methacrylate | $C_7H_{10}O_3$ | 142.17 | 45 | Dyspnea (labored breathing) | Respiratory stimulation | Unspecified changes in the blood |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 541-41-3 | LV7252000 | Ethyl chloroformate | $C_3H_5ClO_2$ | 108.53 | 47.3 | Changes in lung weight | Weight loss or decreased weight gain | |
| 2941-64-2 | FQ5460000 | Ethyl chlorothioformate | $C_3H_5ClOS$ | 124.59 | 41.2 | Cardiomyopathy, including infarction (disease of the heart muscle, including tissue death resulting from local blood supply loss) | Emphysema (a condition of the lungs marked by enlargement of the alveoli either by dilatation or by breakdown of their walls, resulting in labored breathing and increased susceptibility to infection) | Diffuse hepatitis (liver cells are killed in a random manner, not relating to any particular lobe or zone of the liver) |
| 1498-64-2 | TB9142000 | O-Ethyl-dichlorothiophosphate | $C_2H_5Cl_2OPS$ | 179 | 32 | | | |
| 1498-51-7 | TB9114000 | Ethyl phosphorodichloridate | $C_2H_5Cl_2O_2P$ | 162.94 | 84.6 | | | |
| 151-56-4 | LE0924000 | Ethylenimine | $C_2H_5N$ | 43.08 | 28.4 | | | |
| 24468-13-1 | FQ5330000 | 2-Ethylhexyl chloroformate | $C_9H_{17}ClO_2$ | 192.71 | 34.3 | | | |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LC_{50}$ (ppm) | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 7782-41-4 | LR2170000 | Fluorine | $F_2$ | 38 | 46.3 | Conjunctive irritation | Dyspnea (labored breathing) | Weight loss or decreased weight gain |
| 371-62-0 | KV2324000 | 2-Fluoroethanol | $C_2H_5FO$ | 64.07 | 3.18 | | | |
| 79-14-1 | MG6160000 | Glycolic acid | $C_2H_4O_3$ | 76.06 | 2.28 | Changes relating to olfaction other than a deviated or ulcerated nasal septum, change of the olfactory nerve, or change in the sense of smell | Dyspnea (labored breathing) | Weight loss or decreased weight gain |
| 77-47-4 | HK1106000 | 1,2,3,4,5,5-Hexachloro-1,3-cyclopentadiene | $C_5Cl_6$ | 272.75 | 1.6 | Somnolence or a generally depressed activity level | Unspecified respiratory changes | |
| 18406-41-2 | JW7266000 | Hexamethoxydisilylethane | $C_8H_{22}O_6Si_2$ | 270.48 | 2.4 | Unspecified respiratory changes | | |
| 74-90-8 | MY6300000 | Hydrogen cyanide | CHN | 27.03 | 20 | | | |
| 7783-66-6 | NW2408000 | Iodine pentafluoride | $F_5I$ | 221.9 | 98.1 | Convulsions or effect on seizure threshold | Acute pulmonary edema (rapid onset of excess fluid accumulation in the lungs) | Fatty liver degeneration |
| 13463-40-6 | NX6062000 | Iron carbonyl | $C_5FeO_5$ | 195.9 | 10 | Somnolence or a generally depressed activity level | Dyspnea (labored breathing) | Weight loss or decreased weight gain |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 30674-80-7 | PC1218000 | 2-Isocyanatoethyl methacrylate | $C_7H_9NO_3$ | 155.17 | 6 | | | |
| 55-91-4 | TC3948000 | Isoflurophate | $C_6H_{14}FO_3P$ | 184.17 | 1.99 | Muscle weakness | Dyspnea (labored breathing) | Changes in the structure or function of the salivary glands |
| 10471-78-0 | | 2-Isopropenyl-2-oxazoline | $C_6H_9NO$ | 230.88 | 7.7 | | | |
| 68-11-1 | AJ4690000 | Mercaptoacetic acid | $C_2H_4O_2S$ | 92.12 | 55.7 | Food intake in animals | Dyspnea (labored breathing) | Changes in lung weight |
| 920-46-7 | PC1750000 | Methacryloyl chloride | $C_4H_5ClO$ | 104.54 | 14 | | | |
| 558-25-8 | PD2016000 | Methanesulfonyl fluoride | $CH_3FO_2S$ | 98.1 | 1.75 | Inhibition, induction or change in blood or tissue levels of true cholinesterase | | |
| 79-22-1 | FQ5362000 | Methyl carbonochloridate | $C_2H_3ClO_2$ | 94.5 | 22 | | | |
| 453-18-9 | AJ2058000 | Methyl fluoroacetate | $C_3H_5FO_2$ | 92.08 | 3.32 | | | |
| 421-20-5 | LU2884000 | Methyl fluorosulfate | $CH_3FO_3S$ | 114.1 | 1.25 | Lachrymation (excessive tearing) | Changes in motor activity (specific assay) | Dyspnea (labored breathing) |
| 60-34-4 | MX5208000 | Methyl hydrazine | $CH_6N_2$ | 46.09 | 34 | | | |
| 624-83-9 | NZ5754000 | Methyl isocyanate | $C_2H_3NO$ | 57.06 | 9.15 | Lachrymation (excessive tearing) | Dyspnea (labored breathing) | |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LC_{50}$ (ppm) | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 676-97-1 | SZ9660000 | Methyl phosphonic dichloride | $CH_3Cl_2OP$ | 132.91 | 26 | Excitement | Dyspnea (labored breathing) | Unspecified dermatitis after systemic exposure |
| 12108-13-3 | OV9576000 | 2-Methylcyclopentadienyl manganese tricarbonyl (MMT) | $C_9H_7MnO_3$ | 218.1 | 8.52 | Conjunctive irritation | Somnolence or a generally depressed activity level | Dyspnea (labored breathing) |
| 35203-06-6 | CT7938000 | *N*-Methylene-6-ethyl-2-methylaniline | $C_{10}H_{13}N$ | 147.24 | 93 | Unspecified changes associated with the eye | Somnolence or a generally depressed activity level | Dyspnea (labored breathing) |
| 140-76-1 | UZ4004000 | 2-Methyl-5-vinylpyridine | $C_8H_9N$ | 119.18 | 19.4 | | | |
| 7786-34-7 | HB6104000 | Mevinphos | $C_7H_{13}O_6P$ | 224.17 | 3.5 | Tremor | Acute pulmonary edema (rapid onset of excess fluid accumulation in the lungs) | Changes in the structure or function of the salivary glands |
| 7783-77-9 | QK5418000 | Molybdenum hexafluoride | $F_6Mo$ | 209.94 | 38.8 | Structural or functional change in the trachea or bronchi | Respiratory obstruction | Hemorrhage (copious bleeding) |
| 13463-39-3 | RB0042000 | Nickel carbonyl | $C_4NiO_4$ | 170.75 | 4.38 | | | |
| 10102-44-0 | RE9912000 | Nitrogen dioxide | $NO_2$ | 46.01 | 88 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 10544-72-6 | RF0322000 | Nitrogen tetroxide | $N_2O_4$ | 92.02 | 27.9 | Convulsions or effect on seizure threshold | Unspecified cardiac changes | Acute pulmonary edema (rapid onset of excess fluid accumulation in the lungs) |
| 62-75-9 | JF9856000 | *N*-Nitrosodimethylamine | $C_2H_6N_2O$ | 74.1 | 78 | Unspecified changes associated with the eye | Somnolence or a generally depressed activity level | Hemorrhage (copious bleeding) |
| 57-57-8 | RX2352000 | 2-Oxetanone | $C_3H_4O_2$ | 72.07 | 37.5 | | | |
| 10028-15-6 | SA2240000 | Ozone | $O_3$ | 48 | 4.8 | Acute pulmonary edema (rapid onset of excess fluid accumulation in the lungs) | Hemorrhage (copious bleeding) | |
| 376-53-4 | AV2842000 | Perfluoroadiponitrile | $C_6F_8N_2$ | 252.08 | 6.01 | Somnolence or a generally depressed activity level | Unspecified respiratory changes | Unspecified changes in the kidneys, ureter, and/or bladder |
| 376-89-6 | ME8988000 | Perfluoroglutaronitrile | $C_5F_6N_2$ | 202.07 | 8.11 | Somnolence or a generally depressed activity level | Unspecified respiratory changes | Unspecified changes in the kidneys, ureter, and/or bladder |
| 108-95-2 | SL9170000 | Phenol | $C_6H_6O$ | 94.12 | 82.1 | | | |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LC_{50}$ (ppm) | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 103-71-9 | CY2520000 | Phenyl isocyanate | $C_7H_5NO$ | 119.13 | 4.52 | Somnolence or a generally depressed activity level | Acute pulmonary edema (rapid onset of excess fluid accumulation in the lungs) | Cyanosis (bluish or purplish cast to skin and mucous membranes due to lack of oxygen |
| 140-29-4 | AL4130000 | Phenylacetonitrile | $C_8H_7N$ | 117.16 | 44.9 | Altered sleep time, including changes in the righting reflex | Muscle contraction or spasticity | Dyspnea (labored breathing) |
| 2687-12-9 | CW3633000 | 1-Phenyl-3-chloro-1-propene | $C_9H_9Cl$ | 152.63 | 4.65 | Somnolence or a generally depressed activity level | Respiratory depression | Decrease in body temperature |
| 638-21-1 | SY6930000 | Phenylphosphine | $C_6H_7P$ | 110.1 | 38 | Dyspnea (labored breathing) | Lachrymation (excessive tearing) | |
| 298-02-2 | TC1092000 | Phorate | $C_7H_{17}O_2PS_3$ | 260.39 | 0.258 | | | |
| 7803-51-2 | SY4830000 | Phosphine | $H_3P$ | 34 | 11 | Dyspnea (labored breathing) | | |
| 10025-87-3 | TD6832000 | Phosphorus oxychloride | $Cl_3OP$ | 153.32 | 32 | | | |
| 1185-09-7 | | 1,1,2,2-Tetrachloroethyl sulfenyl chloride | $C_2HCl_5S$ | 174.16 | 6.2 | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 5216-25-1 | XX3766000 | $\alpha,\alpha,\alpha$-*p*-Tetrachloro toluene | $C_7H_4Cl_4$ | 229.91 | 13.3 | Somnolence or a generally depressed activity level | Convulsions or effect on seizure threshold | Structural or functional change in the trachea or bronchi |
| 78-00-2 | TU5040000 | Tetraethyl lead | $C_8H_{20}Pb$ | 323.47 | 16.1 | Excitement | Cyanosis (bluish or purplish cast to skin and mucous membranes due to lack of oxygen | |
| 597-64-8 | WR6118000 | Tetraethyltin | $C_8H_{20}Sn$ | 234.97 | 11.9 | Muscle weakness | Dyspnea (labored breathing) | Hemorrhage (copious bleeding) |
| 2778-42-9 | CV6454000 | Tetramethyl-*m*-xylylene diisocyanate | $C_{14}H_{16}N_2O_2$ | 244.32 | 2.3 | Dyspnea (labored breathing) | Respiratory stimulation | Decrease in body temperature |
| 509-14-8 | PD2464000 | Tetranitromethane | $CN_4O_8$ | 196.05 | 18 | Methemoglobinemia (a condition in which the iron in a hemoglobin molecule is unable to transport oxygen effectively to the tissues)-carboxyhemoglobin (carbon monoxide bound to hemoglobin preventing oxygen exchange) | | |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LC_{50}$ (ppm) | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 294-93-9 | XJ3220000 | 1,4,7,10-Tetraoxacyclo dodecane | $C_8H_{16}O_4$ | 176.24 | 27 | Sensory change involving peripheral nerves | Unspecified liver changes | Weight loss or decreased weight gain |
| 108-98-5 | DB3304000 | Thiophenol | $C_6H_6S$ | 110.18 | 33 | Respiratory stimulation | Somnolence or a generally depressed activity level | Lachrymation (excessive tearing) |
| 3982-91-0 | XS4662000 | Thiophosphoryl chloride | $Cl_3PS$ | 169.38 | 20 | | | |
| 7646-78-8 | XU7588000 | Tin tetrachloride | $Cl_4Sn$ | 260.49 | 9 | | | |
| 7550-45-0 | XV3248000 | Titanium chloride | $Cl_4Ti$ | 189.7 | 51.6 | | | |
| 584-84-9 | CX0518000 | 2,4-Toluene diisocyanate | $C_9H_6N_2O_2$ | 174.17 | 14 | Lachrymation (excessive tearing) | Excitement | Dyspnea (labored breathing) |
| 1321-38-6 | | Toluene diisocyanate (mixture of 2,4- and 2,6-isomers) | $C_9H_6N_2O_2$ | 196.24 | 6 | | | |
| 921-03-9 | UH4522000 | Trichloroacetone | $C_3H_3Cl_3O$ | 161.41 | 29.5 | | | |
| 76-02-8 | AO0392000 | Trichloroacetyl chloride | $C_2Cl_4O$ | 181.82 | 63.9 | | | |
| 594-42-3 | PC6468000 | Trichloromethanesulfenyl chloride | $CCl_4S$ | 185.87 | 2.75 | | | |
| 98-07-7 | XX3976000 | $\alpha,\alpha,\alpha$-Trichlorotoluene | $C_7H_5Cl_3$ | 195.47 | 9.5 | Muscle contraction or spasticity | Respiratory depression | Weight loss or decreased weight gain |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 998-30-1 | WI6062000 | Triethoxysilane | $C_6H_{16}O_3Si$ | 164.31 | 37.2 | Ataxia (incoordination) | Acute pulmonary edema (rapid onset of excess fluid accumulation in the lungs) | Changes in kidney tubules, including acute renal failure and acute tubular necrosis |
| 35037-73-1 | | Trifluoromethoxyphenyl isocyanate | $C_8H_4F_3NO_2$ | 203.12 | 6.3 | | | |
| 98-16-8 | XX8456000 | $\alpha,\alpha,\alpha$-Trifluoro-*m*-toluidine | $C_7H_6F_3N$ | 161.14 | 66.8 | Muscle weakness | Cyanosis (bluish or purplish cast to skin and mucous membranes due to lack of oxygen | Respiratory depression |
| 2487-90-3 | WI6188000 | Trimethoxysilane | $C_3H_{10}O_3Si$ | 122.22 | 42 | | | |
| 141-59-3 | SF2044000 | 2,4,4-Trimethyl-2-pentane thiol | $C_8H_{18}S$ | 146.32 | 50.1 | Convulsions or effect on seizure threshold | Unspecified respiratory changes | Weight loss or decreased weight gain |
| 15112-89-7 | WI5754000 | Tris(dimethylamino)silane | $C_6H_{19}N_3Si$ | 161.37 | 57 | Lachrymation (excessive tearing) | Ataxia (incoordination) | Changes in the structure or function of the salivary glands |
| 100-43-6 | VA3262000 | 4-Vinylpyridine | $C_7H_7N$ | 105.15 | 39.5 | | | |

**TABLE 3 Industrial Chemicals Extremely or Highly Toxic by the Dermal Route of Exposure**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LD_{50}$ | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 75-86-5 | ON3024000 | Acetone cyanohydrin | $C_4H_7NO$ | 85.12 | 17 μl/kg | | | |
| 309-00-2 | JD4970000 | Aldrin | $C_{12}H_8Cl_6$ | 364.9 | 15 mg/kg | Changes relating to olfaction other than a deviated or ulcerated nasal septum, change of the olfactory nerve, or change in the sense of smell | Convulsions or effect on seizure threshold | Excitement |
| 107-11-9 | BA4858000 | Allylamine | $C_3H_7N$ | 57.11 | 35 mg/kg | Primary irritation after topical exposure (causes redness, swelling, and/or pain, and other evidence of irritation upon first contact) | Chronic pulmonary edema (excess fluid accumulation and retention over time) | |
| 28772-56-7 | GZ7154000 | Bromadiolone | $C_{30}H_{23}BrO4$ | 527.44 | 2.1 mg/kg | | | |
| 95465-99-9 | TC3388000 | Cadusafos | $C_{10}H_{23}O_2PS_2$ | 270.42 | 24.4 mg/kg | | | |
| 8065-48-3 | TC8792000 | Demeton | $C_8H_{19}O_3PS_2$. $C_8H_{19}O_3PS_2$ | 516.72 | 24 mg/kg | | | |
| 814-49-3 | TB7994000 | Diethyl chlorophosphate | $C_4H_{10}ClO_3P$ | 172.56 | 8 μl/kg | | | |
| 926-64-7 | AL3304000 | Dimethylamino acetonitrile | $C_4H_8N_2$ | 84.14 | 32 mg/kg | | | |
| 1122-58-3 | UZ0910000 | 4-Dimethylamino pyridine | $C_7H_{10}N_2$ | 122.19 | 13 mg/kg | | | |
| 77-77-0 | KW9058000 | Divinyl sulfone | $C_4H_6O_2S$ | 118.16 | 22 μl/kg | Primary irritation after topical exposure (causes redness, swelling, and/or pain, and other evidence of irritation upon first contact) | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2104-64-5 | TA6020000 | EPN (Ethoxy-4-nitrophen-oxyphenylphosphine sulfide) | $C_{14}H_{14}NO_4PS$ | 323.32 | 30 mg/kg | Somnolence or a generally depressed activity level | Unspecified gastrointestinal changes |
| 13194-48-4 | TC3416000 | Ethoprop | $C_8H_{19}O_2PS_2$ | 242.36 | 2.4 mg/kg | | |
| 107-16-4 | AL3556000 | Glycolonitrile | $C_2H_3NO$ | 57.06 | 5 mg/kg | Primary irritation after topical exposure (causes redness, swelling, and/or pain, and other evidence of irritation upon first contact) | |
| 105-31-7 | MT5768000 | 1-Hexyn-3-ol | $C_6H_{10}O$ | 98.16 | 15.8 mg/kg | | |
| 78-97-7 | ON2940000 | Lactonitrile | $C_3H_5NO$ | 71.09 | 20 $\mu$l/kg | | |
| 950-10-7 | KF13860-00 | Mephosfolan | $C_8H_{16}NO_3PS_2$ | 269.34 | 28.7 mg/kg | | |
| 126-98-7 | UI2520000 | Methacrylonitrile | $C_4H_5N$ | 67.1 | 12.5 mg/kg | | |
| 453-18-9 | AJ2058000 | Methyl fluoroacetate | $C_3H_5FO_2$ | 92.08 | 20 mg/kg | Convulsions or effect on seizure threshold | |
| 556-61-6 | PC6272000 | Methyl isocyanate | $C_2H_3NS$ | 73.12 | 33 mg/kg | | |
| 3680-02-2 | WW8330000 | Methyl vinyl sulfone | $C_3H_6O_2S$ | 106.15 | 32 $\mu$l/kg | | |
| 7786-34-7 | HB6104000 | Mevinphos | $C_7H_{13}O_6P$ | 224.17 | 4.7 mg/kg | | |
| 5903-13-9 | AE0938000 | Nissol | $C_{13}H_{12}FNO$ | 217.26 | 1.75 mg/kg | | |
| 311-45-5 | TB4298000 | Paraoxon | $C_{10}H_{14}NO_6P$ | 275.22 | 5 mg/kg | Direct parasympathomimetic (mimicking the "rest and relaxation" action of the parasympathetic nervous system, for example, reduces heart rate, dilates blood vessels, and reduces blood pressure, etc.) | |

(*continued overleaf*)

**TABLE 3 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | Molecular Formula | Molecular Mass | $LD_{50}$ | Toxic Effects | | |
|---|---|---|---|---|---|---|---|---|
| 56-38-2 | TC9772000 | Parathion | $C_{10}H_{14}NO_5PS$ | 291.28 | 15 mg/kg | | | |
| 298-02-2 | TC1092000 | Phorate | $C_7H_{17}O_2PS_3$ | 260.39 | 3.1 mg/kg | | | |
| 947-02-4 | NP4102000 | Phosfolan | $C_7H_{14}NO_3PS_2$ | 255.31 | 23 mg/kg | | | |
| 107-19-7 | UO7966000 | Propargyl alcohol | $C_3H_4O$ | 56.07 | 16 mg/kg | Unspecified dermatitis after systemic exposure | | |
| 3689-24-5 | XS8050000 | Sulfotep | $C_8H_{20}O5P_2S_2$ | 322.34 | 20 mg/kg | | | |
| 13071-79-9 | TC0350000 | Terbufos | $C_9H_{21}O_2PS_3$ | 288.45 | 1 mg/kg | | | |
| 2001-95-8 | YZ0098000 | Valinomycin | $C_{54}H_{90}N_6O_{18}$ | 1111.5 | 5 mg/kg | Tremor | Convulsions or effect on seizure threshold | Weight loss or decreased weight gain |
| 3984-22-3 | JX5551000 | 2-Vinyl-1,3-dioxolane | $C_5H_8O_2$ | 100.13 | 25 mg/kg | | | |

toxic effects information when available from RTECS or ChemIDplus Advanced at NLM.

Tables 4 and 5 contain membership in regulatory lists and toxicity guideline values for chemicals toxic by the inhalation and dermal routes, respectively. Regulatory lists included in the tables are the Department of Homeland Security's interim final rule on Chemical Facility AntiTerrorism Standards (DHS, see Federal Register Vol. 72 17687–17745 [10]), Chemical Weapons Convention (Organisation for the Prohibition of Chemical Weapons, OPCW), the US High Production Volume list (US HPV), and European Union High Production Volume Chemicals list (EU HPVC). Tables 4 and 5 also contain (i) Acute Exposure Guideline Levels (AEGL-3—the airborne concentration of a substance above which it is predicted that the general population, including susceptible individuals, could experience life-threatening health effects or death), (ii) Emergency Response Planning Guideline (ERPG-3—the maximum airborne concentration below which it is believed that nearly all individuals could be exposed for up to 1 h without experiencing or developing life-threatening health effects), and (iii) Temporary Emergency Exposure Limit (TEEL-3—the maximum concentration in air below which it is believed nearly all individuals could be exposed without experiencing or developing life-threatening health effects).

Of the 126 industrial chemicals listed in Table 2 (toxic by inhalation), 44 (35%) have $LC_{50}$ values that are less than or equal to 10 ppm, which is extreme toxicity by the Hodge and Sterner/Hine and Jacobsen scale. Similarly, 9 of the 31 chemicals (29%) listed in Table 3 (toxic by dermal exposure) have toxicities at or below 5 mg/kg or 5 $\mu$l/kg (or extreme toxicity). More than half (16 of 31) of the dermally toxic chemicals have pesticidal uses, while those identified with inhalation toxicity typically are used exclusively in industrial/commercial applications. There are nine isocyanates (e.g. trifluoromethoxyphenylisocyanate, 4-chlorophenyl isocyanate, and toluene diisocyanate), eight halophosphorus compounds (e.g. isoflurophate, diethyl phosphorochloridothionate, and thiophosphoryl chloride), and seven acid chlorides (e.g. trichloroacetyl chloride, thiophosphoryl chloride, and 1,1,2,2-tetrachloroethylsulfenyl chloride) in Table 2. The chemicals in the two tables range from reactive inorganic (e.g. chlorine, tin tetrachloride, and diborane) and organic (e.g. methyl fluorosulfate, methyl hydrazine, and acrolein) chemicals to organometallics (e.g. methylcyclopentadienyl manganese tricarbonyl (MMT), bromotributyltin, and diethyl telluride), hydrides (e.g. arsine, phenyl phosphine, and phosphine), and $\alpha$-halo compounds (e.g. chloroacetaldehyde, 1,3-dichloroacetone, and methyl fluoroacetate).

This wide range of chemical structures presents a problem for both industry and government to develop sensors that are sufficiently specific and sensitive to detect this range of chemicals at concentrations that will be protective of the potentially exposed populations. Specificity is important because, as noted above, one of the problems facing emergency response and medical teams is if the identity of the chemical used in a terrorist event is unknown, medical countermeasures appropriate to the toxicant used may not be available or even considered by the teams. Therefore, developing sensors specific to a chemical or class of chemicals (e.g. isocyanates) or capable of identifying the sensed chemical (e.g. gas chromatograph/mass spectrometers) is a critical

**TABLE 4 Membership on Regulatory Lists and Guideline Values for Chemicals Toxic by the Inhalation Route**

| CAS No. | RTECS No. | Chemical Name | DHS | OPCW | US HPV | EU HPVC | AEGL-3 10 min (ppm) | ERPG-3 (ppm) | TEEL-3 |
|---|---|---|---|---|---|---|---|---|---|
| 1752-30-3 | AL2338000 | Acetone thiosemicarbazide | | | | | | | 100 mg/m$^3$ |
| 107-02-8 | AS9660000 | Acrolein | • | | • | • | 6.2 | | |
| 2937-50-0 | LV7168000 | Allyl chloroformate | | | | | | | |
| 26842-43-3 | SF1435000 | 2-Amino-2,4-dimethylpentanenitrile | | | | | | | |
| 19355-69-2 | UD5155000 | 2-Aminoisobutyronitrile | | | • | | | | |
| 7647-18-9 | CA1722000 | Antimony pentachloride | | | | | | | 125 mg/m$^3$ |
| 7784-42-1 | CC9968000 | Arsine | • | | | | 0.91 | | |
| 98-87-3 | CW9716000 | Benzal chloride | | | • | • | | | 500 mg/m$^3$ |
| 100-44-7 | XW9324000 | Benzyl chloride | | | • | • | | 25 | |
| 55-91-4 | TC3948000 | Bis(1-methylethyl) phosphorofluoridic acid ester | | | | | | | 3.6 mg/m$^3$ |
| 111-44-4 | KX1708000 | Bis(2-chloroethyl) ether | | | • | | | | 100 ppm |
| 542-88-1 | KX1750000 | Bis(chloromethyl) ether | • | | | | | 0.5 | |
| 1461-23-0 | WR3458000 | Bromotributyltin | | | | | | | |
| 78-94-4 | EX4312000 | 3-Buten-2-one | | | | | | | 0.25 ppm |
| 4262-43-5 | CD1127000 | *t*-Butylarsine | | | | | | | |
| 75-87-6 | FW7714000 | Chloral | | | • | • | | | 250 mg/m$^3$ |
| 7782-50-5 | FX8204000 | Chlorine | • | | • | • | 50 | | |
| 7790-91-2 | FX8372000 | Chlorine trifluoride | • | | | | 84 | | |
| 13637-63-3 | FX8386000 | Chlorine pentafluoride | • | | | | | | 60 ppm |
| 107-20-0 | AB4928000 | Chloroacetaldehyde | | | | | | | 45 ppm |
| 79-11-8 | AH6664000 | Chloroacetic acid | | | • | • | | | 20 ppm |
| 78-95-5 | UG8134000 | Chloroacetone | | | • | | | | 7.5 ppm |
| 2315-36-8 | AC3934000 | 2-Chloro-*N,N*-diethylacetamide | | | | | | | |
| 1622-32-8 | KT2954000 | 2-Chloroethanesulfonyl chloride | | | | | | | 150 mg/m$^3$ |
| 107-07-3 | KU7910000 | 2-Chloroethanol | | | | • | | | 7 ppm |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 107-27-7 | PA7966000 | Chloroethyl mercury | | | | | | 2.5 mg/m$^3$ |
| 107-30-2 | KX3066000 | Chloromethyl methyl ether | • | | • | | 2.6 | |
| 106-48-9 | SM5446000 | *p*-Chlorophenol | | | | • | | 400 mg/m$^3$ |
| 104-12-1 | NZ5348000 | 4-Chlorophenyl isocyanate | | | | | | |
| 2909-38-8 | NZ5334000 | 3-Chlorophenyl isocyanate | | | | | | |
| 76-06-2 | PD3906000 | Chloropicrin | • | • | | | 1.5 | |
| 26447-14-3 | UD4312000 | Cresyl glycidyl ether | | | | • | | |
| 4170-30-3 | HB4606000 | Crotonaldehyde | • | | • | • | 44 | |
| 460-19-5 | HD6146000 | Cyanogen | • | | | | | 15 ppm |
| 675-14-9 | YC3052000 | Cyanuric fluoride | | | | | | 75 mg/m$^3$ |
| 17702-41-9 | HP5880000 | Decaborane | | | | | | 15 mg/m$^3$ |
| 56-18-8 | KC1302000 | 3,3′-Diaminodipropylamine | | | | | | |
| 105-83-9 | KC1316000 | 3,3′-Diamino-*N*-methyldipropylamine | | | | | | |
| 19287-45-7 | IB2688000 | Diborane | • | | | | 7.3 | |
| 534-07-6 | UG8862000 | 1,3-Dichloroacetone | | | | | | 2 mg/m$^3$ |
| 110-57-6 | EW9534000 | *trans*-1,4-Dichloro-2-butene | | | • | | | 7.5 ppm |
| 79-35-6 | LD6370000 | 1,1-Dichloro-2,2-difluoroethylene | | | | | | |
| 22591-21-5 | EW3934000 | 1,1-Dichloro-3,3-dimethyl-2-butanone | | | • | | | |
| 62-73-7 | TB3360000 | Dichlorvos | | | • | | | 100 ppm |
| 1464-53-5 | EU5824000 | 1,2:3,4-Diepoxybutane | | | | | | 10 ppm |
| 2524-04-1 | TB8148000 | Diethyl phosphorochloridothionate | | | • | • | | |
| 627-44-1 | PA8694000 | Diethylmercury | | | | | | 2.5 mg/m$^3$ |
| 627-54-3 | KT2996000 | Diethyltelluride | | | | | | |
| 28178-42-9 | CV6664000 | 2,6-Diisopropylphenyl isocyanate | | | | | | |
| 624-92-0 | KE2380000 | Dimethyl disulfide | | | • | • | | 250 |

(*continued overleaf*)

**TABLE 4 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | DHS | OPCW | US HPV | EU HPVC | AEGL-3 10 min (ppm) | ERPG-3 (ppm) | TEEL-3 |
|---|---|---|---|---|---|---|---|---|---|
| 2524-03-0 | TB8176000 | Dimethyl phosphorochloridothionate | | | • | • | | | 150 mg/m$^3$ |
| 77-78-1 | WX4466000 | Dimethyl sulfate | | | • | • | | | 7 ppm |
| 2867-47-2 | PC0994000 | 2-(Dimethylamino)ethyl methacrylate | | | • | • | | | |
| 2439-35-2 | AT2044000 | 2-(Dimethylamino)ethyl acrylate | | | • | • | | | |
| 24424-99-5 | ID4235000 | Di-*tert*-butyldicarbonate | | | | | | | |
| 106-91-2 | PC1022000 | 2,3-Epoxypropyl methacrylate | | | • | | | | |
| 541-41-3 | LV7252000 | Ethyl chloroformate | | | • | • | | | 10 ppm |
| 2941-64-2 | FQ5460000 | Ethyl chlorothioformate | | | • | | | | |
| 1498-64-2 | TB9142000 | *O*-Ethyl dichlorothiophosphate | | | | | | | |
| 1498-51-7 | TB9114000 | Ethyl phosphorodichloridate | | | • | | | | |
| 151-56-4 | LE0924000 | Ethylenimine | • | | • | • | 51 | | |
| 24468-13-1 | FQ5330000 | 2-Ethylhexyl chloroformate | | | • | • | | | |
| 7782-41-4 | LR2170000 | Fluorine | • | | | | 39 | | |
| 371-62-0 | KV2324000 | 2-Fluoroethanol | | | | | | | 1.25 ppm |
| 79-14-1 | MG6160000 | Glycolic acid | | | • | • | | | 0.75 mg/m$^3$ |
| 77-47-4 | HK1106000 | 1,2,3,4,5,5-Hexachloro-1,3-cyclopentadiene | | | • | • | | | 0.0179 ppm |
| 18406-41-2 | JW7266000 | Hexamethoxydisilylethane | | | | | | | |
| 74-90-8 | MY6300000 | Hydrogen cyanide | • | • | • | • | 27 | | |
| 7783-66-6 | NW2408000 | Iodine pentafluoride | • | | | | | | |
| 13463-40-6 | NX6062000 | Iron carbonyl | • | | • | • | 0.23 | | |
| 30674-80-7 | PC1218000 | 2-Isocyanatoethyl methacrylate | | | | | | 1 | |
| 10471-78-0 | | 2-Isopropenyl-2-oxazoline | | | | | | | |
| 68-11-1 | AJ4690000 | Mercaptoacetic acid | | | • | • | | | |
| 920-46-7 | PC1750000 | Methacryloyl chloride | | | | | | | 6 ppm |
| 558-25-8 | PD2016000 | Methanesulfonyl fluoride | | | | | | | 3.49 ppm |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 79-22-1 | FQ5362000 | Methyl carbonochloridate | • | | • | • | | | 4 ppm |
| 453-18-9 | AJ2058000 | Methyl fluoroacetate | | | | | | | 5 mg/m$^3$ |
| 421-20-5 | LU2884000 | Methyl fluorosulfate | | | | | | | 0.25 ppm |
| 60-34-4 | MX5208000 | Methyl hydrazine | • | | | | 16 | | |
| 624-83-9 | NZ5754000 | Methyl isocyanate | • | | • | | 1.2 | | |
| 676-97-1 | SZ9660000 | Methyl phosphonic dichloride | • | • | | | | | 15 mg/m$^3$ |
| 12108-13-3 | OV9576000 | 2-Methylcyclopentadienyl manganese tricarbonyl (MMT) | | | • | | | | 7.5 mg/m$^3$ |
| 35203-06-6 | CT7938000 | *N*-Methylene-6-ethyl-2-methylaniline | | | • | | | | |
| 140-76-1 | UZ4004000 | 2-Methyl-5-vinylpyridine | | | | | | | 40 mg/m$^3$ |
| 7786-34-7 | HB6104000 | Mevinphos | | | | | | | |
| 7783-77-9 | QK5418000 | Molybdenum hexafluoride | | | | | | | |
| 13463-39-3 | RB0042000 | Nickel carbonyl | • | | | | 0.46 | | |
| 10102-44-0 | RE9912000 | Nitrogen dioxide | | | | | 34 | | |
| 10544-72-6 | RF0322000 | Nitrogen tetroxide | • | | | • | | | 20 ppm |
| 62-75-9 | JF9856000 | *N*-Nitrosodimethylamine | | | | | | | 19 mg/m$^3$ |
| 57-57-8 | RX2352000 | 2-Oxetanone | | | | | | | 15 ppm |
| 10028-15-6 | SA2240000 | Ozone | | | | | | | 5 ppm |
| 376-53-4 | AV2842000 | Perfluoroadiponitrile | | | | | | | |
| 376-89-6 | ME8988000 | Perfluoroglutaronitrile | | | | | | | |
| 108-95-2 | SL9170000 | Phenol | | | • | • | | 200 | |
| 103-71-9 | CY2520000 | Phenyl isocyanate | | | | • | | | |
| 140-29-4 | AL4130000 | Phenylacetonitrile | | | | • | | | 30 mg/m$^3$ |
| 2687-12-9 | CW3633000 | 1-Phenyl-3-chloro-1-propene | | | | | | | |
| 638-21-1 | SY6930000 | Phenylphosphine | | | | | | | 15 ppm |
| 298-02-2 | TC1092000 | Phorate | | | | | | | 0.6 mg/m$^3$ |

(*continued overleaf*)

**TABLE 4 (*Continued*)**

| CAS No. | RTECS No. | Chemical Name | DHS | OPCW | US HPV | EU HPVC | AEGL-3 10 min (ppm) | ERPG-3 (ppm) | TEEL-3 |
|---|---|---|---|---|---|---|---|---|---|
| 7803-51-2 | SY4830000 | Phosphine | • | | | | 7.2 | | |
| 10025-87-3 | TD6832000 | Phosphorus oxychloride | • | • | • | • | 1.1 | | |
| 1185-09-7 | | 1,1,2,2-Tetrachloroethylsulfenyl chloride | | | | | | | |
| 5216-25-1 | XX3766000 | $\alpha,\alpha,\alpha$-*p*-Tetrachlorotoluene | | | • | • | | | |
| 78-00-2 | TU5040000 | Tetraethyl lead | | | • | • | | | 60 mg/m$^3$ |
| 597-64-8 | WR6118000 | Tetraethyltin | | | | | | | 50 mg/m$^3$ |
| 2778-42-9 | CV6454000 | Tetramethyl-*m*-xylylene diisocyanate | | | • | | | | |
| 509-14-8 | PD2464000 | Tetranitromethane | • | | | | 2.2 | | |
| 294-93-9 | XJ3220000 | 1,4,7,10-Tetraoxacyclododecane | | | | | | | |
| 108-98-5 | DB3304000 | Thiophenol | | | • | | | | 3.5 ppm |
| 3982-91-0 | XS4662000 | Thiophosphoryl chloride | | | | • | | | |
| 7646-78-8 | XU7588000 | Tin tetrachloride | | | • | • | | | 200 mg/m$^3$ |
| 7550-45-0 | XV3248000 | Titanium chloride | • | | | • | 38 | | |
| 584-84-9 | CX0518000 | 2,4-Toluene diisocyanate | • | | • | | 0.65 | | |
| 1321-38-6 | | Toluene diisocyanate (mixture of isomers) | | | | | | | |
| 921-03-9 | UH4522000 | Trichloroacetone | | | | | | | |
| 76-02-8 | AO0392000 | Trichloroacetyl chloride | | | | | | | 6 ppm |
| 594-42-3 | PC6468000 | Trichloromethanesulfenyl chloride | • | | • | • | 1.6 | | |
| 98-07-7 | XX3976000 | $\alpha,\alpha,\alpha$-Trichlorotoluene | | | • | • | | | 25 mg/m$^3$ |
| 998-30-1 | WI6062000 | Triethoxysilane | | | | | | | 115 ppm |
| 35037-73-1 | | Trifluormethoxyphenylisocyanate | | | | | | | |
| 98-16-8 | XX8456000 | $\alpha,\alpha,\alpha$-Trifluoro-*m*-toluidine | | | • | • | | | 150 mg/m$^3$ |
| 2487-90-3 | WI6188000 | Trimethoxysilane | | | • | | | 5 | |
| 141-59-3 | SF2044000 | 2,4,4-Trimethyl-2-pentanethiol | | | | | | | |
| 15112-89-7 | WI5754000 | Tris(dimethylamino)silane | | | | | | | |
| 100-43-6 | VA3262000 | 4-Vinylpyridine | | | • | | | | |

**TABLE 5 Membership on Regulatory Lists and Guideline Values for Chemicals Toxic by the Dermal Route**

| CAS No. | RTECS No. | Chemical Name | DHS | US HPV | EU HPVC | AEGL-3 10min ($mg/m^3$) | TEEL-3 |
|---|---|---|---|---|---|---|---|
| 75-86-5 | ON3024000 | Acetone cyanohydrin | • | • | • | 27 | |
| 309-00-2 | JD4970000 | Aldrin | | | | | 25 $mg/m^3$ |
| 107-11-9 | BA4858000 | Allylamine | • | | | 150 | |
| 28772-56-7 | GZ7154000 | Bromadiolone | | | | | 1 $mg/m^3$ |
| 95465-99-9 | TC3388000 | Cadusafos | | | | | |
| 8065-48-3 | TC8792000 | Demeton | | | | | 10 $mg/m^3$ |
| 814-49-3 | TB7994000 | Diethyl chlorophosphate | | | | | 8 $mg/m^3$ |
| 926-64-7 | AL3304000 | Dimethylaminoacetonitrile | | | | | |
| 1122-58-3 | UZ0910000 | 4-Dimethylaminopyridine | | | | | |
| 77-77-0 | KW9058000 | Divinyl sulfone | | | | | |
| 2104-64-5 | TA6020000 | Ethoxy-4-nitrophenoxy-phenylphosphine sulfide (EPN) | | | | | 5 $mg/m^3$ |
| 13194-48-4 | TC3416000 | Ethoprop | | | | | 50 $mg/m^3$ |
| 107-16-4 | AL3556000 | Glycolonitrile | | • | | | 4 ppm |
| 105-31-7 | MT5768000 | 1-Hexyn-3-ol | | | | | |
| 78-97-7 | ON2940000 | Lactonitrile | | • | | | 150 $mg/m^3$ |
| 950-10-7 | KF1386000 | Mephosfolan | | | | | 9 $mg/m^3$ |
| 126-98-7 | UI2520000 | Methacrylonitrile | • | | | 32 | |
| 453-18-9 | AJ2058000 | Methyl fluoroacetate | | | | | 5 $mg/m^3$ |
| 556-61-6 | PC6272000 | Methyl isocyanate | | • | | | 500 $mg/m^3$ |
| 3680-02-2 | WW8330000 | Methyl vinyl sulfone | | | | | |
| 7786-34-7 | HB6104000 | Mevinphos | | | | | 4 $mg/m^3$ |
| 5903-13-9 | AE0938000 | Nissol | | | | | |
| 311-45-5 | TB4298000 | Paraoxon | | | | | |
| 56-38-2 | TC9772000 | Parathion | | | • | | 10 $mg/m^3$ |
| 298-02-2 | TC1092000 | Phorate | | | | | 0.6 $mg/m^3$ |
| 947-02-4 | NP4102000 | Phosfolan | | | | | 9 $mg/m^3$ |
| 107-19-7 | UO7966000 | Propargyl alcohol | | • | • | | 60 ppm |
| 3689-24-5 | XS8050000 | Sulfotep | | | | | 10 $mg/m^3$ |
| 13071-79-9 | TC0350000 | Terbufos | | | | | 1 $mg/m^3$ |
| 2001-95-8 | YZ0098000 | Valinomycin | | | | | 2.5 $mg/m^3$ |
| 3984-22-3 | JX5551000 | 2-Vinyl-1,3-dioxolane | | | | | |

factor. In addition, deployed sensors must be sufficiently sensitive to ensure that the potentially exposed population is protected while not producing false alarms that may occur if the sensor is overly sensitive (in this context, if a chemical is correctly identified by a sensor, but the concentration is below the concern level, then the detect should be considered a false positive because it will produce an unnecessary alarm). Other performance parameters, including response times, power requirements, service life, maintenance requirements, calibration needs, size, and detection, range all factor into the suitability of a sensor or sensor suite for use in homeland security applications to alert the population to a potential attack.

While it is not the purpose of this article to identify specific sensor technologies or current capabilities, two examples of the above discussion are provided. Table 2 identifies nine isocyanates that meet the Hodge and Sterner/Hine and Jacobsen criteria (i.e. 3-chlorophenyl isocyanate, 4-chlorophenyl isocyanate, 2,6-diisopropylphenyl isocyanate, 2-isocyanatoethyl methacrylate, methyl isocyanate, phenyl isocyanate, tetramethyl-*m*-xylylene diisocyanate, trifluormethoxyphenylisocyanate, and toluene diisocyanate). As a chemical class, therefore, isocyanates appear to be highly extremely toxic and shows high priority for sensor development (eight of the nine isocyanates are in the extremely toxic range). In addition, isocyanates and specifically methyl isocyanate have been involved in industrial accidents that highlight their danger and ability to cause harm to a large population (e.g. the 1984 release of methyl isocyanate in Bhopal, India). Current commercially available sensor technologies that are capable of distinguishing isocyanates and provide quantification, however, appear to be limited to paper tape technologies (the paper technology also appears to be specifically limited to diisocyanates). There is therefore a critical need to develop all types of sensors that are capable of identifying and quantifying isocyanates and deployable in homeland security applications.

In contrast to the isocyanates, the four hydrides presented in Table 2 (arsine, diborane, decaborane, and phosphine) appear to have over 20 adequate commercial sensors that are able to detect three of the four chemicals (no commercial sensors were found for decaborane). These hydrides show $LC_{50}$ of 5.1–46 ppm for a 4-h exposure and all sensors have sensitivities that are well below the regulatory values for these chemicals, response times that are 1 min or less, and high selectivities.

In conclusion, there are more than 150 highly or extremely toxic commercially available compounds that were identified using a relatively restrictive definition of high and extreme toxicity. These compounds span a wide range of structures including isocyanates, halogens, acid chlorides, silanes, allylic/benzylic halides, nitrogen oxides, and phosphate esters. The diversity of chemical structures present a challenge for manufacturers to design suites of sensors that will be able to both identify and quantify these chemicals in homeland security applications. These include, for example, applications that will inform emergency responders and medical teams treating exposed populations about the identity of the chemical used so that the most effective medical countermeasures can be administered quickly. The identified chemicals additionally should provide an initial list that can be used to direct research efforts focused on developing new medical

countermeasures, developing new "greener" synthetic methods and replacement chemicals that will eliminate the need for these toxic chemicals, and developing more robust security methods to protect the public from the threat of a terrorist event using these chemicals.

## ACKNOWLEDGMENTS

The author wishes to thank Dr Richard Niemeier of the National Institute for Occupational Safety and Health, and Drs Patricia McGinnis and Peter McClure of Syracuse Research Corporation for enlightening discussions too numerous to count about toxicology and methods to identify toxic chemicals; Dr Benjamin Garrett of the Federal Bureau of Investigation for enlightening discussions about this article; Dr Lara Chappell for help in preparing some of the lists presented here, and Mr Brian Krafthefer of Honeywell International and Dr John Raymonda of CUBRC for discussions and information on sensors and sensor technology while developing a report for the National Technology Alliance (a US Government program).

## REFERENCES

1. Shea, D. A., and Gottron, F. (2004). *Small-scale Terrorist Attacks Using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons*, Congressional Research Service report for Congress. Order Code RL32391.
2. Karasik, T. (2002). *Toxic Warfare*, Rand Corporation. ISBN 0833032070. http://www.rand.org/publications/MR/MR1572/. September 21, 2005.
3. Cave, D., and Fadam, A. (2007). *The Reach of War; Iraq Insurgents Employ Chlorine in Bomb Attacks*, New York Times, New York, p. A1, 22 February 2007.
4. Partlow, J. (2007). *Baghdad Plan Has Elusive Targets: U.S. Patrols Still Unable to Tell Friend From Foe*, Washington Post, Washington, DC, p. A01, 26 February 2007.
5. Sharp, P. A. (2005). 1918 Flu and Responsible Science. *Science* **310**, 17.
6. Hauschild, V. D., and Bratt, G. M. (2005). Prioritizing industrial chemical hazards. *J. Toxicol. Environ. Health Part A* **68**, 857–876.
7. Hodge, H. C., and Sterner, J. H. (1949). Tabulation of toxicity classes. *Am. Ind. Hyg. Assoc. Q.* **10**, 93–96.
8. Hodge, H. C., and Sterner, J. H. (1956). Combined tabulation of toxicity classes. In W. S. Spector, Ed. *Handbook of Toxicology*, Vol. 1 – Acute Toxicities of Solids, Liquids and Gases to Laboratory Animals, W.B. Saunders Company, Philadelphia, PA.
9. Hine, C. H., and Jacobsen, N. W. (1954). Safe handling procedures for compounds developed by the petro-chemical industry. *Am. Ind. Hyg. Assoc. Q.* **15**, 141–144.
10. Department of Homeland Security (DHS) (2007). Chemical Facility Anti-Terrorism Standards. Interim Final Rule. *Fed. Regist.* **72**, 17687–17745.

# 2D-TO-3D FACE RECOGNITION SYSTEMS

MICHAEL I. MILLER, MARC VAILLANT, WILLIAM HOFFMAN, AND PAUL SCHUEPP
*Animetrics, Conway, New Hampshire*

## 1 INTELLIGENT VIDEO SYSTEMS

### 1.1 The Need for Intelligent Video Systems

Intelligent image and video interpretation systems of the future will be highly integrated with emergent video databases interacting with real-time access control and surveillance. The intelligent video surveillance software market, including video analysis, is experiencing meteoric growth. Airports, borders, ports, energy plants, historical buildings, monuments, manufacturing plants, retail establishments, and businesses all require access control and surveillance video solutions. Forrester predicts that 40% of businesses will need integrated security. The access control market is expected to reach nearly 14 billion dollars in 2009 [1]. Ultimately, these systems will integrate with and allow for the retrieval and cueing of the massive data stores such as the FBI's archives that contain both annotated as well as un-annotated video resources.

Figure 1 depicts an access control and video surveillance system handling the identities and monitoring dynamically the locations of individuals. According to ABI Research [2], the video surveillance market, already $13.5 billion as of 2006, will grow to $46 billion by 2012. The goal of spotting individuals of particular identities, and indexing and analyzing video archives is a fundamental challenge to the future of noncooperative FR. Solving the problem of dynamically identifying faces from live streaming or stored video will enable integrated, intelligent security solutions of the future.

The principal focus of this article is to describe the emerging 2D-to-3D technologies for extending FR systems historically applied to document verification and access control to the uncontrolled environments, which require pose and lighting invariant ID such as is required for tracking and recognizing faces in noncooperative surveillance and video applications.

### 1.2 The Barrier to Face

The surveillance environment has posed great challenges for FR technologies. Due to FR's nonintrusive nature, it has been pushed to the forefront as the biometric of choice. The International Civil Aviation Organization has embraced FR as its biometric standard. Yet, we must emphasize that, to date, the facial biometric has not adequately penetrated this marketplace. Presently, most systems do not incorporate FR biometrics. The major difficulty is that its advantage—its noninvasive, touch-free nature—is also its daunting challenge. Comparing it to fingerprint for the moment, imagine a "touch-free" fingerprint

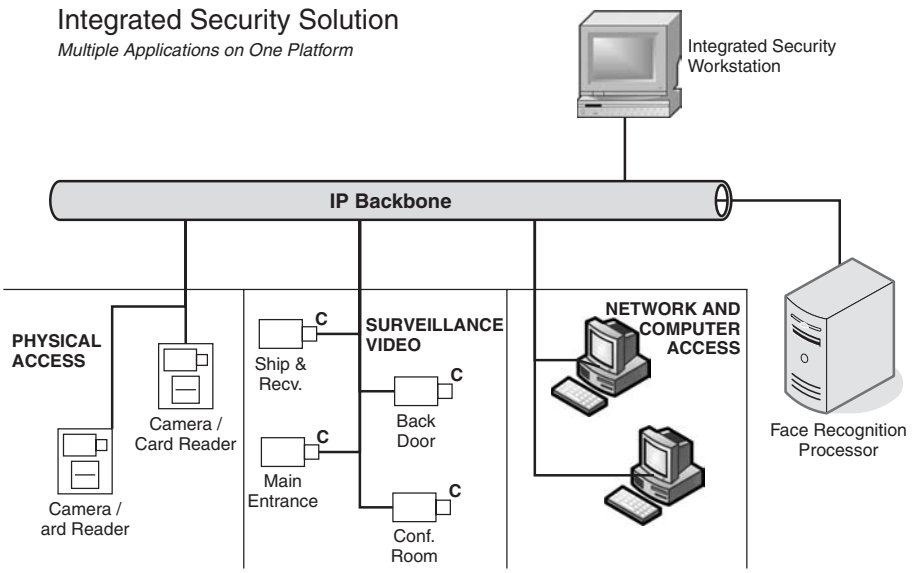



**FIGURE 1** An intelligent video surveillance system.

system in which any random medium—perspiration, oil, sand, grit—you name it, could be between the finger and the sensor. Alternatively, imagine that the finger could be at any "distance to the sensor", and could be occluded by gloves or bandages. Could we expect to deploy fingerprint biometrics in such conditions and require "constant performance independent of environmental variables"—hardly.

Such issues directly confound the successful deployment of FR technologies including the huge range of camera qualities (CCTV, Webcams, high resolution imagery, etc.), the infinite variety and schema of environmental lightings, arbitrary subject's positioning, facial hair, ornaments such as eyeglasses and jewelry, and complex backgrounds. The left column of Figure 2 depicts control photographs associated with access and document verification. The right column shows uncontrol photographs with the confounding variations of lighting and complex backgrounds. Figure 3 shows the results from the Facial Recognition Grand Challenge (FRGC) 2005 report [3] depicting the gap in performance between controlled and uncontrolled data by FR systems. FR performance is studied worldwide by examining false reject rate (FRR) or verification rate (1-FRR) as a function of false accept rate (FAR). The table lists out the FRRs in percentages at an FAR of 0.001 meaning the systems only accepted people incorrectly 1 out of 1000 times. The difference in median performance of participants is 60% between the control and uncontrol.

The confounding challenges of the uncontrolled environment resulting in this gap must be solved in order to make effective use of existing video recordings and to embark upon "action oriented" intelligent analytical systems that will provide next generation security methods. This article examines how 2D-to-3D technologies provide the crucial technological link from the historical application of controlled front facial recognition for access control and document verification to the intelligent systems of video surveillance.

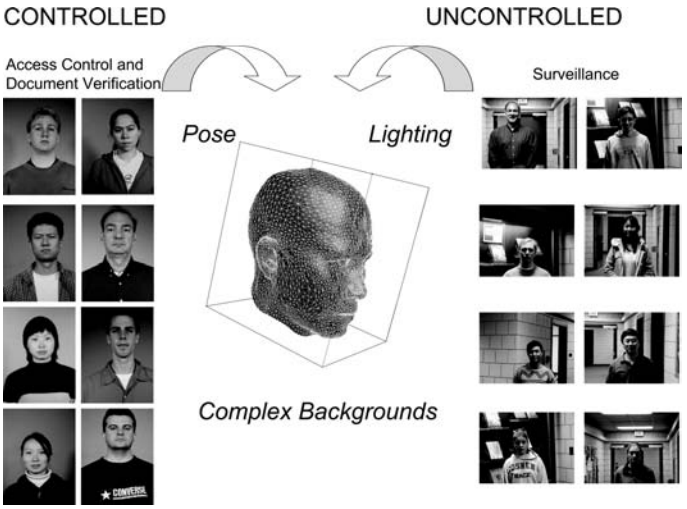



**FIGURE 2** Control photographs associated with access control and document verification (left column), and uncontrol photographs (right column) with the confounding variations.

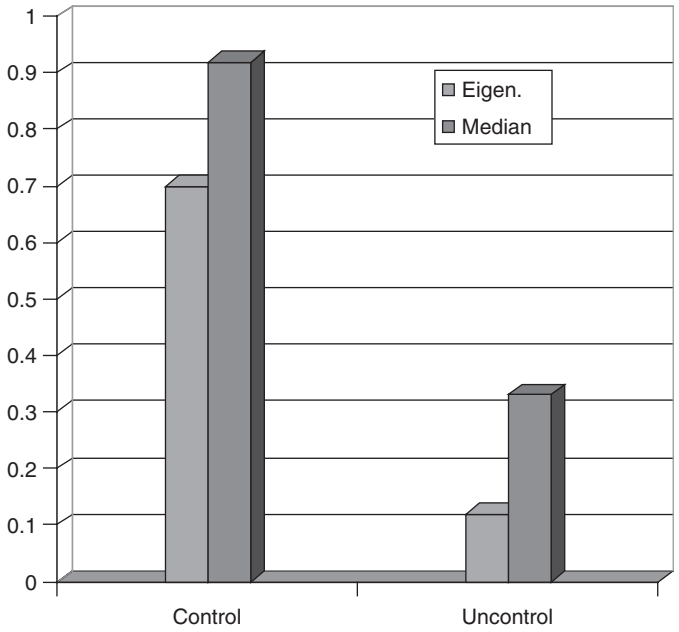



**FIGURE 3** Gap in Performance of FR Systems, June 2005 FRGC for Control versus Uncontrol.

### 1.3 2D-to-3D Bridges the Performance Gap for Intelligent Video Systems

FR today works well in a "controlled setting" where the camera-person interaction is cooperative, illumination is monitored, and backgrounds are simple and uncluttered. Facial identification systems and face trackers have been in use for at least a decade. Typically, facial identification systems comprise detection and identification systems based on

the manipulation of 2D likenesses of faces, which represent photometric and geometric variation robustly as manifest in the 2D likeness.

The "uncontrolled" surveillance environment introduces uncooperative subjects where facial pose is relatively arbitrary, lighting is infinitely variable, and backgrounds are arbitrarily complex. Next generation FR must accommodate these kinds of variations for successful transition from the controlled "checkpoint" access application to the "uncontrolled" surveillance video application. Purely 2D legacy FR technologies are limited in their deployment to the more controlled environments of access control and document verification. Figure 4 shows an example of 2D representational lattice model used in many of the legacy 2D FR systems.

Since 2D systems are limited to the manipulation of 2D geometric variations of in-plane geometric variation, they can be used for tracking and/or identification of faces while accommodating in-plane variation. However, they degrade as the target subjects are viewed out of plane. Since they rely on 2D likeness they cannot be robust to changes in both photometric and geometric variation, which depend on the 3D shape of the face and its interaction with variations in the external lighting illumination. 2D-to-3D technology provides a unified technological infrastructure for addressing all of these technical challenges, accommodating simultaneous high performance for imaging volumes at a physical access checkpoint (a more "controlled" scenario), as well as the "image at a distance" surveillance scenario.

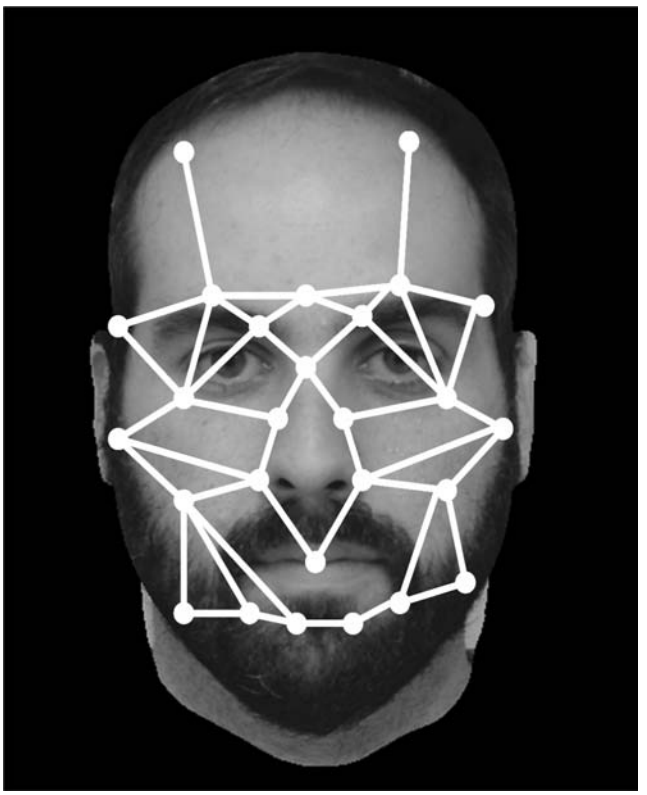


**FIGURE 4** 2D representation used in many legacy FR systems.

**FIGURE 5** The multiple views associated with the 2D-to-3D geometric model.

Figure 5 depicts a 3D geometric model and texture representing the 2D photograph resulting from the 2D-to-3D technology. It is the core 3D data structure generated from a 2D image that can provide the opportunity for FR systems to pass between controlled frontal interactions between camera probing and arbitrary positions of uncalibrated surveillance cameras. The 3D geometric data structures unify (i) the uncalibrated nature of camera position to viewer allowing for identification to be invariant to pose (position and rotation), (ii) the infinite variety of variations introduced via the external variability of the lighting world can be accommodated via the representation of the light field associated with the observed luminance on the geometry, and (iii) the dynamic coherence of video is directly encoded into the rigid motions associated with the 3D object representation.

## 2 COMPUTATIONAL ANATOMY AND DIFFEOMORPHISMS FOR 2D-TO-3D MODEL GENERATION

Geometry based 3D facial ID systems are robust to geometric variation of the pose of individual faces and efficiently detects and identifies faces from projective imagery such as measured by conventional video cameras. The key technological advance required for their application using conventional projective imaging cameras lies in a system to automatically determine the 3D geometry of a person's face with a finite set of images or photographs or through the analysis of a persistent set of images from video data. The technological term being used to describe the generation of 3D geometries from single or multiple projective planar images is *2D-to-3D geometric model generation*. Knowledge of the 3D geometry of a subject allows for automated understanding of variables, such as photometric and chromatic characteristics of the environment or particular video, occlusion compensation, and pose. The use of a structured 3D model allows for more finite analysis of human faces for expression analysis and direction of gaze for any pose.

### 2.1 Computational Anatomy

Advances in 2D-to-3D technologies championed by companies such as Animetrics are based on recent inventions in computational anatomy [4–9] that uses mathematical algorithms to compute equations of motion, which form the basis for biometrics in the study of the shape and form of biological structures. These equations generate metrically precise geometries, which can be used for recognition and identification purposes.

In computational anatomy, 3D analysis of deformable structures provides a natural platform for the merging of coarse features associated with detection of objects, proceeding to the finest scales associated with full recognition of objects via deformable

templates. The inference setting in computational anatomy has been almost exclusively in 3D; no special preference is given to particular poses of objects such as anatomical structures. The construction of geometric shapes is controlled by the dimension of the input imagery, composed of 0 (point), 1 (curves), 2 (surfaces), and 3 dimensional (volumes) imagery. The smoothness of the mappings is enforced through their control via the classic Eulerian ordinary differential equation for smooth flows of diffeomorphisms.

Computational anatomy studies anatomical manifolds and natural shapes in imagery using infinite dimensional diffeomorphisms, the natural extension of the finite dimensional matrix groups (rotation, translation, scale, and skew). Shapes and imagery are compared by calculating the diffeomorphisms on the image and volume coordinates $X \subset R^2, R^3$, which connect one shape to the other via the classical Eulerian flow equations:

$$\frac{d\phi_t}{dt} = v_t \circ (\phi_t) \tag{1}$$

The space of anatomical configurations is modeled as an orbit of one or more templates under the group action of diffeomorphisms:

$$I = \{I : I = I_{\text{temp}} \circ (\phi)\} \tag{2}$$

The unknown facial anatomical configurations are represented via observed imagery $I^D$ consisting of points, curves, surfaces, and subvolumes. They are compared by defining a registration distance; $d : \left(I, I^D\right) \mapsto R^+$. Then the mapping, or correspondence, between anatomical configurations is generated by solving the minimum energy flow connecting the two coordinate systems and measuring the length or square root energy:

$$\inf_{\dot{\phi} = v(\phi)} \int_0^1 \|v_t\|_V^2 \, dt \text{ such that } d\left(I_{\text{temp}} \circ (\phi_1^{-1}), I^D\right) = 0 \tag{3}$$

where $\|v_t\|_V^2$ measures the energy of the vector in the smooth Hilbert space $V$ with norm-square $\|v_t\|_V^2$. The computation performed becomes the matching of one object to the other by solving the minimization:

$$\inf_{\dot{\phi} = v(\phi)} \int_0^1 \|v_t\|_V^2 \, dt + \beta d^2 \left(I_{\text{temp}} \circ (\phi_1^{-1}), I^D\right) \tag{4}$$

where $\beta$ controls the weight. The mathematics of such equations are examined in our work [4–9].

Shown in Figure 6 are the results of using the Computational Anatomy equations for deforming one surface manifold to another [20, 21]. The top row shows the flow of surfaces under diffemorphisms solving equation 4 mapping the template surfaces (panel 1) onto the target surface (panel 6). The bottom row (dashed line) shows the histogram of vertex distances between the original template and target surfaces (after rigid registration). The solid line shows the distance between vertices after diffeomorphic correspondence.

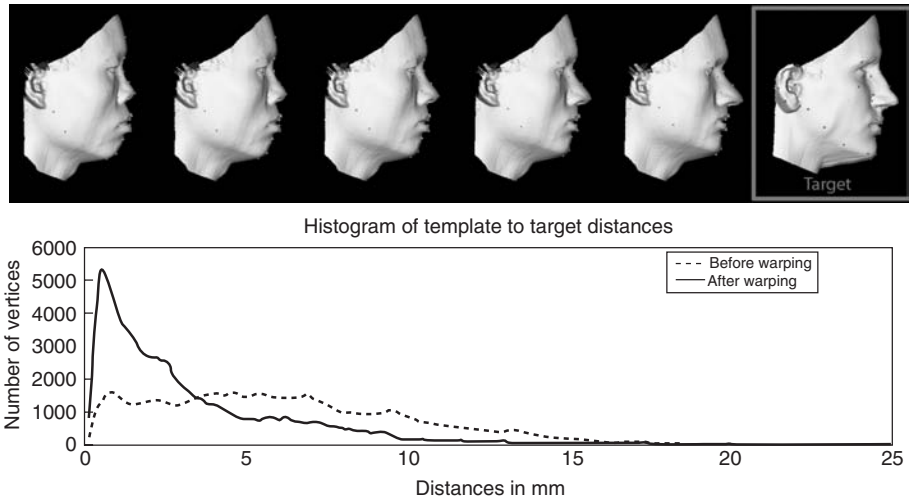



**FIGURE 6** Top row shows a flow of surfaces under diffeomorphisms solving Eq. (4) mapping the template surface (panel 1) onto the target surface (panel 6). Bottom row dashed line shows the histogram of vertex distances between the original template and target.

## 2.2 One and Two-View Geometry Generation

The work in computational anatomy for tracking and deformation of objects is generally in 3D, rather than manipulating motions in the image plane, working with the full Euclidean motions in space and time [10–14]. The power of such 3D approaches is that they are not limited to estimated translation and rotational motion in the image plane, therefore they imply complete invariance to full 3D pose, scale, and translation. The 2D-to-3D model geometry generation technology enables the conversion of the two-dimensional photo into a three-dimensional geometry, which can then be rotated and seen from any view. To accomplish this, the three-dimensional equations of geometric motion associated with biological shape are integrated with the projective equations of flat 2D imagery. Through proper integration of analysis of the two-dimensional images into features and a geometrically correct process for smooth deformation, it is possible to generate realistic, accurate, fully structured, and defined three-dimensional geometric models. They are combined with the projective equations accommodating

$$P : (x, y, z) \rightarrow p(x, y, z) = \left( \frac{\alpha_1 x}{z}, \frac{\alpha_2 y}{z} \right) \tag{5}$$

associated with video imagery. The core problem, at least for deformable objects, is to infer the flow of the dense volume representations of the 3D geometric objects from 2D projective imagery. The inference problem is to estimate the low-dimensional matrix group for tracking associated with rigid body dynamics, as well as work on high-dimensional transformations for tracking deformable motions (such as facial expressions), and to incorporate information obtained from projective geometry.

Diffeomorphic mapping of anatomical configuration leverages progress in computational anatomy [4–9] supported by the National Institutes of Health for the study of anatomical structure. The methods for constructing geometric models from 2D manifold representations of the face via triangulated graphs estimates diffeomorphic mapping

**FIGURE 7** The 2D-to-3D pipeline depicting the projective photograph (panel 1), face and eye detection, and two-dimensional feature analysis in the projective plane (panel 3), and the 3D geometric model generation in register and rotation with the given photograph (panel 4).

of templates onto pictures from single or multiple views of the individual invariant to camera pose. The algorithms incorporate both sparse and dense image information using mapping algorithms developed in computational anatomy. Figure 7 depicts the basic 2D-to-3D geometric model generation technology pipeline. The basic components required are two-dimensional image feature analysis (2DIFA), including eye detection and fiducial feature, and curve and subarea delineation. This is depicted in panel 3 of Figure 7. Once the 2DIFA is completed, the 3D model consisting of a triangulated mesh or quadrilateral representation is generated, which corresponds to the features generated with the photograph. The triangulated mesh model is depicted in panel 4 of Figure 7.

### 2.3 Statistical Validation of 2D-to-3D Model Generation

Figures 8, 9 and 10 show results from generating a single merged geometry from front and side view high resolution photographs. Shown in Figure 8 is an example of single textured geometry generated from a front and side view. The left column of Figure 8 shows the two input photographs; the middle column shows the textured model. The right column shows the front and side views of the single geometry. Figure 9 depicts a comparison of a subset of the anatomically defined fiducial marks superimposed over the manually defined features.

To examine the accuracy of the created mdoel geometries, 130 fiducial points have been attached to each model. These fiducial points are then compared to their positions in the image plane as viewed through the projective geometry. To illustrate, the points taken from the geometric model projected into the projective plane are shown in Figure 9. Superimposed over these model projected points are hand labelled manual points in the image plane for those features.

The geometric model generation produces a three-dimensional model from two-dimensional images by solving Eqs. 1–5. The accuracy of the models is essential for their accurate use for reorientation and normalization for improving identification rates with off-pose data. The geometric accuracy of the multiview geometry generation in the projective plane can be demonstrated via generation of hand featured databases with trained manual raters. Manual raters were trained to delimit in the order of 20 highly recognizable features in the projective imagery for front and 10 features for side view data. On each 3D model 130 fiducially identifiable points were defined on the surface of the volume. These points are the anatomical markers for the accuracy analysis. Each 3D model generated from the photographs was placed into the 3D space associated with the rigid motion generated for the solution of each variational problem.

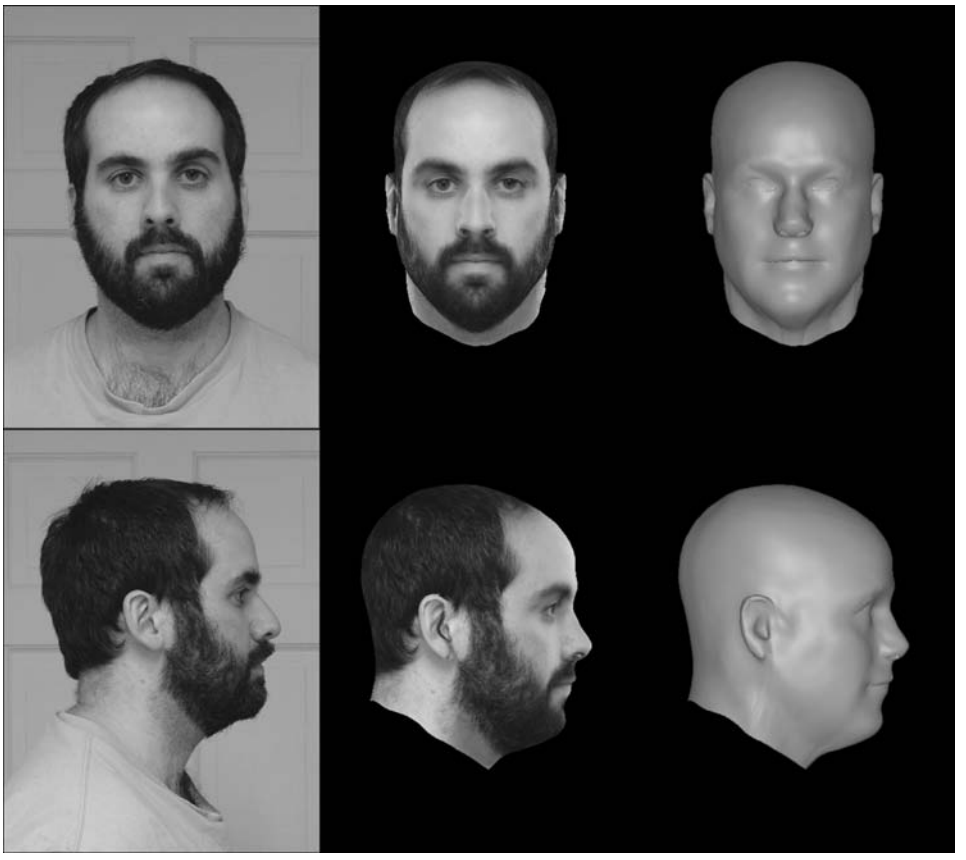


**FIGURE 8** An example of single textured geometry generated from a front and side view: column 1 shows two photographs, column 2 the textured geometry, and column 3 the geometry in grayscale.

Using the projective equation, the 130 fiducial markers were projected into the image plane (if not occluded) and were compared to each of a subset of the 40 identifiable features that were manually marked in the respective photograph. The root mean square error (RMSE) was calculated for each of the manually labeled photographs on which the experiment was performed. Figure 10 shows a single textured photograph with an associated 3D geometry which is in register with the photograph Each geometry consists of a triangulated mesh of vertices and triangles with associated normals. Every geometry generated has a minimum of 130 labeled features that are in correspondence with features which can be defined in the projective image plane.

### 2.4 Root Mean Squared Error on Controlled and Uncontrolled Imagery

Validations have been performed on several standard databases. Figure 11 shows the results of the face recognition grand challenge (FRGC) controlled and uncontrolled data validation. Upwards of 500 total geometries were generated from the control and uncontrol photographs using Eqs. 1–5. Each were hand featured for comparison for statistical validation. For the control data, the average RMSE (square root of the sum of the squares)

**FIGURE 9** The comparison of a subset of the anatomically defined fiducial marks superimposed over the manually defined features; green points are taken from the geometry, projected into the projective plane; red points show the manually defined features.

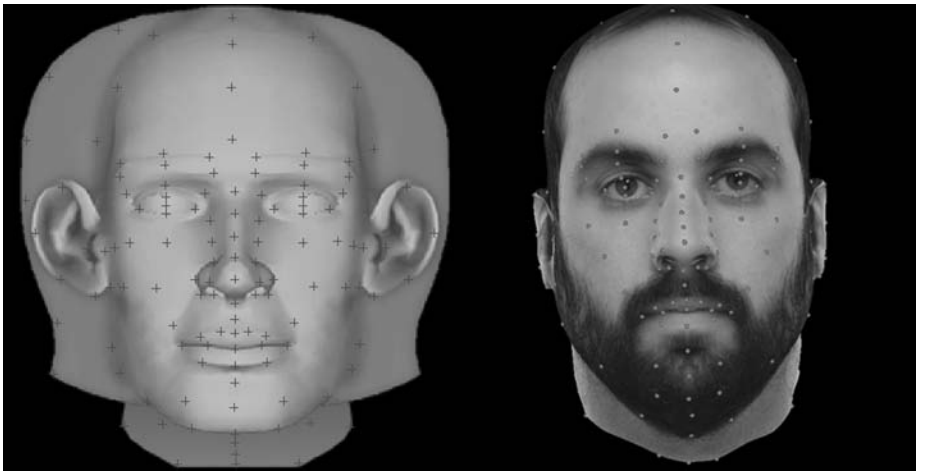


**FIGURE 10** Model with fiducial points.

averaged over the landmarked features is about 3.0 pixels on a standard 64 pixels between the eyes image corresponding to approximately 1/20 of an eye distance (Fig. 12 left panel). For the uncontrolled FRGC data, comprised of high resolution images taken with intentional variation in scale and in environments with a high degree of clutter and lighting variation, the RMSE increases to 3.8 pixel normalized to the standard 64 pixels between the eyes (Fig. 12 right panel).

Figure 12 shows a similar RMSE analysis performed as a function of pose angle on the $15^{\circ}$, $25^{\circ}$ and $40^{\circ}$ Facial Recognition Technology Database (FERET) imagery. In this

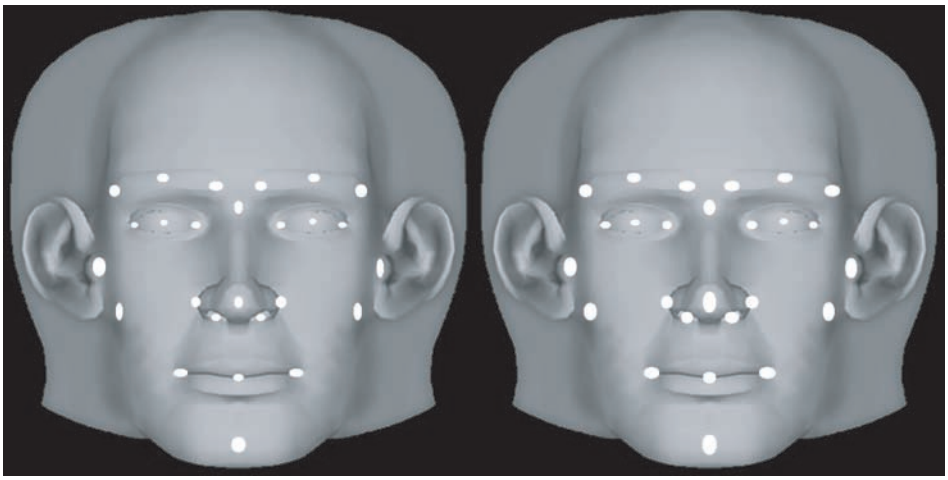


**FIGURE 11** RMSE ellipses for FRGC controlled data (left) and uncontrolled data (right) for the 2D-to-3D model geometry generation.

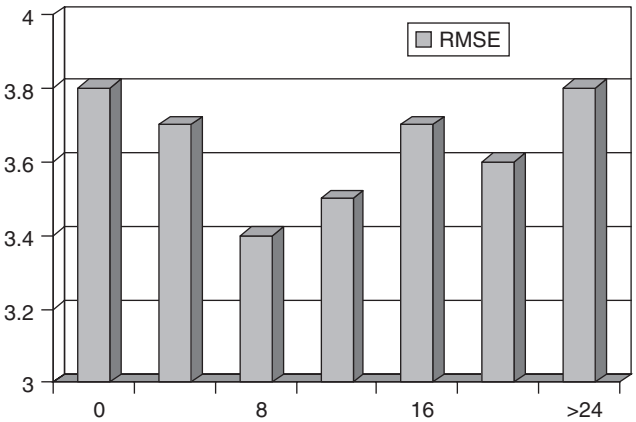



**FIGURE 12** RMSE for square root of the sum of squares for 2D-to-3D model generation for FERET indexed as a function of y-orientation of the head.

case, the RMSE accuracy was examined to understand whether accuracy of the model generation is linked to the particular y-pose (plotted along $x$-axis) under study.

### 2.5 Rigid Motion Reconstruction Accuracy

Clearly, the errors in model generation accuracy are determined by the quantitative ability to estimate the rigid motions accurately. Not only must the shape of the 3D model be generated to be compatible with the photographs, but the rotation angles of the model fitting the photographs must also be captured accurately as well. The reliability and stability of pose estimation results from the chain of events: head detection rate, 2DIFA, and fine pose estimation. Table 1 shows the results obtained for the control and uncontrol FRGC data. The deviations of the acquired poses are shown in the last three columns.

**TABLE 1 Deviation Results for Rotation Estimation of Controlled and Uncontrolled Imagery**

| Data set | Failure/ Degraded | Head Detection Success | Fine Pose Estimation Success (%) | X Std. Dev. | Y Std. Dev. | Z Std. Dev. |
|---|---|---|---|---|---|---|
| Controlled (608) | 0 | 100% | 100 | 4.38 | 1.71 | 0.66 |
| Uncontrolled (492/508) | 1 | 15 | 96.5/99.8 | 3.12 | 2.38 | 1.19 |

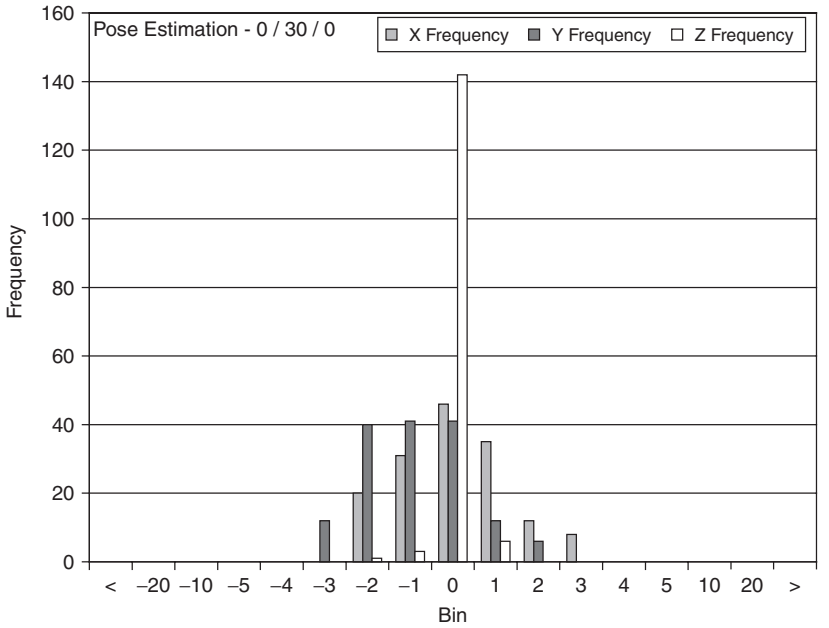



**FIGURE 13** Histogram of rotation errors for each axis, X-pitch (red), Y-yaw (green), Z-roll (blue) for simulated imagery generated at 30° Y-yaw. The histogram counts ($y$-axis) show the errors in degrees ($x$-axis) obtained from the rigid motion acquisition compared to the known 0, 30, 0 rigid motions of the models.

The accuracy or bias of the capture of the rigid motion can be estimated by generating photographs of known rotations and positions, from which these parameters are acquired by building the geometric models to fit the photographs. This was done for rigid motions of 30° in X-pitch, Y-yaw, and Z-roll directions.

Figure 13 shows the results of studying accuracy of rigid motions for 3D models generated at known orientation of 0°, 30°, 0° X-pitch, Y-yaw, Z-roll, respectively. The rigid motion algorithm was used to acquire the pitch, yaw, and roll from the simulated projective imagery generated from the models at the known orientations. Errors are shown via the histogram.

## 3 THE 2D-TO-3D TECHNOLOGY FOR PHOTOMETRIC REPRESENTATION

The arbitrary nature of lighting presents a significant confounding variable for FR systems. Lighting representation provides the opportunity to create data structures and

features, which provide conditions to make visual and computer-based recognition robust to arbitrary lighting conditions for identification purposes. The 3D model generated provides a direct substrate from which the luminance or lighting fields can be estimated as a "nuisance variable," essentially an extra data structure that itself represents the external environmental variables of the light sources and not the identity of the individual being imaged. 2D-to-3D technologies provide the opportunity to directly generate a 3D map of light intensities that are constructed in the infinite vector space of all lightings.

The 3D geometric models generated consist of two data structures: (i) the triangulated or quadrilateral mesh of vertices and normals representing the geometric positions of the 3D face and (ii) the second "texture" (determined by the albeido of the skin) data structure consisting of an red green blue (RGB) color vector $T(\cdot)$ at every vertex. Given any single or multiple set of photographs there is a lighting field—or luminance scalar field $L(\cdot)$—associated with each vertex of the model. The resulting observed photographs are the result of the interaction of the luminance field $L(\cdot)$ and the texture or albeido field $T(\cdot)$. To first order, the normal directions of the vertices of the models interact with the angular direction of the externals light source to determine the actual intensity of the measured image plane photometric values. The estimation of the luminance field $L(\cdot)$ directly removes the extra nuisance variation that is independent of the actual identity of the individuals—therefore is important for any ID system—and can be exploited for building photometrically invariant FR systems.

The 2D-to-3D solution represents the measured image $I(\cdot)$ in multiplicative form

$$I(x) = L(x)T(x), x \in FACE \tag{6}$$

where the texture or albeido is a vector field indexed over the face consisting of the RGB intensity vector. The multiplicative luminance field $L(\cdot)$ represents the interaction of the external lighting sphere with the surface of the face. The 3D geometry of the face provides the opportunity to manipulate the multiplicative luminance independently of the albeido or texture field, which is representative of the true identity of the individual.

Figure 14 shows examples illustrating the use of the 2D-to-3D technology to reconstruct both the geometric position and shape of the model as well as a luminance representation. The left column shows four example photographs. The middle column shows four luminance fields $L(\cdot)$ estimated on the reconstructed geometric model generated from the photographs in the left column. The right column shows the texture field resulting from the photographs on the left with the luminance resulting from variations in lighting removed.

## 4 2D-TO-3D GEOMETRIC MODEL NORMALIZATION

Once the 3D geometry is generated, it presents the opportunity to manipulate the projective imagery observed via conventional cameras. There are two kinds of normalization that are being actively pursued for FR technologies:

1. the first is geometric or pose normalization;
2. the second is termed *photometric normalization*.

We now examine each of these.

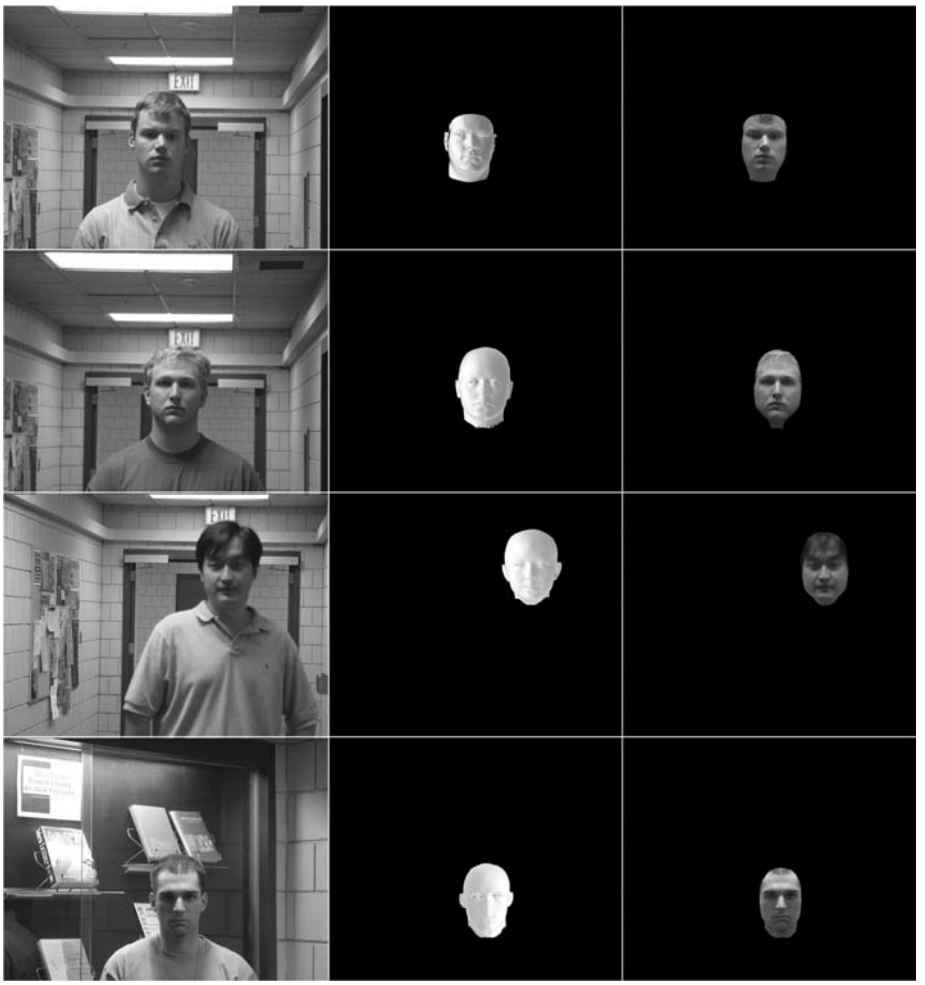


**FIGURE 14** Column 1 shows four examples of photographs, column 2 shows four luminance fields estimated on the model associated with the photographs on the left, and column 3 shows the texture field resulting from the photographs on the left with the luminance normalized.

### 4.1 2D-to-3D Geometric Normalization

Given the 3D geometry fitted into the projective imagery, it is possible to manipulate the projective image to arbitrary neutral coordinates. Figure 15 shows the geometric pose normalization. The incoming photograph is shown in panel 1 with the reconstructed geometry model shown in register in panel 2. The model is then geometrically normalized to any scale and orientation as shown in panel 3. Panel 4 shows the re-textured model at this neutral geometric position.

### 4.2 2D-to-3D Photometric Normalization

Given a 3D geometry fitted into the projective imagery, it is possible to manipulate the projective image to arbitrary photometric coordinates. Figure 16 shows the use of

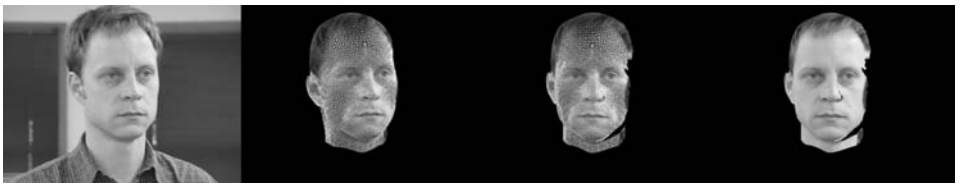


**FIGURE 15** Geometric pose normalization. The incoming photograph is shown in panel 1, the reconstructed geometry in register is shown in panel 2, the geometrically normalized model is shown in panel 3, and the re-textured model at neutral pose and lighting.

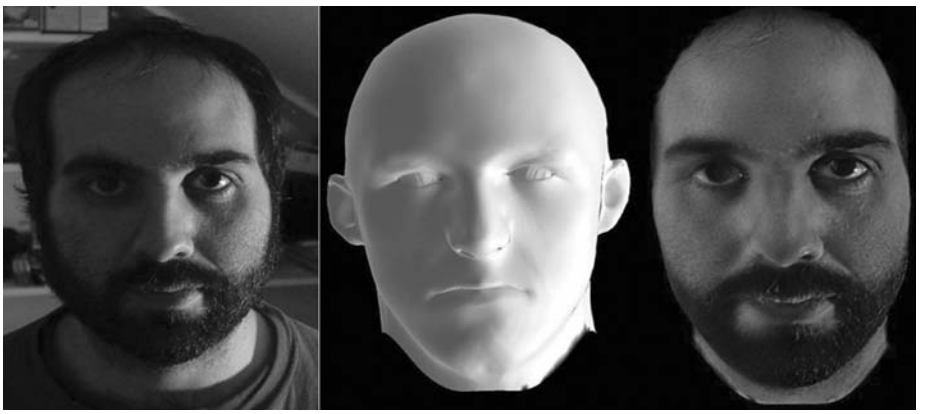


**FIGURE 16** Panel 1 shows the photograph, panel 2 shows the reconstructed luminance on the reconstructed model, panel 3 shows the luminance normalized textured model.

photometric normalization. Panel 1 shows the photograph, panel 2 shows the reconstructed luminance field $L(\cdot)$ on the reconstructed model coordinates, and panel 3 shows the luminance normalized texture reconstruction $T(\cdot)$ on the model coordinates. Note that in panel 3 the strong shadowing is removed in the normalized texture field $T(\cdot)$.

### 4.3 Boosting Facial Recognition Systems via 2D-to-3D Geometric Model Generation

The 2D-to-3D geometry technology can be used to build pose and lighting invariant FR systems thereby boosting conventional 2D ID system performance in difficult environments. Clearly, conventional 2D ID systems degrade in applications where pose and lighting are highly variable; 2D-to-3D model generation technology has been applied in several large experiments exploring the boosting of conventional Face ID via pose variability normalization. Figure 17 shows an illustration of 2D-to-3D technology for generating enhanced galleries in several large DoD tests [15]. Each row shows the application of the 2D-to-3D geometric model generation for enhancing the gallery of pictures to contain representations that accommodate variation of pose and or luminance.

Gallery enhancement provides the opportunity to enhance existing legacy FR systems. Figure 18 shows the results of 2D-to-3D gallery enhancement of one of the conventional high performance 2D FR systems currently in use worldwide attained in a Unisys test

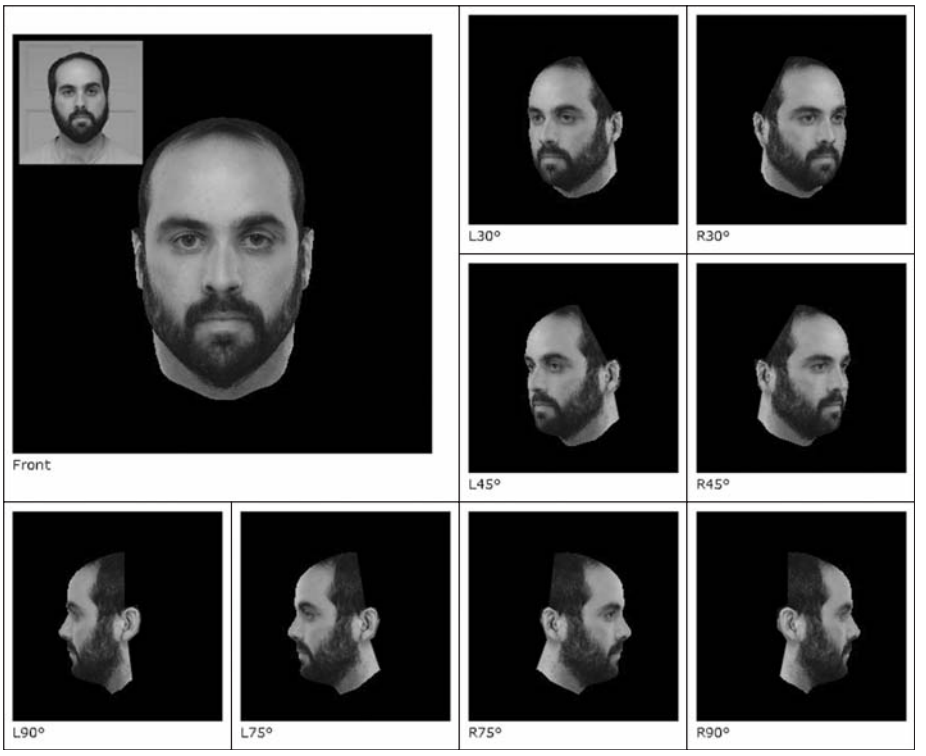



**FIGURE 17** The use of 2D-to-3D technology for gallery enhancement. Each row shows the application of the geometric model.

for the DoD [15, 16]. The figure shows two performance curves of the FRR attained as a function of the FAR plotted along the $x$-axis.

The red curve is the 2D conventional ID system using the 2D-to-3D technology for gallery enhancement [15]. Note that the FRR was monotonically reduced for any fixed FRR. The FRR of 0.02 is depicted by the dashed line, the FRR is reduced by a factor of 10 from 0.01 to 0.001 by the gallery enhancement (from black to red).

## 5 POSE AND LIGHTING INVARIANT FACIAL RECOGNITION SYSTEMS BASED ON 2D-TO-3D GEOMETRY GENERATION

### 5.1 2D-to-3D Enabled Frontal Pose-Invariant Facial Recognition Systems

Conventional high performing 2D systems degrade dramatically in their extension from application of the controlled physical access checkpoint setting to the surveillance setting. In the surveillance setting, most faces are captured with some degree of pose, or nonfrontal view of the face. FR systems built upon 2D-to-3D technology have built in pose invariance and provide the robustness to handle the challenges of video surveillance.

Figure 19 depicts a 2D-to-3D enabled FR ID system [17, 18]. As depicted, the 2D-to-3D technology automatically represents all poses and lightings and can manipulate

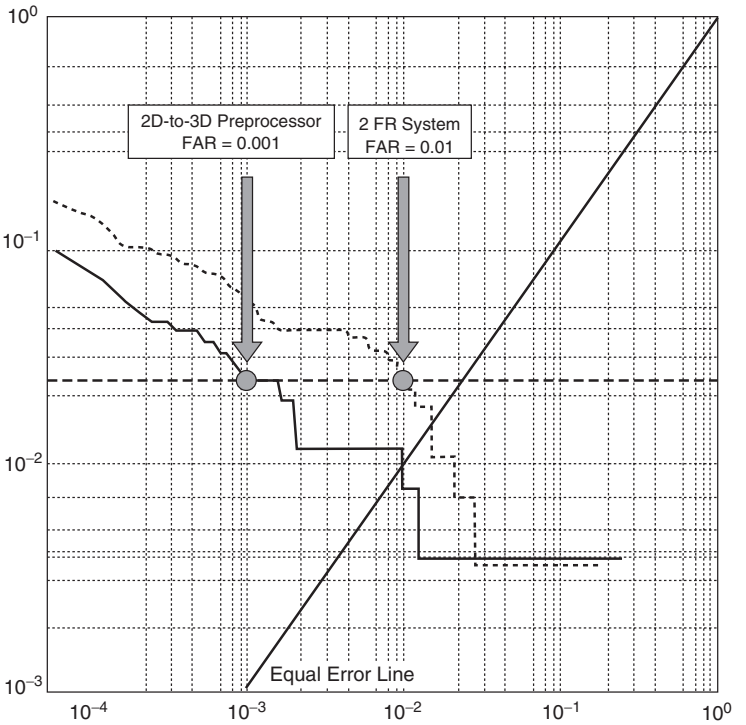



**FIGURE 18** The application of 2D-to-3D technology for gallery enhancement. The curves shows the performance of the ID system as a function of FRR versus FAR. The dashed curve is a 2D FR system; the solid curve is the 2D FR system running with the gallery enhancement.


**FIGURE 19** A pose and photometric invariant ID system [17, 18] built on 2D-to-3D technology is shown.

and normalize these faces to any pose position (i.e. neutral pose). This process is most beneficial for enhancing the face matching algorithm.

Figure 20 depicts the FR performance achievable with 2D-to-3D technologies when attempting to recognize face images at 40° of pose compared to that of a leading 2D conventional FR system [17]. The lower light solid shows a 94% verification rate at the FAR of 0.1%. This means that 94% of the time the system was able to recognize and verify that the person is who he says he is. At the same time, the system only accepted people incorrectly 1 out of 1000 times (i.e. the FAR). If the FAR is constrained to approximately 1 out of 100, or a 1% FAR, then it follows that the verification rate goes up.

Figure 20 shows a comparison of the 2D-to-3D enabled ID system (lower light solid) with a leading 2D conventional recognition system performance (bold solid). We see a dramatic improvement in performance. At a 95% verification rate of the 2D-to-3D technology, the conventional 2D system has degraded to 42%.

### 5.2 Lighting Invariant 2D-to-3D Facial Recognition Systems

The 3D models generated via the 2D-to-3D technologies support ID while accommodating lighting variation [18]. Figure 21 shows the FAR versus FRR performance for the FRGC uncontrol single gallery versus single probe experiment. The bold upper line shows performance for singleton galleries and the solid lower thin line for two in the gallery. In each case a single uncontrolled probe was compared to a single uncontrolled gallery

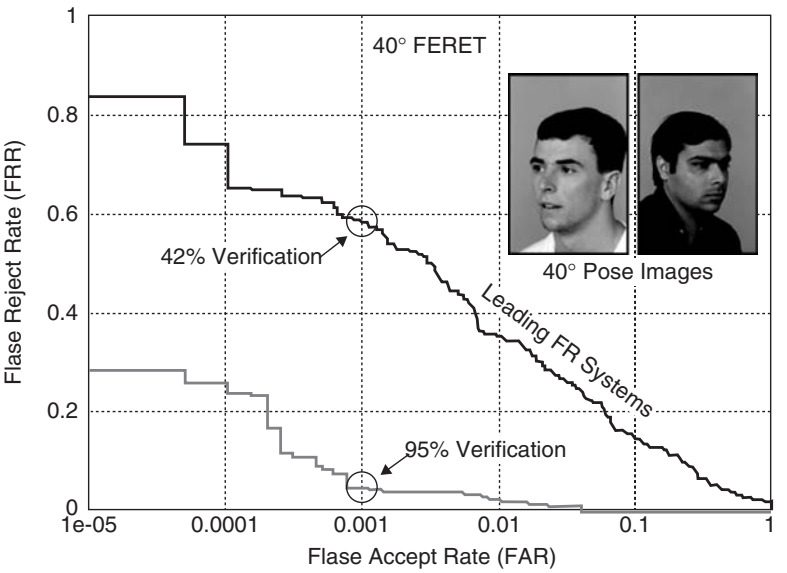



**FIGURE 20** Pose invariance performance of 2D-to-3D ID systems [17, 18]. FRR as a function of FAR performance for the 40° probe FERET database is shown. The gallery is populated with front images of the same individuals.

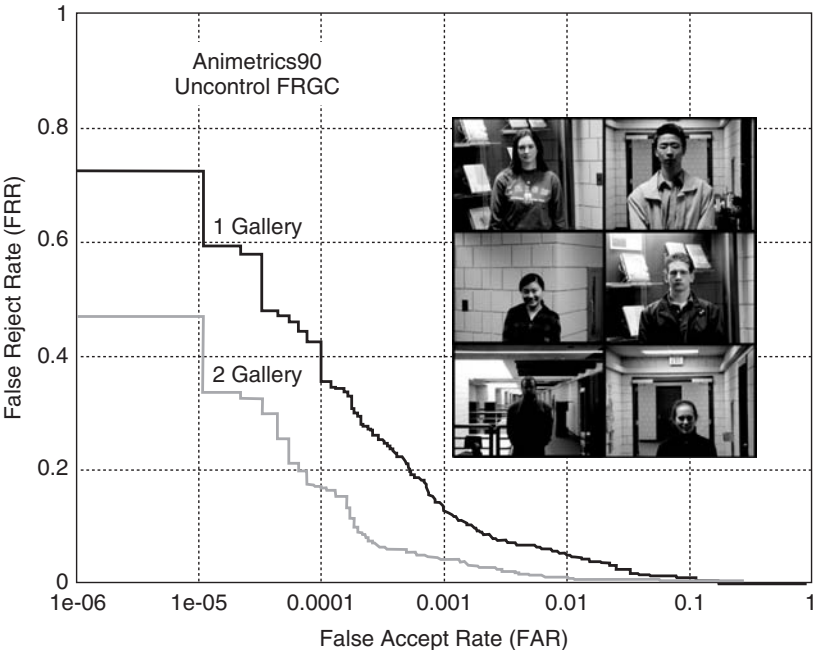



**FIGURE 21** FRR versus FAR performance of the FRGC uncontrol single gallery versus single probe experiment. The red line shows performance for singleton gallery and the green line for two in the gallery.

token representing each class. The green line shows the performance of the 2D-to-3D enabled ID system given two gallery tokens for each class.

### 5.3 2D-to-3D Full Profile Identification Systems

The 3D geometric model provides for the integration of the profile biometric with the nonprofile biometric. Essentially, the 3D generated model is the organizing coordinate system for fusing all of the texture (albeido) and geometric information into a single common coordinate system. Figure 22 depicts the features in profile of the 3D model.

Once a 2D-to-3D model geometry and texture field is registered with the model coordinate system, the ID system can exploit this and generate pose-invariant ID. Figure 23 shows the results of the construction of a full profile ID system using the 2D-to-3D geometric model generation [19].

## 6 CONCLUSION

This article presents newly emerging 2D-to-3D geometric model generation technologies and their application to "noncooperative" FR surveillance systems. We demonstrate that the generated 3D models can be used to unify pose-invariant and lighting invariant ID systems. Results are demonstrated to use these 2D-to-3D model generation technologies for enhancing 2D systems via "pose normalization" as well as "gallery enhancement".

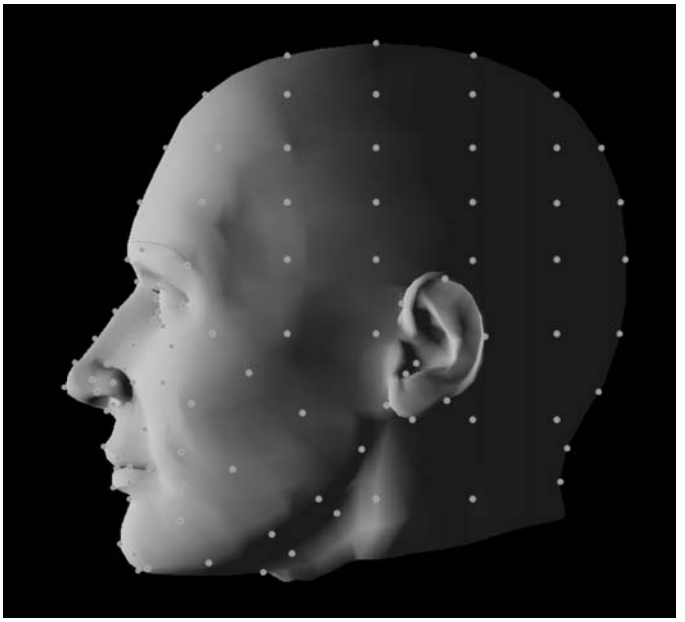


**FIGURE 22** The model fiducial features for profile.

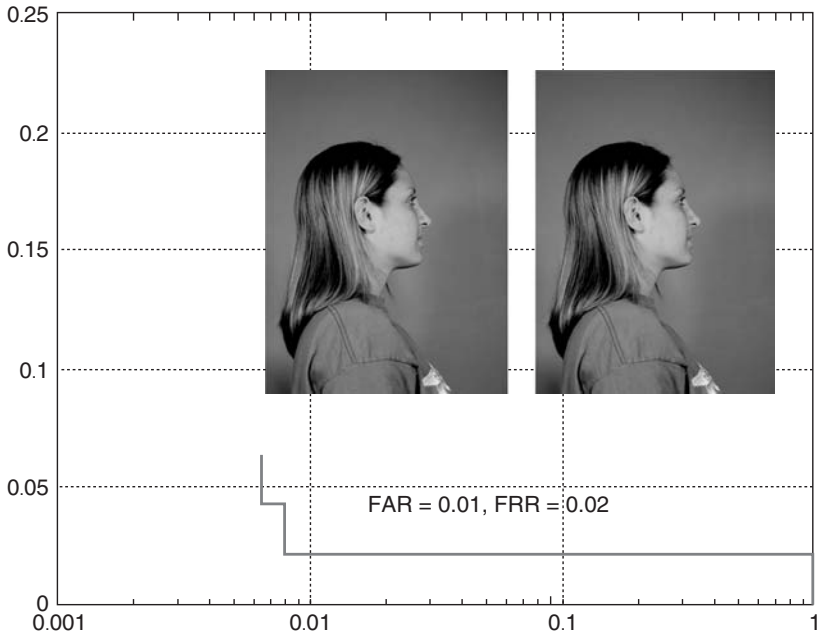



**FIGURE 23** The FRR as a function of FAR performance of the profile single gallery versus single probe experiment.

As well, we demonstrate FR systems, which incorporate these 3D coordinate systems for complete 180° ID.

## REFERENCES


1. Research and Consulting Outsourcing Services (RNCOS).. (2007). Access Control Technologies and Market Forecast World Over, p. 14.
2. ABI Research.. (2008). *Video Surveillance Systems: Explosive Market Growth and New Market Opportunities*, reference: http://www.securityinfowatch.com/article/printer.jsp?id=14777.
3. FRGC. (2005). Report http://www.frvt.org/FRGC/FRGC_Phillips_BC2005.pdf.
4. Grenander, U. and Miller, M. I. (1998). Computational anatomy: an emerging discipline. *Q. Appl. Math*. **56**, 617–694.
5. Dupuis, P., Grenander, U., and Miller, M. I. (1998). Variational problems on flows of diffeomorphisms for image matching. *Q. Appl. Math*. **56**, 587–600.
6. Miller, M. I., Banerjee, A., Christensen, G. E., Joshi, S. C., Khaneja, N., Grenander, U., and Matejic, L. (1997). Statistical methods in computational anatomy. *Stat. Methods Med. Res*. **6**, 267–299.
7. Miller, M. I. and Younes, L. (2001). Group actions, homeomorphisms, and matching: a general framework. *Int. J. Comput. Vision* **41**, 61–84.
8. Miller, M. I., Trouve, A., and Younes, L. (2002). On the metrics and Euler-Lagrange equations of computational anatomy. *Annu. Rev. Biomed. Eng*. **4**, 375–405.
9. Miller, M. I. (2004). Computational anatomy: shape, growth and atrophy comparison via diffeomorphisms. *NeuroImage* **23**, S19–S33.
10. Grenander, U. and Miller, M. I. (1994). Representations of knowledge in complex-systems. *J. Roy. Stat. Soc. B Met*. **56**, 549–603.
11. Grenander, U., Miller, M. I., and Srivastava, A. (1998). Hilbert-Schmidt lower bounds for estimators on matrix lie groups for ATR. *IEEE Trans. Pattern Anal. Mach. Intell*. **20**, 790–802.
12. Miller, M. I., Grenander, U., O'Sullivan, J. A., and Snyder, D. L. (1997). Automatic target recognition organized via jump-diffusion algorithms. *IEEE Trans. Image Process*. **6**, 157–174.
13. Miller, M. I., Srivastava, A., and Grenander, U. (1995). Conditional-mean estimation via jump-diffusion processes in multiple-target tracking recognition. *IEEE Trans. Signal Process*. **43**, 2678–2690.
14. Srivastava, A., Miller, M. I., and Grenander, U. (1997). Ergodic algorithms on special euclidean groups for ATR. *Progress in Systems and Control: Systems and Control in the Twenty-First Century*. Birkhauser, Boston, Vol. 22, pp. 327–350.
15. Mucke, E. (2004). *A Surveillance System Using Facial Image Enhancement with 3D Face Model Creation: Test Report to Unisys for Animetrics*, p. 12.
16. Miller, M. I., Vaillant, M., and Hoffamn, W. (2007). *SetPose: A 2D-to-3D Model Generation Technology for Library Enhancement and Pose Normalization*, http://www.animetrics.com/.
17. Miller, M. I., Vaillant, M., and Hoffamn, W. (2007). *Animetrics90: A 2D-to-3D Model Generation Pose invariant ID System*, http://www.animetrics.com/.
18. Miller, M. I., Vaillant, M., and Hoffamn, W. (2007). *Animetrics90: A 2D-to-3D Model Generation Lighting invariant ID System*, Whitepaper, http://www.animetrics.com/.
19. Miller, M. I., Vaillant, M., and Hoffamn, W. (2007). *Animetrics180: A 2D-to-3D Model Generation Full Profile ID System*, http://www.animetrics.com/.
20. Vaillant, M., and Glaunes, J. (2005). Surface matching via currents. *IPMI* **3565**, 381–392.
21. Vaillant, M., Qiu, A., Glaunes, J., and Miller, M. I. (2007). Diffeomorphic metric surface mapping in superior temporal gyrus. *Neuroimage*. **34**, 1149–1159.

# EYE AND IRIS SENSORS

RIDA HAMZA AND RAND WHILLOCK
*Honeywell International, Golden Valley, Minnesota*

## 1 BIOMETRICS FOR HUMAN IDENTIFICATION

Biometrics is the study of automated methods for recognizing humans based on intrinsic physical or behavioral traits. In information technology, biometric authentications refer to technologies that measure and analyze physical characteristics in humans for authentication purposes. Examples of physical characteristics used for identification include fingerprints, eye retinas and irises, facial patterns, and hand measurements. The use of biometric indicia for identification purposes requires a particular biometric factor to be unique for each individual, readily measureable, and invariant over time. Although many indicia have been proposed, fingerprints are perhaps the most familiar example of a successful biometric identification scheme. As is well known, no two fingerprints are the same, and they do not change except through injury or surgery. Identification through fingerprints suffers from the significant drawback of requiring physical contact with the person. No method exists for obtaining a fingerprint from a distance, nor does any such method appear likely.

Recently, the iris of the human eye has been used as a biometric indicator for identification. We have witnessed wide-scale deployment of iris technology across many product categories.

The human iris has extremely data-rich physical structures that are unique to each human being. Biomedical literature suggests that iris features are as unique and distinct as fingerprints. These extraordinary structures consist of a multitude of patterns—arching ligaments, furrows, ridges, crypts, rings, corona, freckles, zigzag collaret, and other distinctive features—that make discrimination possible even between genetic twins. Even in the same person, no two irises are identical in texture or detail. The unique and highly complex texture of the iris of every human eye is essentially stable over a person's life.

As an internal component of the eye, the iris is protected from the external environment; yet, it is easily visible even from yards away as a colored disk behind the clear protective window of the eye's cornea and surrounded by the white tissue of the eye.

Although the iris stretches and contracts to adjust the size of the pupil in response to light, its detailed texture remains largely unaltered. While analyzing an iris image, distortions in the texture can be readily reversed mathematically to extract and encode an iris signature that remains the same over a wide range of pupillary dilations. The richness, uniqueness, and immutability of iris texture, as well as its external visibility, make the iris suitable for automated and highly reliable personal identification. Using a video camera, registration and identification of the iris can be performed automatically and unobtrusively, without any physical contact. All these desirable properties make iris recognition technology a reliable personal identification tool.

## 2 SCIENTIFIC OVERVIEW OF IRIS TECHNOLOGY

### 2.1 Technology Basics

The basic iris recognition approach that is the backbone of most fielded systems converts a raw iris image into a numerical code that can be easily manipulated. An automated iris recognition system is made up of several major components, which include at minimum: iris localization that determines the boundaries of the iris with the pupil and the limbus, iris map feature extraction, encoding, and an enrollment matching process. Figure 1 illustrates typical process stages of a recognition system.

In image acquisition, a digital image of the eye may be obtained at multiple resolutions, eye orientations and transitions, under variant illumination conditions, and in noise-laden environments. Segmentation defines the most suitable, usable area of the iris for feature extraction and analysis. The eyelids, deep shadow, and specular reflection are eliminated in the segmentation process. The texture patterns within the iris region are then extracted. The feature extraction process captures the unique texture of the iris pattern, and the encoder compresses the information into an optimal representation to expedite a matching process. The matching process computes the number of bits matched in the iris barcode against multiple templates of barcodes in a database.

The most crucial stage of iris recognition is isolating the actual iris region in the digitized image; herein, we refer to this process as segmentation or localization. In most of the existing systems, the iris region is approximated by geometric models, that is, two circles or ellipses, to simplify the image processing segmentation of the iris and pupil. Prior to encoding the extracted iris patterns, a normalization process adjusts the width of the pupillary boundary to the limbus zone to bring uniformity in cross-matching iris images taken at different resolutions and in different lighting and acquisition environments.

As the eye image goes through various deformations, normalization can be a crucial step in the overall analysis. Normalization scales the extracted iris region cropped from the image to allow for a fair comparison with the database templates, which may have been extracted from regions of different sizes. Dimensional inconsistencies among the captured iris images can occur for many reasons. The iris stretches or contracts as the pupil dilates with varying levels of illumination. Varying distance of image capture and image orientation may occur because the camera or the subject's head tilts. There may

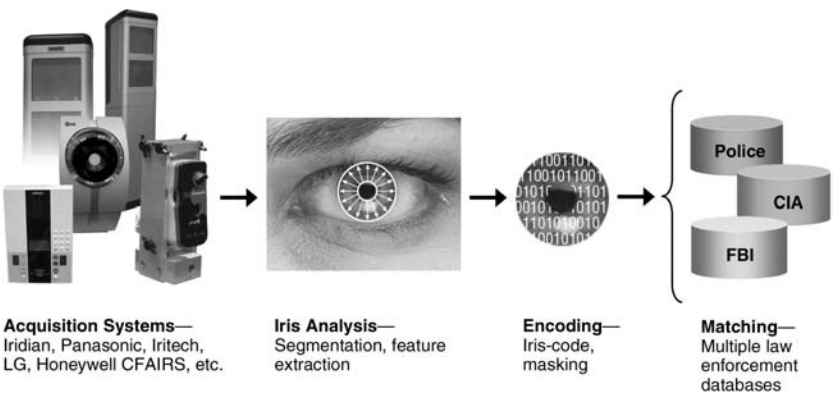



**FIGURE 1** Typical iris recognition processes.

be local rotation of the eye within the eye socket. The subject or the subject's face might not be aligned directly with the acquisition device.

After the data related to the iris is normalized, the iris data is encoded into small byte iris codes. The encoding scheme converts a polar image map of an iris into a numeric code that can be manipulated for either storage or comparison to other stored iris codes. The encoded iris data can be sent to a storage module, if for example, it is a sample to be stored for comparison to other encoded iris data. The encoded iris data can also be sent to a module that compares it to stored data and looks for a match or a probable match.

Image enhancement may be applied to minimize illumination artifacts, that is, nonuniform brightness that illuminates some areas more than others within the iris annular region. Reducing the illumination artifacts can improve the quality of subsequent encoding and feature extraction steps. Perspective orientation effects may be addressed before feature extraction; however, this process could add more computational burden on the system. Some recent active contour segmentation algorithms do not appear to require these preprocessing steps to extract accurate features of the iris.

### 2.2 Research Review

Although prototype systems and techniques were proposed in the early 1980s, it was not until the mid-1990s that autonomous iris recognition systems became a reality. The deployment of an autonomous iris recognition system by Iridian (a.k.a. IriScan) was made possible by the work of Prof. John Daugman of Cambridge University. (The foundation of the iris recognition is well described in [1]). Since then, researchers in the field have made great progress. Most of these developments were built around the original Daugman methodology, with some key contributions such as the work of Wildes using a Hough transform for detecting the iris boundaries and eyelid edges [2–4] and pattern matching on the basis of an isotropic band-pass decomposition derived from applying Laplacian-pyramid spatial filters to the image data. Iris boundary detection takes place in a two-step process: (i) the sclera boundaries are detected using gradient-based filters tuned in vertical orientations. (ii) eyelid edges are detected using gradient filters that are oriented toward the horizontal edges. The horizontal orientation is determined by eyelash position within the eye image, based on the assumption that the head is in an upright position.

Hough-based methods require threshold values for edge detection, which may result in the removal or omission of critical information (e.g. edge points), resulting in failure to detect the iris or pupil regions. The brute-force approach of Hough transform is also computationally intensive, so it may not be suitable for real-time applications. Furthermore, since it works on local spatial features, the method may fail where the image is subject to local noise in the eye image. These features can make Wildes' method computationally expensive, since it relies on image registration, rescaling, and matching.

The Daugman integro-differential operator [1] is considered a variation of the Hough transform, since it makes use of derivatives of the image and performs a search to find geometric information that determines spatial parameters identifying the circles of the iris and pupil. The operator searches for a maximum partial derivative of the image over a circular model as a function of the circular radius and center. The eyelids can be detected in a similar fashion by performing the integration over elliptic arcs to simulate the eyelid curvatures. The advantage of the Daugman operator over Hough is that it does not require threshold values because it is based on raw derivatives. However, some images that suffer from heavy local spatial noise (e.g. spread specular reflections along

the eye image, speckles due to digitization, and so forth) can raise challenges for both of these methods.

One approach to dealing with the eyelid occlusions that mask portions of the image makes use of linear fitting. However, the eyelid boundaries can be irregular and difficult to segment because of the presence of eyelashes. Another approach to this problem is to model the eyelids with parabolic curvatures and use the extracted configuration of model components to fine-tune the image intensity derivative information. This alternative can be computationally expensive, because it is based on edge detection and nonlinear curve fitting.

Boles' iris processing prototype builds a one-dimensional (1D) representation of the iris gray-level profiles [5]. An interesting aspect of this work is the ability of the wavelet transforms to eliminate the effect of glare due to reflection of the light source on the surface of the iris, a problem with which even some fielded devices cannot cope. Boles tested various resolutions and selected those that contained most of the energy from the iris signature and were thus least affected by noise.

Other research efforts have produced alternatives to the Daugman/Iridian (currently part of L-1 Identify solutions) methodology. Kim from Iritech introduced the multi-sector, multiresolution approach [6]. The work in [7] and [8] initiated the active contour concept and snake delineation for localization of nonideal irises. In the past few years, the authors have focused on developing new algorithms for a standoff iris recognition system [9–11].

The original foundation of the iris technology and algorithms derived from the information found in the literature do not address problems such as side looking eyes, self-occlusion, nonfrontal face images, etc. Recognition of this situation led to the development of alternative solutions [7, 10–12] to address the real-time operational requirements of a standoff iris recognition system. Unlike previous approaches, the conceptual design of [11, 13] employs an efficient and robust 1D fast segmentation approach built around our concept for the polar segmentation (POSE) system [9].

Major research activities have focused mainly on developing alternative segmentation and encoding techniques, while the conceptual design of an iris recognition system has not deviated much from the original foundation of the technology. In particular, the normalization step, the rubber sheet model proposed by Daugman [14] is the commonly used framework for mapping the deformed iris patterns because of dilation and occlusions into a fixed-size map. The technique maps each point in the Cartesian domain to its corresponding polar coordinates. The result is a fixed-size, unwrapped feature map. Some attempts have been made to base the normalization procedure using a Bayesian approach [15] by deriving a maximum *a posteriori* probability estimate of the relative deformation among iris patterns before the matching process.

Another unique iris pattern matching technique uses a 1D process that improves the encoding scheme for low-quality images. The technique proposes to provide a better representation of the iris features decomposed from the two-dimensional (2D) constructed iris polar representation map [16] when images are of poor quality, making it possible to process low-quality images that would be rejected by other methods. The matching process does not require circular shifting since the angular information is summed up and processed as a single score. Gaussian moments applied on a 1D representation of feature vectors have been advocated for the best representation of local features to indirectly quantify the variations in textures due to coronas, stripes, furrows, and so forth. 2D encoding schemes may appear to be much more reliable than a 1D process because of the inherited 2D relational spatial features in a 2D encoded signature. However, the 1D

method allows encoding a lower level of iris image quality that is more suitable for a quick search mode.

To provide accurate recognition or identification of individual irises, it is important to encode the most discriminating information present in the polar presentation of the extracted iris. For some applications, only the most significant features of the iris patterns may need to be encoded so that comparisons between two subjects can be made easily and quickly.

The encoding scheme generates a template of a few bits that captures the essence of an iris pattern. The extracted numeric code is then used to compare the pattern to stored codes. Encoding the iris signature includes applying an algorithm such as wavelet, Gabor filters, or other techniques, described below, to extract textural information from images. These methods process detailed patterns of the iris to produce a bit-wise template of bits of information and exclude some of the corrupt areas using masking within the iris pattern. Encoding filters are chosen to achieve the best recognition rate and preserve the unique iris pattern information in a template.

Wang et al. [17–19] use local intensity variation and local ordinary measures to define a new iris encoding scheme. The authors [20], generate quantized phasor information represented by more than two bits, which are prioritized with the most significant bits over the least significant bits when conducting matching. The merit of this scheme is that it provides a quick way to match subjects and also generates the most probable match instead of the best match when facing poor quality iris images and patterns. In addition, the different bits can be weighted differently for matching using any of the information divergence measures.

Encoding can include the actual encoding of the extracted features processed at different resolution levels using different means of filtering and processing. The encoding mechanism can involve applying one or more selected filters to the segmented iris images. Filters used by the state-of-the art techniques include wavelet and bank filters. The wavelet approach may have an advantage over traditional Fourier transform in that the frequency data is localized. Gabor filters may also be able to present a conjoint representation of the iris pattern in a spatial and frequency domain. Log-Gabor filtering is more reliable than Gabor filtering. In a different study [21, 22], Haar filters were shown to be comparable to Gabor filters. Haar-based filters can be implemented more easily than Gabor filters because we can take advantage of the fact that the integral image representation can be computed using only addition operations. Just recently, Monro et al. [8] introduced a new patch encoding by applying zero-crossings of a 1D discrete cosine transform (DCT) coefficients of overlapped angular patches. The approach was fielded as part of the Smart Sensors Ltd. offerings.

The increased interest in iris technology has prompted new research in the field. Articles on iris recognition technology blossomed in a range of publications from scientific journals to Business Week and biometrics magazines. The iris challenger evaluation (ICE) program for 2006 provides a good perspective of where iris technology stands in comparison to other biometrics. ICE 2006 established the first independent performance benchmark of available algorithms. Although the evaluation was limited to only a few participants, the results of both ICE 2005 and ICE 2006 hold great promise for iris technology with a false reject rate between 0.01 and 0.03 at a false acceptance rate of $10^{-3}$ [23]. Furthermore, the reported performance of these algorithms did not account for failure to acquire in accordance with image quality assessments. Thus, the false nonmatching rate (FNMR) versus false matching rate (FMR) can be better even on larger

datasets. The work reported in [24] probes the uniqueness and richness of iris patterns even when deployed to match billions of subjects—a requirement that must be met to deploy the technology for border control and the global war on terror.

## 3 CHALLENGES IN IRIS TECHNOLOGY

Iris recognition systems are designed to provide noninvasive and reliable authentication biometrics; however, current commercial solutions deployed by law enforcement and other agencies are impaired by stringent eye acquisition requirements, human intervention required for operation, difficulties with gazed irises, difficulties of encoding poorly captured iris images, lack of interoperability among different systems, and difficulties in processing moving irises.

### 3.1 Stringent Iris Acquisition Requirements

A major concern of existing iris recognition systems is that iris pattern features that uniquely identify humans can be easily missed because of the lack of accurate acquisition of the biometric data or to deviations in operational conditions. Iris recognition is a low-error, highly accurate method of retrieving biometric data, but iris scanning and iris image processing are costly and time consuming. Fingerprinting, facial patterns, and hand measurements have afforded lower cost, quicker solutions. During the past few years, iris recognition has matured sufficiently for it to compete economically with other biometric methods. Inconsistent iris image acquisition conditions, which most often occur in uncontrolled environments, sometimes cause systems to reject valid subjects or to validate imposters. In contrast, under controlled conditions, iris recognition has proven to be very effective. Iris recognition relies on more distinct features than other biometric techniques, and therefore provides a reliable solution by offering a much more discriminating biometric data set.

Constraints may be placed on the lighting levels, position of the scanned eye, and environmental temperature. These constraints can lead to a more accurate iris acquisition, but are not practical in many real world operations.

### 3.2 Standoff Iris Segmentation Challenges

Current iris recognition solutions do not reflect the full potential of the technology. The robustness of the standoff iris segmentation approach relies heavily on accurate iris segmentation techniques. Computing iris features requires a high quality segmentation process that focuses on the subject's iris and properly extracts its borders. Because iris segmentation is sensitive to the acquisition conditions, it is a very challenging problem. Most current devices try to maximize the segmentation accuracy by constraining the operation conditions and requiring subject cooperation. Such conditions make current iris systems unsuitable for many law enforcement, homeland security, and counterterrorism applications where subjects are not always cooperative.

When applied to nonconstrained operations, iris segmentation techniques of current systems fail miserably. Such operations may include subjects captured at variant ranges from the acquisition device or they may not align the eye directly with the imaging equipment. These conditions raise concerns about how to process accurate iris segmentation with limited operational constraints.

Most of the existing systems make use of first derivatives of image intensity to find edges to segment the borders of geometric models representing the boundaries of the iris. Other algorithms use costly procedures for geometric model searches throughout the digital image. Significant progress has mitigated this problem; however, these developments were mostly built around the original methodology, namely, circular/elliptical contour segmentation that has proven to be problematic in uncontrolled conditions. Some alternatives to the traditional approach still suffer similar issues with segmentation robustness under uncontrolled conditions.

A method that provides an iris recognition technique suited to moving "standoff" iris applications is much needed—that is, a system in unconstrained conditions that still provides an accurate, real-time result on the basis of the collected biometric data.

### 3.3 Lack of Database Cross Validation

Current commercial solutions for law enforcement and other agencies are impaired because data cannot be shared across systems. With the advent of economical successes of iris recognition devices, we have seen wide-scale deployment of the technology across many product categories. Most of these systems use a similar sequence of processes to that shown in Figure 1, but the diversity of implementation has resulted in multiple iris databases that lack interoperability. Cross validation with data collected by different law enforcement agencies is not supported, which decreases the usefulness of the iris as a robust biometric.

Some research effort has been made to build a common framework to enable interoperability and cross validation to implement a *versatile iris recognition tool* that is portable, interoperable, and deployable in any existing iris database maintained by law enforcement agencies. However, the market has not yet shown enough interest in support of such capabilities.

### 3.4 Image Quality Requirements and Preprocessing

Digital eye images are subject to a wide variety of distortions during acquisition, transmission, and reproduction. These distortions can degrade iris recognition performance. Performance of an iris recognition system depends heavily on a successful outcome at each stage of the iris recognition process. In turn, each stage may depend on the quality of the captured iris image. An objective image quality metric can play a variety of roles throughout iris processing. Many artifacts may affect one or more of these processes.

Under ideal conditions, a perfectly captured iris pattern clearly displays the texture of an iris that can be represented in a unique iris barcode. Many factors such as eye closure, obscuration, an off-angle eye, occlusions, imperfect acquisition with electronic noise, nonuniform illumination, different sensor wavelength sensitivity, pupil dilation, and specular light reflection can cause the captured iris map to be far from ideal. In particular, smearing, blurring, defocus, and poor resolution can result in poor quality images and can have a negative impact on iris segmentation and feature extraction and encoding. Encoding a blurry image may result in multiple false acceptances. It is crucial to avoid these poor quality images—especially during enrollment when false acceptance matches can occur because of smeared features and false rejection matches can occur because of obscuration, occlusions, or drastic dilation and gazing.

To counter this vulnerability, current systems have attempted to define quantitative measures that can automatically assess the quality of iris images before processing and

develop an appropriate set of quantitative iris image quality metrics (IIQMs). The IIQMs are defined relative to image features based on acquisition performance. The quality of the image should correlate well with subjective iris processes. The IIQMs can be integrated into the preprocessing procedure to assess the quality of the iris image before the iris recognition process is initiated. On the basis of an evaluation with these metrics, the operator can accept the input image, reconfigure the processing to deal with degradations, or request a new capture of the iris.

## 4 FUTURE RESEARCH DIRECTIONS

Future research needs to bring iris recognition systems up to a more mature technology level capable of making iris biometrics a reliable, evidence-based tool while addressing the pitfalls of current iris devices.

### 4.1 Critical Needs Analysis

New research efforts are mainly directed toward solving the critical needs of the security market and to extending the technology to noncooperative standoff applications. Such applications are becoming crucial for law enforcement agencies in support of counterterrorism practices. The advancement of standoff iris recognition research presents opportunities to implement new systems well suited to high-security access control or "at-a-distance biometrics" applications with little or no constraints on subject positioning or orientation. An iris recognition operation may include subjects captured at various ranges from the acquisition device or include subjects who may not have an eye directly aligned with the imaging equipment. For such applications, it can be difficult to implement the level of control required by most of the existing systems for reliable iris recognition operations. Some emerging technical approaches to standoff iris recognition cope with asymmetry in acquired iris imaging, allowing systems to operate under uncontrolled operations as long as some of the iris annular is visible.

Recent contributions to the field are directed toward assessment of the quality of an eye image in real-time as a quality control procedure. These techniques may allow poor image acquisition to be corrected through recapture and facilitate the acquisition of a best possible image within the capture time window configured in the system. This acquisition results in a process for providing more good quality iris images to improve iris identification accuracy and the integrity of iris recognition systems. An objective of these advancements is to define rules to assess iris image quality and use these rules as discriminators for recovering information from poor quality iris images or reconfiguring the processing steps based on the image quality assessment.

Other research efforts focus primarily on developing tools that will enable interoperability among systems, making it possible to recognize enrolled irises from any commercially available acquisition device. The application of iris technologies that are more interoperable will make the technology more useful for law enforcement and broaden the use of the iris as a biometric.

### 4.2 Emerging Technical Approaches

In general, emerging techniques are focused on building a common framework to enable system interoperability, portability, and deployment in adverse environments

with noncooperative subjects. Most recent research activities deviate from the original theme of the iris recognition approach based on regular linear fitting models, because of its limitations in handling noncooperative subjects. One prominent technical approach is the application of active contour techniques to model a more complex view of the iris at an off-angle. The following paragraphs describe three emerging concepts.

***4.2.1 Standoff Iris Recognition System.*** Very few techniques address the true nature of iris irregularity in iris segmentation [7, 9, 12]. Apart from estimating the iris borders, the segmentation routine should also detect occlusions due to eyelashes, reflections, and eyelids. The authors have developed a standoff iris recognition system [13] and an algorithmic segmentation approach that address the real-time operational requirements of a standoff iris recognition system. The system can be regarded as "hands-off" or automatic iris processing. Consistent with the principles of noninvasive biometrics, this new segmentation technique is introduced along with a new encoding scheme resulting in an improved biometric algorithm. The feature extraction is based on a simplified polar segmentation (POSE) using a process with low computational load. The approach has proven useful for performing iris recognition under suboptimal image acquisition conditions. It is well suited for iris segmentation that detects all boundaries (inner, outer, eyelid and sclera, etc.) of the image iris simultaneously. This technical approach provides accurate segmentation and identifies good iris patterns under uncontrolled imaging conditions as illustrated in Figure 2.

Unlike existing art, which is often based on the brute force of a Hough transform, iterative active contour, or fitting model based on partial derivatives to tailor the iris edges to circular or regular matching templates, POSE employs an efficient and robust enhancement approach built around a POSE technique [5]. POSE differs from state-of-the art techniques in that it conducts a 1D segmentation process in the polar domain, replaces the exhaustive search for geometric models, and avoids the use of costly edge detection and curve fitting by executing a straightforward peak search on 1D signals. The technique can detect boundaries of the iris borders of any regular or irregular shape that might be due to eye gazing or suboptimal image acquisition conditions.

Recent improvements made to the POSE segmentation technique have resulted in a more robust and computationally efficient real-time iris recognition prototype [13]. The new POSE system takes the analysis of edges into the polar domain at an earlier stage

**FIGURE 2** Honeywell POSE performance under uncontrolled imaging conditions.

and uses local patterns and an enhanced version of the original POSE proposition to detect iris features. The process is still based on mapping a located eye image into a polar domain with respect to a centered point in the pupil of the eye image. The centered point—not necessarily the exact center of the pupil—can be identified within the pupil region using any of a number of common eye finding algorithms. Once the inner and outer borders of an iris are estimated, the iris region can be extracted, normalized, and mapped into a compressed format where a barcode is generated for processing or database storage.

The POSE approach makes it possible to detect the irregular shape of iris curves using additional rules related to the nature of curve patterns and symmetry. This approach extracts the iris signature using a guided analysis to correctly normalize the stretching and compression of the patterns and bring uniformity into the interpretation of the patterns. The symmetry properties are used to cluster the edge points into at least two categories: (i) sclera and iris boundary points and (ii) iris and eyelid boundary points to be analyzed differently. This analysis helps to cluster obscured pixels and affected areas and weighs them with low scores or masks them out of the analysis. These weights are taken into consideration when patterns are matched against multiple codes in a database and are given weights based on the pattern visibility and exposure to the camera system during acquisition. This process assures that questionable data, such as near possible occlusions, is not weighted as highly as known good information.

Another standoff iris segmentation approach that addresses the real nature of non-ideal irises was introduced in [7]. Ross and Shah have formulated a snake segmentation approach that is based on geodesic active contours (GAC). The motive for using GAC models is to obviate the predication of the boundary limits, which in turn provides a better fit for tightened boundary around the iris borders. An anisotropic diffusion procedure is part of the solution for processing intraregion smoothing while inhibiting interregion smoothing of the iris rubber sheet image. The segmentation approach outlines the iris boundaries and the edges of the eyelid simultaneously to isolate the iris texture from its surroundings.

With the exception of the mandate for iteration in the technique, both propositions (i.e. POSE in [13] and [7]) should lead to similar solutions that can elicit the irregular limbic boundary of the iris (far from the circles and ellipses as previously modeled) to process smooth iris features. The reliability of the reaction of the latter technique to some challenging cases, for example, splitting and merging iris boundaries during evolution when processing an iris with more pronounced localized features (or iris images with heavy reflections) is yet to be proved. These artifacts can affect the stopping criteria before the segmentation reaches the actual iris boundaries—a common drawback of any snake approach when dealing with local minima.

***4.2.2 Invariant Radial Encoding Scheme.*** The major downfall of earlier segmentation techniques is that the systems focus on segmentation of the inner and outer border of the iris to normalize the iris scaling and allow for cross matching of all records of iris barcodes. Many factors, including eyelid and eyelash occlusions that obscure the outer iris border and poor illumination that makes it difficult to distinguish from the sclera, may make it impossible to map the outer border accurately. Inaccurate mapping results in incorrect segmentation of the iris, which in turn negatively impacts the rest of the biometric recognition process. In addition, when applied to uncontrolled conditions, these segmentation techniques deteriorate for nonfrontal eyes. Such conditions may include

subjects captured at various ranges and orientations from the acquisition device or subjects who may not have their eye directly aligned with the imaging equipment.

A new encoding scheme has been designed to avoid these pitfalls. The scheme uses a new approach to extract dyadic local iris features to account for the dilation nature of irises with low computational load. It does not rely on accurate segmentation of the outer bounds of the iris region, which is essential in prior techniques; rather, it relies on the identification of peaks and valleys in the iris contrast (i.e. the noticeable points of change in contrast in the iris). Regardless of a chosen filter, the encoding scheme does not use the exact location of the occurrence of peaks detected in the iris, but uses the magnitude variation of detected peaks relative to a referenced first peak. Since this algorithm does not rely on the exact location of pattern peaks and valleys, it does not require accurate segmentation of the outer boundary of the iris, which also eliminates the need for a normalization process.

Similar to previous approaches, to account for rotational inconsistencies and imaging misalignment when the information measure of two templates is calculated, one template is shifted left and right bit-wise (along the angular axis) and a number of distance measures are calculated from successive shifts. This bit-wise shifting in the angular direction corresponds to rotation of the original iris region by an angular resolution unit. From the calculated distance measures, only the lowest value is considered to be the best matching score of two templates.

***4.2.3 Iris on the Move®.*** As stated above, one of the major benefits of iris technology is its noninvasive nature, which makes it practical to analyze subject identity without any physical contact. However, most fielded iris devices failed to meet this criterion, limiting their usefulness for security applications and border controls. Iris on the Move from Sarnoff Corporation [25] was the first to reinforce the noninvasiveness benefit and has worked toward an actual development to recognize an iris at a distance. Although the recognition algorithms and processes are based on previous techniques (e.g. Daugman and others), the system uses a conceptual design that takes advantage of advancements in optics and system engineering to capture an iris passing through a gate. The system is a ground-breaking iris recognition system for moving subjects and has opened the door for other players to contribute to the field. Other emerging techniques are leveraging the advancements in optics and iris algorithmic approaches to build cutting-edge iris recognition systems capable of capturing and processing an iris at farther distances—making the technology more practical for law enforcement applications.

## 5 CONCLUSION

Recent iris technology evolution has indeed demonstrated the reliability of iris biometrics as an effective means for human identification and recognition. Some prototype systems have even demonstrated standoff iris acquisition and recognition. As it stands, current iris technology offerings can enormously benefit law enforcement agencies. However, gains must be made to further improve performance and tap the full potential of iris recognition—especially for moving subjects. Subject motion presents technical challenges for iris segmentation and feature extraction. The task is made more difficult by factors including poorly captured or occluded iris images, obscuration, motion blur, and illumination artifacts. The field faces other challenges as well, including the unmet

needs for full interoperability between different systems and acquisition of irises at greater distances.

## REFERENCES


1. Daugman, J. How iris recognition works. *IEEE Trans. Circ. Syst. Video Technol*. **14**(1), 21–30.
2. Wildes, R. P. (1997). Iris recognition: an emerging biometric technology. *Proc. IEEE* **85**(9), 1348–1363.
3. Wildes, R. P., Keith, H., and Raymond, K. (1996). *Automated, Non-invasive Iris Recognition System and Method*, US Patent No. 5∼572∼596, US Government Printing Office, Washington, DC.
4. Wildes, R. P., Asmuth, J., Green, G., Hsu, S., Kolczynski, R., Matey, J., and McBride, S. (1994). A system for automated iris recognition. *Proceedings of the Second IEEE Workshop on Applications of Computer Vision*. Los Angeles, CA, pp. 121–128.
5. Boles, W. W. (1997). A security system based on human iris identification using wavelet transform. *First International Conference on Knowledge-based Intelligent Electronic Systems*. Adelaide, Australia, pp. 533–541.
6. Kim, D. H., and Ryoo, J. S. June 19, 2001 *Iris Identification System and Method of Identifying a Person Through Iris Recognition*, US Patent Application No. 62,247,813 B1.
7. Ross, A., and Shah, S. (2006). Segmenting non-ideal irises using geodesic active contours. In *Proceedings of 2006 Biometrics Consortium*, University of Virginia, Morgantown, REF 1-4244-0487. Available at: http://www.csee.wvu.edu/∼ross/pubs/RossIrisGAC_BSYM2006.pdf.
8. Monro, D. M., and Rakshit, S. (2005). *JPEG 2000 Compression of Human Iris Images for Identity Verification*, ICIP report. Smart Sensors Ltd, Portishead, UK, research supported by the University of Bath.
9. Hamza, R. (2005). January 26, 2005 filed *A 1D Polar Based Segmentation Approach (POSE)*, US Non-Provisional Patent Application Serial NO. 11/043,366.
10. Hamza, R. (2005). Filed January 26, 2005. *Invariant Radial Iris Segmentation*, U.S. Provisional Application No. 60/647,270. US Patent Application Honeywell File No. H0011492.
11. Hamza, R. (2006). Filed March 3, 2006. *A Distance Iris Recognition System*, U.S. Provisional Application No. 60/778,770.
12. Proenca, H., and Alexandre, L. (2007). Toward noncooperative iris recognition: a classification approach using multiple signatures. *IEEE Trans. Pattern Anal. Mach. Intell.*, **29**(4), 607–612.
13. Hamza, R. (2007). Filed Feb 15, 2007. *Standoff Iris Recognition System*. U.S. Provisional Application No. 11/675,424.
14. Daugman, J. G.. 1994. US Patent No. 5∼291∼560, Biometric personal identification system based on iris analysis. US Government Printing Office, Washington, DC.
15. Thornton, J., Savvides, M., and Vijaya Kumar, B. V. K. (2007). A Bayesian approach to deformed pattern matching of iris images. *IEEE Trans. Pattern Anal. Mach. Intell.*, **29**(4), 596–606.
16. Du, Y., Ives, R., Etter, D., Welch, T., and Chang, C.-I. (2004). *A One-dimensional Approach for Iris Identification*, EE Dept, US Naval Academy, Annapolis, MD, http://www.usna.edu/EE/EE_Research/Biometrics/Papers/5404-57.pdf.
17. Ma, L., Tan, T., Zhang, D., and Wang, Y. (2004). Local intensity variation analysis for iris recognition. *Pattern Recognit.*, **37**(6), 1287–1298.
18. Ma, L., Wang, Y., and Tan, T. (2002). Iris recognition using circular symmetric filters. *Proceedings of the 16th International Conference on Pattern Recognition*. Quebec, Canada

Vol. 2:414-17. http://www.sinobiometrics.com/publications/lma/Iris Recognition Using Circular Symmetric Filters.pdf.

19. Sun, Z., Tan, T., and Wang, Y. (2006). Robust encoding of local ordinal measures: a general framework of iris recognition. *Proceedings of 2006 Biometrics Consortium Conference*. pp. 270–282.
20. Hamza, R. (2007). Filed on March, 2007. *Indexing and Database Search System*. US Patent Application 1100.1449101. Honeywell File No. H0014322.
21. Guo, G. (2006). *Face, expression, and iris recognition using learning base approaches*. Technical report #1575, August 2006, Computer Sciences Department, University of Wisconsin, Madison.
22. Lim, S., Lee, K., Byeon, O., and Kim, T. (2001). Efficient iris recognition through improvement of feature vector and classifier. *ETRI J.*, **23**(2), 61–70.
23. Phillips, P. J., Scruggs, W. T., O'Toole, A. J., Flynn, P. J., Bowyer, K. W., Schott, C. L., and Sharpe, M. *FRVT 2006 and ICE 2006 Large-Scale Results*, National Institute of Standards and Technology, NISTIR 7408. Arlington, VA.
24. Daugman, J. G. (2006). Probing the uniqueness and randomness of IrisCodes: Results from 200 billion iris pair comparisons. *Proc. IEEE* **94**(11), 1927–1935.
25. http://www.sarnoff.com/products_services/government_solutions/homeland_security/iom_brochure, 2007.

# A TANDEM MOBILITY SPECTROMETER FOR CHEMICAL AGENT AND TOXIC INDUSTRIAL CHEMICAL MONITORING

H. William Niu, David E. Burchfield, and Andrew W. Szumlas

*Hamilton Sundstrand Corporation, Pomona, California*

Andrew Anderson

*Sionex Corporation, Bedford, Massachusetts*

## 1 INTRODUCTION

Increased efforts by government agencies to provide chemical warning systems for military and civilian locations have fueled the search for more sensitive and selective

detectors. To better satisfy the demands required of sensors for these applications, we have developed an instrument that combines the technologies of differential and ion mobility. These two spectrometric techniques separate chemical warfare agent (CWA) and toxic industrial chemical (TIC) compounds in a complementary fashion, and allow the differential mobility spectrometer (DMS)–ion mobility spectrometer (IMS) to provide sensitive and selective detection for homeland security applications. This article describes the tandem DMS–IMS, its salient features, and the benefits that can be realized by application of the new sensor to homeland security applications.

## 2 SCIENTIFIC OVERVIEW OF TANDEM MOBILITY SPECTROMETRY

The detection capability of an analytical instrument is not only limited by detector sensitivity, but also by the environmental background presented in the sample. Hyphenated instrumentation uses combinations of two analytical techniques that enhance selectivity and interference rejection capability. An innovative example of this type of technology is the tandem DMS–IMS, which accomplishes the combination goals of hyphenated instrumentation.

### 2.1 Ion Mobility Spectrometry (IMS)

IMS is a technique that detects target compounds by measurement of their velocities (equivalent to measurement of the ions' gas-phase mobilities) as electrically charged target ions are drawn through a buffer gas [1, 2]. Measurement of ion mobilities as a function of time of flight in a drift tube under an applied electric field was developed in the early 1970s. The technique is simple in principle. A conventional IMS consists of an atmospheric pressure ionization (API) source, a drift tube, and a detector. As shown in Figure 1, ions are produced from air molecules by an ionizer such as an electrical discharge or radioactive source. Both positively and negatively charged ions are created

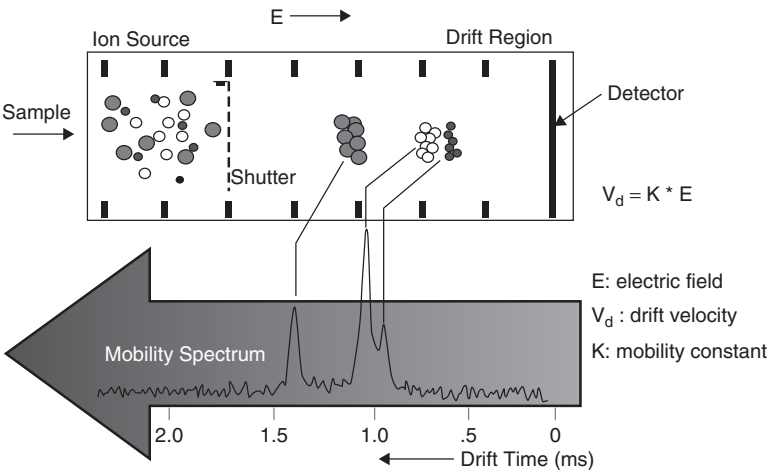



**FIGURE 1** Schematic for a conventional ion mobility spectrometer. Ions arrive at the detector according to their mobilities (courtesy of Prof. Eiceman).

in the source and, if water is present at ppm or higher concentrations, these reactant ions typically percolate down to hydrated protons $\{(H_2O)_n \cdot H^+\}$ and $O_2^-$, respectively. These "reactant ions" can transfer charge to trace contaminants by either proton or electron transfer or can directly react with contaminants to generate ions. Any ions formed are then drawn through the analyzer under an electric field, timed as they transit a drift region, and the time to their arrival at a detector is converted to mobility. An ion's mobility is related to its mass and cross-sectional area in the gas phase. The IMS is analogous to a time-of-flight mass spectrometer. Application of IMS technology trades the exceptional selectivity of the mass spectrometer for instrument simplicity, especially elimination of a vacuum pump.

Because water plays an important part in ion-molecule chemistry, it is necessary to control the water vapor concentration within the spectrometer; optimum performance is best achieved by operating with relatively dry air containing low ppm levels of water vapor. For this reason, recirculated dry air is supplied to the spectrometer for most field applications.

On balance, IMS is attractive due to its high intrinsic sensitivity, conceptual simplicity, and potential for miniaturization. For over 20 years, ion mobility spectrometers have been successfully deployed for detecting CWAs for military applications and explosives at airports. This technique has also been applied to environmental monitoring, usually in conjunction with a gas chromatograph. In addition, IMS is highly sensitive and amenable to portable and inexpensive instrumentation.

### 2.2 Differential Mobility Spectrometry (DMS)

A variation of IMS is called *differential mobility spectrometry (DMS)* or *field asymmetric ion mobility spectrometry ( FAIMS )* [3, 4]. In DMS, ions are carried down a drift tube by a gas flow while being subjected to an oscillating Radio Frequency (RF) electric field transverse to the flow direction. Depending on how the various ions' mobilities change under the high and low alternating fields, the RF waveform will drive some ions out of the flow, allowing only a narrow range of ion species to transit the drift tube and reach the detector. In this manner, the DMS operates as an RF ion filter analogous to a quadrupole mass spectrometer. The use of long dwell times, similar to selected ion monitoring in mass spectrometry, can generate high sensitivity (effectively 100% throughput) for ions of interest. The DMS can also be scanned continuously across the range of ions present or it can be step-scanned to extract target ions sequentially from a mixture.

A DMS analyzer consists of an ionization source, a tunable ion filter sandwich constructed of microfabricated electrodes, and two ion detectors (one for positive ions and one for negative ions). Figure 2 shows a DMS ion filter and illustrates in more detail the principle behind DMS. As ions move through the ion filter, an asymmetric oscillating field is applied perpendicular to the ion path. The asymmetric RF applies a very high electric field (of the order of 10–20 kV/cm) briefly, followed by a lower field of opposite polarity for a proportionally longer period. Any ions formed in the API source experience this asymmetric field and move with a zigzag motion down the filter. Most ions will adopt an off-axis trajectory, striking an electrode surface where they are neutralized and never reach the Faraday collectors. The resulting neutral molecules are carried out of the spectrometer by the gas flow. Only ions whose high-field mobilities exactly offset their low-field mobilities will make it through the separation region of the detector. The filter is tuned to an ion's specific differential mobility by superimposing a separate Direct

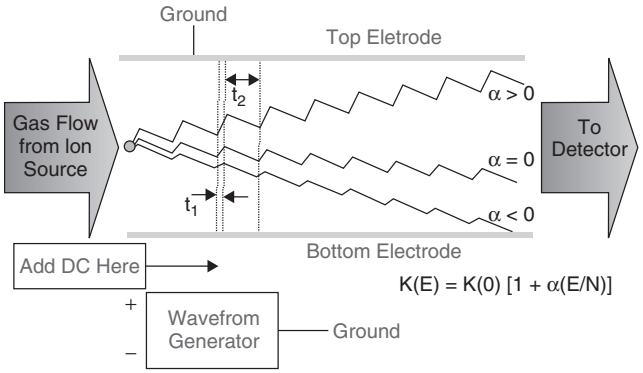



**FIGURE 2** Field asymmetric DMS. Varying the compensation voltage determines the $\alpha$ or differential mobility value of the transmitted ions (courtesy of Prof. Eiceman).

Current (DC) bias on the RF field. This DC or "compensation" field is used to counter a specific target ion's drift toward the walls, restoring a narrow range of differential mobilities to the centerline of the drift tube and forcing all other ions with off-axis trajectories to be neutralized at a wall. Once through the ion filter, all remaining ions are drawn to the Faraday collectors where they present their charge to the amplifier, generating an analytical signal.

The analytical utility of the DMS is realized by sequentially selecting the ions that pass through the filter by scanning the compensation voltage (CV) over a suitable range, typically +10 to −45 V. Typical DMS spectra for dimethyl-methyl-phosphonate (DMMP), a simulant for the nerve agent Sarin, in dry air and lab air are shown in Figure 3.

DMS is a relatively new sensor technology. It has been applied similarly to conventional IMS for the detection of CWAs [5] and explosives [6]. A DMS is also commercially available from the Sionex Corp. (Bedford, MA) as a gas chromatograph detector. While related to IMS, DMS has superior sensitivity compared to IMS and similar classes of

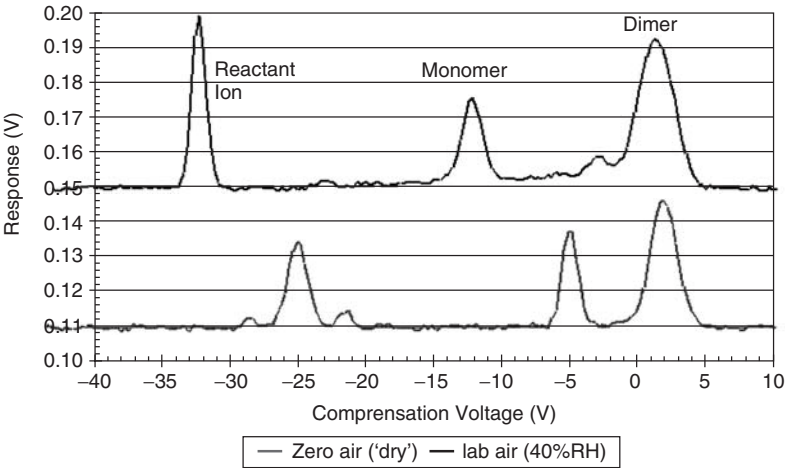



**FIGURE 3** Typical compensation voltage (CV) spectrum for DMMP, a sarin simulant. The reactant ion peak, monomer, and dimer of DMMP are shown as a function of CV.

sensors. It can simultaneously detect positive and negative ions with response times on the order of seconds. Furthermore, the RF amplitude applied to the DMS filter can be varied to change the ion separation characteristics. The microfabricated DMS cell facilitates mass production with affordable cost.

### 2.3 Tandem DMS–IMS

Both IMS and DMS can be made portable for field applications. However, they are each relatively low-resolution devices that are susceptible to background interferences. For atmosphere monitoring at trace levels, a front-end separation device such as a gas chromatograph is usually employed to reduce the sample complexity associated with operation in an atmosphere with many constituents. However, gas chromatography is best performed with an inert carrier to preserve column lifetime and efficacy, which adds to the logistical burden of operation.

The tandem DMS–IMS concept links two mobility devices with different separation mechanisms to enhance selectivity while maintaining simplicity. In a conventional IMS, ions are formed in the source region and gated into a drift tube. Because the width of the ion packet is related to the time, the gate is turned on and the separation of those packets occur over a much longer time with the gate closed, the time-of-flight spectrometer only has about 1% throughput. A DMS has a much higher throughput, approaching 100% when tuned for a target compound. In the tandem arrangement, ions entering the instrument first pass through a DMS filter where target ions are separated from the bulk of the sample. The ions that pass through the DMS are presented to dual IMS drift tubes for detection. The CV of the DMS can be scanned across the entire range of ion species of interest while IMS spectra are collected. Alternatively, the DMS can be programmed to step-scan so that only specific targets are presented to the IMS detectors.

In the configuration presented in Figure 4, the Faraday ion collectors commonly employed in a DMS are replaced by a pair of IMS analyzers. Two small IMS drift cells serve as ion detectors while the DMS is used as a prefilter. In this concept, the analytical chain, which includes the source, DMS, detectors, pneumatics, and electronics, is shared and therefore the overall size is small. The analyzer shown has a total volume of less than 9 $in.^3$ and further miniaturization is possible.

The tandem DMS–IMS generates two-dimensional data, with separation realized along both differential mobility and ion mobility axes. An example spectrum generated by the DMS–IMS is shown in Figure 5. Here, the positive reactant ion peak (RIP) generated by the ion source is shown in the positive ion spectrum. A similar negative ion spectrum is generated simultaneously. The DMS separation dimension is given along the vertical axis in units of CV, and it is apparent from the spectrum that a CV of approximately $-5$ V is needed to allow the RIP to reach the IMS drift tube. The horizontal axis represents drift time in milliseconds. Through either dimension, a two-dimensional spectrum can be displayed by examination of a single drift time or CV as shown on the right-hand side of the figure. This characteristic allows each separation dimension to be examined individually.

Figure 6 illustrates the use of a DMS–IMS to detect a target species that generates ions of both positive and negative polarity. These two spectra show DMS–IMS spectra for the analyte ethyl parathion. For this and other analytes that exhibit this dual-polarity behavior, the truly simultaneous detection provided by the DMS–IMS can be leveraged to assist in detection. If one ion is more prominent than its counterpart in the other channel,

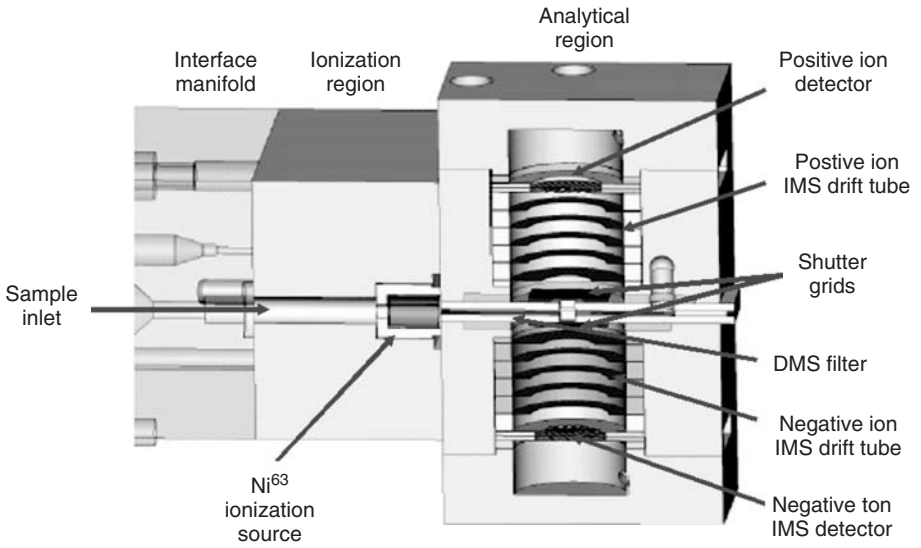



**FIGURE 4** DMS–IMS schematic. The prototype sensor utilizes an orthogonal configuration to simultaneously detect both positive and negative ions.

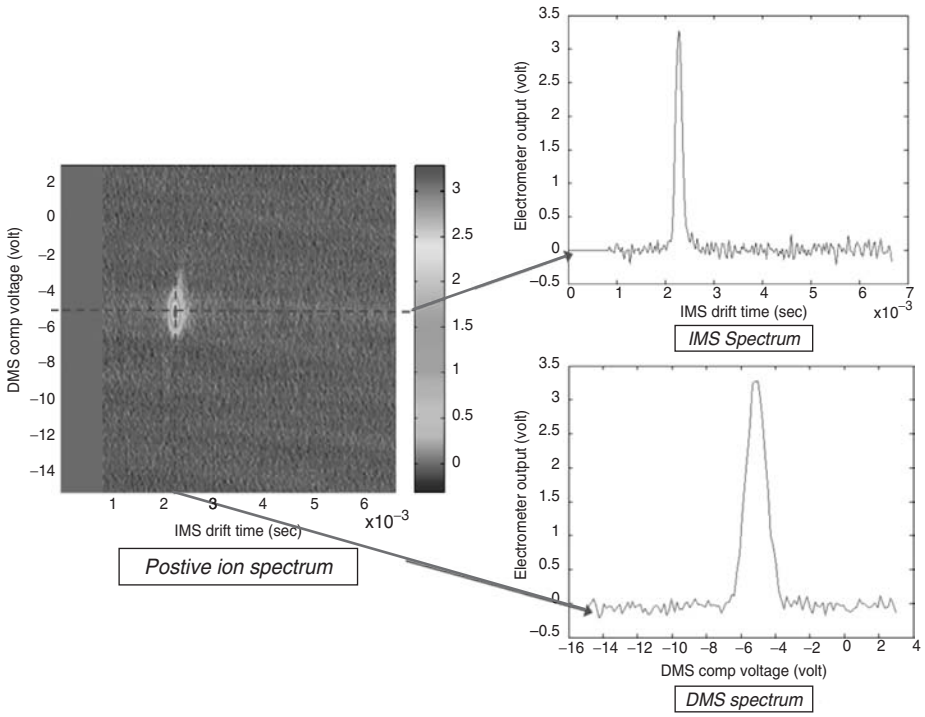



**FIGURE 5** Positive ion DMS–IMS spectrum. This representative RIP spectrum displays the two-dimensional separation characteristics of the new sensor.

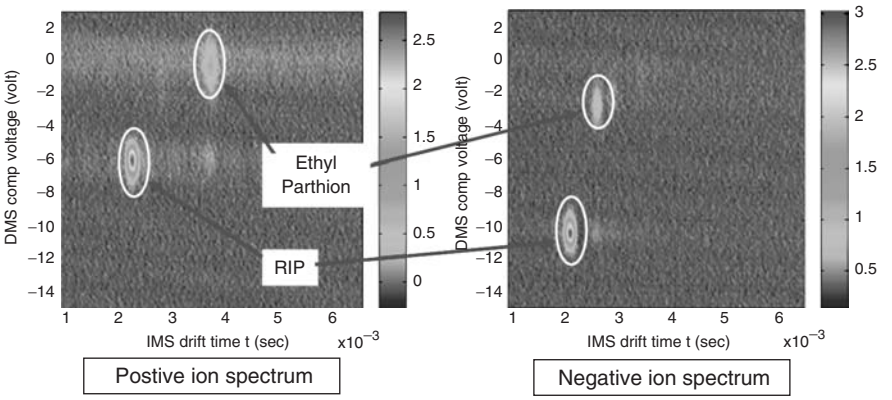


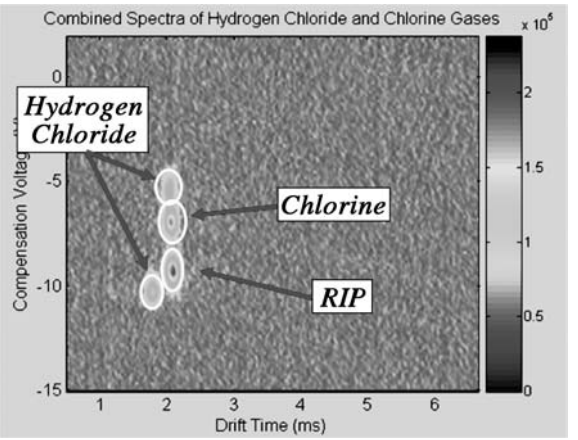

**FIGURE 6** Demonstration of simultaneous positive and negative ion detection. Targets that form both positive and negative ions can be readily detected in the channel of the DMS–IMS that provides greater selectivity or sensitivity.

that ion can be utilized to provide quantitation and lower limit of detection. Additionally, the ion in the other channel can be used to confirm the presence of the ion used for quantitative analysis. In this fashion, the possibility of a false positive is greatly reduced, as two chemical species need to be present at specific locations in both the positive and negative ion channels. Targets that display positive and negative ion identifiers have proven to have quite unique spectral signatures in tests performed to date.

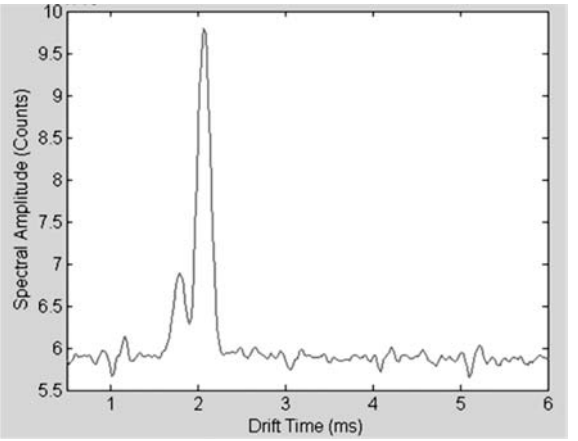
In addition to the benefits of dual-polarity ion detection, the DMS–IMS can also enhance the separation of TICs and CWAs due to the two different separation mechanisms. In general, the DMS prefilter is more effective in the separation of low molecular weight compounds than IMS, while drift-time analysis is more appropriate for the separation of compounds with higher molecular weights. Figure 7 shows a combined DMS–IMS spectrum formed from hydrogen chloride (HCl) and chlorine (panel A) spectra. The clear picture of the four analytical signals that can be attained through use of the DMS–IMS becomes ambiguous upon examination of the same system with either IMS (panel B) or DMS separation (panel C) alone.

## 3 RESEARCH AND FUNDING DATA

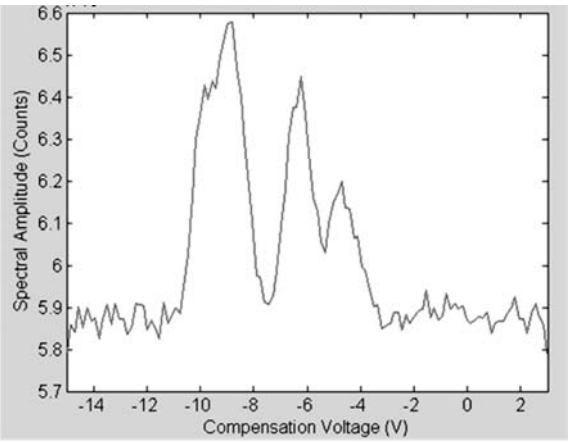
Interest in sensor technologies for homeland security applications has escalated in recent years. Search of two scientific databases shows the number of articles that contain "homeland security" begin to rise after the terrorist attacks of 2001 as shown in Figure 8. Interest in IMS rose concurrently, as ion mobility devices presented an available technology that had previously been applied to CWA detection by military users [7]. Extension of this technology to the detection of TIC compounds has provided a low-resistance path to fielding handheld detectors for first responders. The use of ion mobility for infrastructure protection has proven more challenging because of the demand of low false alarm rates. Coincident with the rise of IMS and its application to homeland security, the technique of DMS became more widely adopted as an analytical technique. A literature search using the keywords of DMS and FAIMS demonstrates the relative youth of the DMS analytical technique when compared to its more mature IMS counterpart. However, DMS




(a)




(b)




(c)

**FIGURE 7** Example of resolution provided by a DMS–IMS sensor. (a) DMS–IMS spectrum obtained from combination of individual hydrogen chloride and chlorine spectra; (b) spectrum of hydrogen chloride and chlorine if using IMS separation only; (c) spectrum of hydrogen chloride and chlorine if only DMS separation were employed.

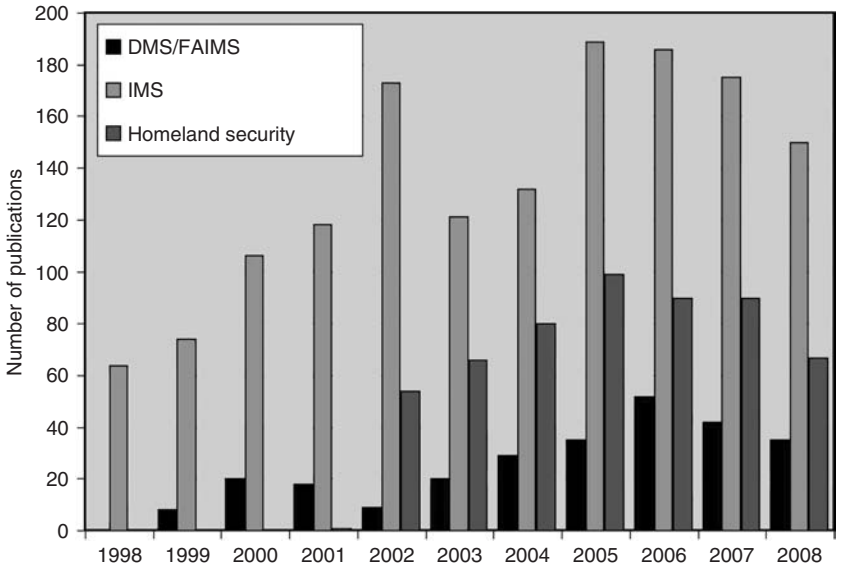



**FIGURE 8** Number of publications in homeland security and mobility sensors in the past ten years. Number of publications per year as compiled from the Institute for Scientific Information (ISI) and Chemical Abstracts databases. Keywords searched were differential mobility spectrometry or FAIMS, ion mobility spectrometry, and homeland security.

has quickly gained acceptance as a viable sensor alternative. As an example, large-scale laboratory FAIMS-MS instruments are now commercially available.

Funding for sensors applied to homeland security or the protection of military personnel and installations has also increased in the current decade. The formation of the Department of Homeland Security (DHS) has provided a conduit for the direct funding of research applied to chemical countermeasures. In fiscal year 2009, the budget request for the DHS Science and Technology Directorate is $869 million. At the same time, the military Joint Program Executive Office for Chemical and Biological Defense requested $352 million for sensors.

## 4 CRITICAL NEEDS ANALYSIS

In homeland security applications, chemical detectors face a difficult operating environment with high demands on performance. Detectors fielded for infrastructure protection or emergency response must provide high sensitivity, excellent selectivity, longevity, and continuous, low cost operation. Furthermore, these detectors must operate in environments with complex chemical backgrounds. Examination of the qualities that are most important in homeland security applications suggest that the selectivity of the detector is of specific importance for detectors deployed to protect individuals at airports, subways, or other critical transportation infrastructure. The need for high selectivity is driven by the fact that if a detector reports a false positive, the subsequent societal disruptions and public panic that the alarm causes are extremely costly. Similarly, first responders require a chemical detector they can trust to provide the information they need to take decisive action in response to potential chemical threats or industrial accidents.

### 4.1 Infrastructure Protection

Chemical detectors play a key role in the protection of public and private infrastructure. Potential chemical attacks could be launched against public transportation hubs like subways, airports, and train stations. In addition, high-profile public and private buildings, as well as embassies abroad, have been identified as potential venues for chemical attacks. For these infrastructure protection applications, multiple chemical detectors would be placed at areas throughout the structure or facility based on either probability of release or modeling of chemical plume movement. The more detectors placed within the structure, the lower the likely response time after a chemical release. However, the more detectors that are desired, the lower their associated cost must be, with both initial and maintenance costs of the full system considered. To keep operational costs low, the detector and sampling system both need to be highly automated and reliable over years of operation.

Technologies similar to IMS and the DMS–IMS have been considered for infrastructure protection applications. A stand-alone DMS was evaluated by Hamilton Sundstrand for its efficacy in the detection of TICs and CWA simulants, and demonstrated excellent sensitivity and selectivity. However, complexity of the sample matrix in some facilities may cause the DMS to have false response issues similar to stand-alone IMS detectors, and it is likely that both DMS and IMS technologies will require a secondary separation technique to help resolve background interferents when placed in real-world operating conditions. Toward this end, a GC–IMS has also been evaluated, and generally displayed excellent analytical performance. However, this combination has the ultimate drawback of limited column reliability, need for a sorbent trap, and longer analysis time.

The DMS–IMS detector system has been designed specifically for extended protection of critical infrastructure. The sensor utilizes a membrane inlet system that selectively admits TIC and CWA compounds while simultaneously reducing the amount of background organic species that can make their way into the analyzer. The inlet system is designed for extended operation in various sample matrices, and since it isolates the detector from the external environment, clean analytical gas can be provided to the DMS–IMS analyzer through use of a simple filter system. The instrument's design supports long-lived, low-maintenance field operation, while it also provides the combination of two separation techniques necessary for these demanding applications.

### 4.2 Portable Applications

First responders often have the greatest need for a highly specific chemical detector. Emergency personnel on the scene of either industrial accidents or potential chemical attacks require a detector that can positively identify any gaseous hazards present in order to coordinate an appropriate response. In addition to selectivity, the responder's device needs to be highly portable, preferably in a handheld form-factor, battery powered, and no more than a few pounds in weight. Detectors that meet these criteria can assist emergency crews to accurately assess the incident and initiate a proper hazard response to save lives.

Different types of chemical detectors have been proposed or are currently available for use by first responders. The available technologies for this application include handheld IMS instruments, chemical-sensing arrays, and flame spectrophotometers [8]. The DMS–IMS technology is also highly amenable to portable applications as it combines IMS technology, currently the most widespread chemical detector for CWA detection, with an additional capability to reduce false positives. At the same time, instrument

simplicity is maintained by the shared sensor platform, which allows the instrument to maintain the small form-factor and robust characteristics necessary for first responder devices.

## 5 FURTHER RESEARCH DIRECTION

At its current development stage, the DMS–IMS detector has proven effective for the detection of a broad range of both CWA and TIC compounds in a laboratory environment. The next stages of development require additional operational tests in real-world infrastructure protection environments. Areas of study to support these field tests include optimization of the instrument configuration and improvements to the detection algorithm. In certain cases, the use of a dopant within the system can suppress background species and enhance the separation possible with the DMS [9]. Dopant introduction, coupled with refinement of the detection algorithm, can assist in the proper identification of targets and reduce overlapping responses for targets and background chemical species. Although unattractive from a logistical standpoint, particular applications where high specificity for a select target list are desired may warrant addition of a gas chromatograph to the sample inlet to provide a third separation dimension.

Additional areas of interest include a widening of potential targets to additional TIC and CWA compounds. The use of the radioactive source employed to date has been driven largely by the need for simplicity. However, additional nonradioactive sources have recently become more prominent [10, 11] in the literature and may provide a new method for additional selectivity or target detection.

## REFERENCES

1. Eiceman, G. A. and Karpas, Z. (2005). *Ion Mobility Spectrometry*, Taylor & Francis Group, Boca Raton, FL.
2. Creaser, C. S., Griffiths, J. R., Bramwell, C. J., Noreen, S., Hill, C. A., and Paul Thomas, C. L. (2004). Ion mobility spectrometry: a review. Part 1. Structural analysis by mobility measurement. *Analyst*. **129**, 984–994.
3. Miller, R. A., Nazarov, E. J., Levin, D. (2007). Differential mobility spectrometry (FAIMS): a powerful tool for rapid gas phase ion separation and detection. *J. Chromatogr. Libr*. **72**, 211–255.
4. Guevremont, R. (2004). High-field asymmetric waveform ion mobility spectrometry: A new tool for mass spectrometry. *J. Chromatogr. A*. **1058**(1–2), 3–19.
5. Krebs, M. D., Zapata, A. M., Nazarov, E. G., Miller, R. A., Costa, I. S., Sonenshein, A. L., and Davis, C. E. (2005). Detection of biological and chemical agents using differential mobility spectrometry (DMS) technology. *IEEE Sensors*. **5**(4), 696–703.
6. Eiceman, G. A., Krylov, E. V., and Krylova, N. S. (2004). Separation of ions from explosives in differential mobility spectrometry by vapor-modified drift gas. *Anal. Chem*. **76**(17), 4937–4944.
7. Eiceman, G. A. and Stone, J. A. (2004). Ion mobility spectrometers in national defense. *Anal. Chem*. **76**(21), 390A–397A.
8. Seto, Y., Kanamori-Kataoka, M., Tsuge, K., Ohsawa, I., Matsushita, K., Sekiguchi, H., Itoi, T., Iura, K., Sano, Y., and Yamashiro, S. (2005). Sensing technology for chemical-warfare agents and its evaluation using authentic agents. *Sens. Actuators B Chem*. **108**, 193–197.

9. Levin, D. S., Vouros, P., Miller, R. A., Nazarov, E. G., and Morris, J. C. (2006). Characterization of gas-phase molecular interactions on differential mobility ion behavior utilizing an electrospray ionization-differential mobility-mass spectrometer system. *Anal. Chem*. **78**(1), 96–106.
10. Andrade, F. J., Shelley, J. T., Wetzel, W. C., Webb, M. R., Gamez, G., Ray, S. J., and Hieftje, G. M. (2008). Atmospheric pressure chemical ionization source. 1. Ionization of compounds in the gas phase. *Anal. Chem*. **80**(8), 2646–2653.
11. Cody, R. B., Laramée, J. A., and Durst, H. D. (2005). Versatile new ion source for the analysis of materials in open air under ambient conditions. *Anal. Chem*. **77**(8), 2297–2302.

## FURTHER READING

Sun, Y, Kwok, Y. O. (2005). *Detection Technologies for Chemical Warfare Agents and Toxic Vapors*. CRC Press, Boca Raton, FL.

# DYNAMIC LOAD BALANCING FOR ROBUST DISTRIBUTED COMPUTING IN THE PRESENCE OF TOPOLOGICAL IMPAIRMENTS

MAJEED M. HAYAT

*Department of Electrical and Computer Engineering and Center for High Technology Materials, University of New Mexico, Albuquerque, New Mexico*

JORGE E. PEZOA AND DAVID DIETZ

*Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, New Mexico*

SAGAR DHAKAL

*Nortel Networks Inc., Richardson, Texas*

## 1 INTRODUCTION

A new class of applications, based on sensor networks (SNs), has emerged in recent years. Examples of these applications are habitat monitoring, intrusion detection, defense and military battlefield awareness, structural health monitoring, and scientific exploration.

These applications share a particular feature, namely, the necessity of collaboration among the sensors. Consequently, the idea of performing distributed computing (DC) naturally appears in an SN environment. In fact, DC is being performed in wireless sensor networks (WSNs) in order to reduce the energy consumption of the set of sensors, make efficient use of network bandwidth, achieve desired quality of service, and reduce the response time of the entire system. These new applications have generated challenging scenarios, and the resource allocation solutions developed for traditional distributed computing systems (DCSs) are not appropriate under these new scenarios [1]. For instance, when DC is performed in a WSN, classical assumptions on node and communication-link reliability are no longer valid because (i) WSNs are typically deployed in harsh environments where sensors are prone to fail catastrophically and (ii) in order to save energy, sensors are allowed to turn themselves off at any time. In addition, assuming that the cost of transmitting data among the sensors is negligible or deterministic is not valid either. Also, large-scale donation-based distributed infrastructures, such as peer-to-peer networks and donation grids, exhibit a similar kind of behavior; the topology of the DCS changes over time as computing elements (CEs) enter into or depart from the DCS in a random fashion. Furthermore, any short-term or long-term damage that can be inflicted to the CEs in these infrastructures adds to this dynamic behavior. Clearly, the new scenarios for DC demand for solutions that can adapt to both fluctuations in the workload and changes in the number of CEs available in the DCS.

We review here modern resource reallocation techniques that are effective in modern dynamic DCSs [2–5]. In particular, we describe dynamic load balancing (DLB) policies that can be used to improve the performance of a DCS in the presence of random topological changes. These policies simultaneously attempt to improve the robustness of the DCS and to use the available CEs in the system efficiently. In this article, we have considered two different performance metrics: the average response time of a software application and the probability of executing an application successfully. These metrics are analytically modeled using the novel concept of stochastic regeneration. Our model takes into account the heterogeneity in the computing capabilities of the CEs, the random failure and recovery times of the CEs, and the random transfer times associated to communication network. Based upon this model, we devise DLB policies that optimize these two performance metrics. First, we discuss DLB policies suitable for scenarios where CEs can fail and recover at random instants of time, as in the case of DC in WSNs or donation-based DCSs. Then, we analyze policies for scenarios where CEs can fail permanently, which model long-term physical damages like those inflicted by weapons of mass destruction (WMD). Our theory is supported by Monte Carlo (MC) simulations and experimental results collected from a small-scale test-bed DCS.

## 2 THE LOAD BALANCING PROBLEM IN DISTRIBUTED COMPUTING

Large, time-consuming applications can be processed by a DCS in a parallel fashion. To this end, applications have to be divided into smaller units, called modules or tasks, which can be processed independently at any CE of the system. Tasks have to be intelligently allocated onto the nodes in order to efficiently use the computing resources available in the DCS. This task allocation is referred to in the literature as load balancing (LB). LB strategies can be divided into static and dynamic, centralized or decentralized, and sender

initiated or receiver initiated [1]. Static LB is performed before the actual execution of the application in the system. At compiling time and based upon statistics of the DCS, the compiler divides the application accordingly into several tasks, which are allocated onto the CEs upon the execution of the application. In DLB, both applications and LB algorithms are being executed in the DCS. The DLB algorithm continuously monitors the queue length of the CEs, and upon the detection of an imbalance, it triggers the reallocation of tasks among the CEs. When the CEs are prone to fail, the LB algorithm must monitor also the working or failed state of the CEs. In this article, we focus on decentralized DLB policies because, in general, DLB policies outperform static LB policies in DCSs where both the system workload and the number of functioning CEs change dynamically with time [1].

In order to optimize a given performance metric, any DLB policy has to answer the following fundamental questions at each CE: (i) *When the jth CE has to trigger a LB action?* (ii) *How many tasks have to be processed at the jth CE?* and (iii) *How many tasks have to be reallocated from the jth CE to the other CEs?* The first question is answered by comparing the load at the $j$th CE with the average load in the system. To this end, information about the number of tasks queued at each CE must be collected by the $j$th CE. We denote by $\hat{Q}_{k,j}(t)$ the number of tasks queued at the $k$th CE as perceived by the $j$th CE at time $t$. Based upon this information, the $j$th CE computes its excess load at time $t$, denoted as $L_j^{\text{ex}}(t)$, using the formula:

$$L_j^{\text{ex}}(t) = Q_j(t) - \frac{\Lambda_j}{\sum_{l=1}^{n} \Lambda_l} \sum_{l=1}^{n} \hat{Q}_{l,j}(t) \tag{1}$$

A positive value for $L_j^{\text{ex}}(t)$ means that the $j$th CE is overloaded compared to the average load in the system, and as a consequence, an LB action must be triggered at time $t$. Note that the $\Lambda_j$ parameters in Eq. (1) can be defined in several ways in order to establish different balancing criteria. If the $\Lambda_j$'s are associated with the processing speed of the CEs, then the balancing criterion is determined by the relative computing power of the nodes. Alternatively, if the $\Lambda_j$'s are associated to the failure rates of the nodes, then the balancing criteria is determined by the reliability of the CEs.

The second question is answered by employing Eq. (1) again. When the excess load at the $j$th CE is positive, the amount of tasks to be processed locally by the $j$th CE is given by the difference between its current and excess loads. The remaining tasks should be reallocated to other CEs. Otherwise, if $L_j^{\text{ex}}(t) \leq 0$ then the $j$th CE has to process all its tasks.

Finally, the third question is answered by computing which CEs are underloaded compared to the average load in the system, as is perceived by the $j$th CE. These underloaded processors are CE candidates to receive tasks. The number of tasks that each candidate CE receives is denoted by $p_{jk}L_j^{\text{ex}}(t)$, where $p_{jk}$ is the partition of the excess load at the $j$th CE assigned to the $k$th candidate receiving CE. Partitions can be defined in several ways: evenly, according to the relative excess load of each candidate CE, and so on. In general, these partitions may not be effective and must be adjusted in order to compensate for the effects of the random communication times. Thus, the load to be transferred from the $j$th to the $k$th CE must be adjusted according to what is called the LB gain, which is denoted as $K_{jk}$. Finally, the number of tasks to be transferred from

the $j$th to the $k$th CE is given by

$$L_{jk}(t) = \left\lfloor K_{jk} p_{jk} L_j^{\text{ex}}(t) \right\rfloor$$

where $[x]$ is the greatest integer less than or equal to $x$.

The LB gains are parameters that ultimately define the number of tasks to reallocate to each CE. We optimally select the value of such gains so that we can minimize the average response time of an application or maximize the probability of successfully serving an application. In order to optimize these metrics properly, first we need a precise model for the response time of an application. The response time is a complex random variable, which combines the randomness of the task processing times at the CEs, the failure and recovery times of the CEs, and the task transfer times in the communication network.

## 3 STOCHASTIC MODELING OF THE RESPONSE TIME

The idea of stochastic regeneration in DCSs is thoroughly reviewed; to do so, we freely draw from our earlier published works [2–4]. Our novel approach based on stochastic regeneration allows us to obtain recurrence equations that characterize both the average response time of an application and the probability of successfully serving an application [2–4]. The key idea is to introduce a special random variable, called the regeneration time, $\tau$, which is defined as the minimum of the following six random variables: the time to the *first* task service by any CE, the time to the *first* occurrence of failure at any CE, the time to the *first* occurrence of recovery at any CE, the time to the *first* arrival of a queue-length information at any CE, the time to the *first* detection of a failure at any CE, or the time to the *first* arrival of a group of tasks at any CE. The key property of the regeneration time is that upon the occurrence of the regeneration event $\{\tau = s\}$, a *fresh* copy of the original stochastic process (from which the random response time is defined) will emerge at time $s$, with a *new* initial system configuration that transpires from the regeneration event.

In order to appreciate how the idea of regeneration works, let us consider the following simplified example. For a two-node DCS, let the following random variables $W_j$, $X_j$, $Y_j$, and $Z_{jk}$ denote the service time of a task at the $j$th CE, the failure time of the $j$th CE, the recovery time of the $j$th CE, and the task transfer time from the $j$th to the $k$th CE, respectively, with $j, k \in \{1, 2\}$, $j \neq k$. Thus, the regeneration time is precisely defined as, $\tau = \min(W_1, W_2 X_1, X_2, Y_1, Y_2, Z_{12}, Z_{21})$. Let us denote by $T_{m_1,m_2}^{\mathbf{I},\mathbf{F}}(t_{\text{b}}; \mathbf{C})$ the random response time of an application that comprises $m_1 + m_2$ tasks, where $t_{\text{b}}$ denotes the balancing instant and $\mathbf{I}$, $\mathbf{F}$, and $\mathbf{C}$ are vectors that monitor the number of tasks in the CEs, the working state of the CEs, and the number of tasks being transferred in the network, respectively. By exploiting the random variable $\tau$, we can compute the average response time of the application as

$$\begin{aligned}\mathrm{E}\left[\mathrm{E}\left[T_{m_1,m_2}^{\mathbf{I},\mathbf{F}}(t_{\text{b}};\mathbf{C}) \,|\tau\right]\right] = \mathrm{E}\Bigg[&\sum_{j=1}^{2} \mathrm{E}\left[T_{m_1,m_2}^{\mathbf{I},\mathbf{F}}(t_{\text{b}};\mathbf{C}) \,\middle|\, \tau = W_j\right] P\left(\tau = W_j\right) \\ &+ \sum_{j=1}^{2} \mathrm{E}\left[T_{m_1,m_2}^{\mathbf{I},\mathbf{F}}(t_{\text{b}};\mathbf{C}) \,\middle|\, \tau = X_j\right] \times P\left(\tau = X_j\right)\end{aligned}$$

$$+\sum_{j=1}^{2}\mathrm{E}\left[T^{\mathbf{I},\mathbf{F}}_{m_1,m_2}(t_\mathrm{b};\mathbf{C})\,\middle|\,\tau=Y_j\right]P\left(\tau=Y_j\right)$$

$$+\sum_{j=1}^{2}\sum_{k=1,\,j\neq k}^{2}\mathrm{E}\left[T^{\mathbf{I},\mathbf{F}}_{m_1,m_2}(t_\mathrm{b};\mathbf{C})\,\middle|\,\tau=Z_{jk}\right]P\left(\tau=Z_{jk}\right)\Bigg] \quad (2)$$

If we consider the regeneration event $\{\tau = W_1\}$ (the service of a task at the first CE), one can show that $\mathrm{E}\left[T^{\mathbf{I},\mathbf{F}}_{m_1,m_2}(t_\mathrm{b};\mathbf{C})\,|\tau=W_1\right]=\tau+\mathrm{E}\left[T^{\mathbf{I},\mathbf{F}}_{m_1-1,m_2}(t_\mathrm{b}-\tau;\,\mathbf{C})\right]$, which means conditional on the service of a task at the first CE the original problem starts afresh with a new initial task distribution (*m–1 tasks at the first CE and* $m_2$ tasks at the second CE) and a new balancing instant (at $t_{\mathrm{b}-\tau}$). Similar "recurrence" relationships can be proven for every possible regeneration event. After considering all possible regeneration events, we can obtain a set of coupled difference-differential equations that completely describe the dynamics of the average response time. Going back to our simplified example, a sample equation from the set is

$$\frac{\mathrm{d}}{\mathrm{d}t_\mathrm{b}}\mathrm{E}\left[T^{\mathbf{I},\mathbf{F}}_{m_1,m_2}(t_\mathrm{b};\mathbf{C})\right]=\sum_{j=1}^{2}\lambda_{d,j}\mathrm{E}\left[T^{\mathbf{I},\mathbf{F}}_{m_1-\delta_{j,1},m_2-\delta_{j,2}}(t_\mathrm{b};\mathbf{C})\right]$$

$$+\sum_{j=1}^{2}\lambda_{f,j}\mathrm{E}\left[T^{\mathbf{I},\mathbf{F}_j}_{m_1,m_2}(t_\mathrm{b};\mathbf{C})\right]$$

$$+\sum_{j=1}^{2}\sum_{k=1,k\neq j}^{2}\lambda_{jk}\mathrm{E}\left[T^{\mathbf{I},\mathbf{F}}_{m_1}+L_{21}\delta_{j,1},m_2+L_{21}\delta_{j,2}(t_\mathrm{b};\mathbf{C})\right] \quad (3)$$

where $\lambda_{d,j}$, $\lambda_{f,j}$ and $\lambda_{jk}$ are the processing rate of the $j$th CE, the failure rate of the $j$th CE and the task transfer rate from the $j$th to the $k$th CE, respectively. The term $L_{jk}$ is the number of tasks transferred from the $j$th to the $k$th CE and $\delta_{j,k}$ is the Kronecker delta. Given that $L_{jk}$ depends on $K_{jk}$, we can formulate an optimization problem where $t_\mathrm{b}$ and the LB gains are judiciously selected so that the response time is minimized. Finally, structurally similar equations can also be obtained for the probability of successfully serving an application, as it is shown in [2–4].

## 4 SMALL-SCALE IMPLEMENTATION OF A DCS

We have implemented a small-scale test-bed DCS to experimentally test our DLB policies. The hardware architecture consists of the CEs and the communication network. Upon the occurrence of a failure, a CE is switched from the so-called working state to the backup state. If a node is in the backup state, then it is not allowed to continue processing tasks, but is allowed to work as a backup system that only receives and transmits tasks, so that no task in the system is missing. The occurrence of failures and recoveries at any CE is simulated by a software. The communication network employed in our architecture is the Internet, where the final links connecting the CEs are either wired or wireless. Our test bed also allows us to introduce, if needed, artificial latency by

employing traffic shaper applications. The software architecture of our DCS is divided in three layers: application, LB, and communication. Layers are implemented in the software using POSIX threads. The application layer executes the application selected to illustrate the distributed processing of matrix multiplication. To achieve variability in the processing speed of the CEs, the randomness is introduced in the size of each row of the matrix by independently choosing its arithmetic precision with an exponential distribution. In addition, the application layer determines the failure and recovery instants at each CE by switching its state from working and to backup. The LB layer executes the LB policy defined for each type of experiment conducted. This layer monitors the queue length of the CEs and triggers the LB action. It also: (i) determines if a CE is overloaded with respect to the other nodes in the system; (ii) computes the amount of task to transmit to other CEs; and (iii) selects which CEs are candidates to receive the excess amount of tasks. Finally, the communication layer of each node handles the transfer of tasks as well as the transfer of queue-length information among the CEs. Each node uses the UDP transport protocol to transfer a queue-length packet to the other CEs, and the TCP transport protocol to transfer the tasks between the CEs. Also, when a CE is in the backup state, this layer receives and transmits tasks, if necessary.

## 5 DLB POLICIES FOR SYSTEMS WHERE CES FAIL AND RECOVER

### 5.1 The Preemptive DLB Policy

The so-called preemptive DLB policy allows a single load transfer between the CEs and no other balancing action is taken afterwards. The DLB action is preemptive in the sense that it will counteract for the combined effects of failures, recoveries, and communication times on the application response time. At time zero, CEs are assumed to be functioning and a CE, say the $j$th CE, transfers $L_{jk}$ $(t_b)$ tasks to the $k$th CE at time $t_b$, where $L_{jk}(t_b) = \left\lfloor K_{jk} p_{jk} L_j^{ex}(t_b) \right\rfloor$ and $L_j^{ex}(t_b)$ is computed using Eq. (1) with the $\Lambda_j$ parameters defined to be equal to the processing rate of the CEs. The LB gains are optimally selected by solving recurrence Eq. (4) in [3].

Figure 1 (extracted from Figure 3 in [3]) depicts the average response time of the matrix multiplication application as a function of the LB gain. Notably, the theoretical, the MC-simulated, and experimental results show a fairly good agreement. In addition, for comparison purposes, the results for the no-failure case are also shown. From the theoretical curves we can observe that a proper task allocation can effectively reduce the average response time of an application. Note that the optimal number of tasks to reallocate is smaller in the scenario when CEs randomly fail and recover, as compared to the no-failure case. Intuitively, we can state that the optimal task reallocation in case of CE failure will always be less than the optimal task reallocation for the no-failure case.

### 5.2 The Responsive DLB Policy

In this policy, each CE initially executes a DLB action at time tb assuming that the CEs are totally reliable. In other words, the policy does not care about future CE failures and subsequent recoveries during the execution of the application. Therefore, the initial LB action is taken to achieve an "approximately" uniform division of the total workload of the DCS among all the nodes, assuming that all the CEs will remain functional. Once again, Eq. (1) is used to detect an imbalance and the $\Lambda_j$ parameters are defined as the

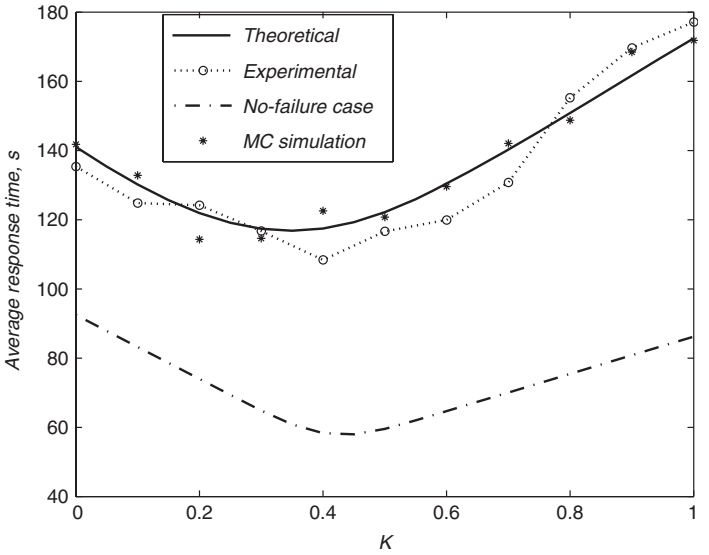



**FIGURE 1** The average response time of the matrix multiplication application as a function of the LB gain $K$ for the preemptive LB policy. Extracted from Figure 3 in [3].

processing rate of the CEs. The first difference with the preemptive DLB policy is that the LB gains are optimally selected solving a set of equations simpler than the one used by the preemptive DLB policy; these equations are stated in Eq. (9) in [2]. The second difference is that upon the occurrence of failure at any CE, the backup system of the failed CE executes an extra LB action in order to compensate for the time that will be wasted during the recovery process of the CE. Upon failure, the backup system of the failed CE reallocates tasks according to the following rule:

$$L_{jk}(t_f) = \left\lfloor \left(\frac{\lambda_{d,j}}{\lambda_{r,j}}\right)\left(\frac{\lambda_{d,k}}{\sum_{l=1}^{n}\lambda_{d,l}}\right)\left(\frac{\lambda_{r,j}}{\lambda_{r,j}+\lambda_{f,k}}\right)\right\rfloor \tag{4}$$

where the $\lambda_{r,j}$ is the recovery rate of the $j$th CE. Note that the first term at the right hand side of Eq. (4) is the average number of tasks that have not been served during the recovery time of the $j$th CE, the second term is the fair share of tasks of the receiving CE, and the third term is the steady-state probability of any CE to be functioning during the recovery time of the $j$th CE. Note that this, upon failure task reallocation, is fixed and determined by the parameters of the CEs.

Table 1 (extracted from Table II in [3]) lists the average response time achieved by the responsive DLB policy for some representative initial workload allocations. For comparison, we also list the average response time achieved by the preemptive DLB policy as well as the no-failure case. We can see that the responsive DLB policy outperforms the preemptive policy in all cases. In general, this behavior is observed for communication links where the transfer times per task are small (about 1 s per task). However, the preemptive DLB policy outperforms the responsive policy in scenarios where the communications times per tasks are larger than 1 s (more details shown in Table III in

**TABLE 1 Experimental and Simulation Results for the Responsive DLB Policy Applied in Scenarios Where Nodes Can Fail and Recover**

| | Responsive DLB Policy | | Preemptive DLB Policy | No Failure |
|---|---|---|---|---|
| Initial Workload | MC simulations | Experimental results | (Theoretical) | |
| (200,200) | 277.9 | 263.4 | 275.0 | 141.9 |
| (200,100) | 202.4 | 188.8 | 210.1 | 106.9 |
| (100,200) | 203.1 | 212.9 | 210.1 | 106.9 |
| (200,50) | 170.8 | 171.4 | 177.1 | 89.3 |
| (50,200) | 170.8 | 177.6 | 177.1 | 89.3 |

For comparison, results for the no-failure case and the preemptive DLB policy are also listed. Extracted from Table II in [3].

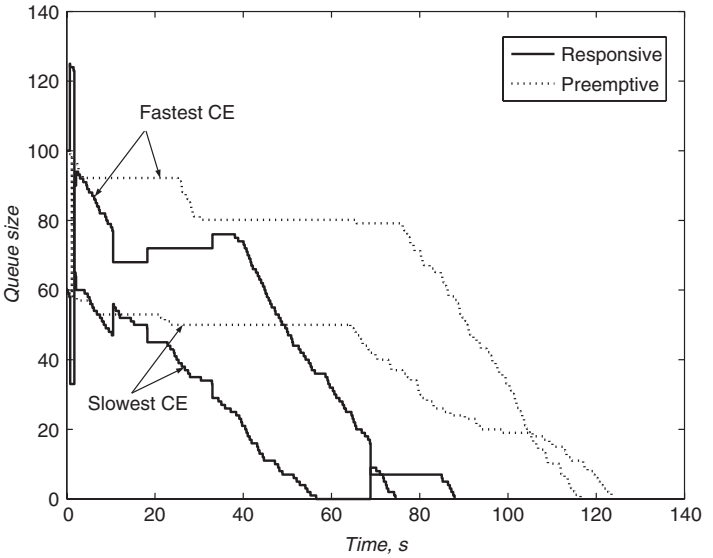



**FIGURE 2** A DCS where CEs can randomly fail and recover: a sample realization of the queues dynamics. Extracted from Figure 4 in [3].

[3]). Finally, in order to compare the dynamics of the DCS under each policy, we show in Figure 2 (extracted from Figure 4 in [3]) the actual queues at each CE during one realization of the experiments performed for the preemptive and responsive DLB policies. We can observe that the long flat portions of the queues correspond to the recovery times of the CEs. The downward (upward) jumps in the queues correspond to the action of transferring (receiving) tasks after every failure instant.

## 6 DLB POLICIES FOR SYSTEMS WHERE COMPUTING ELEMENTS FAIL PERMANENTLY

In harsh environments where nodes fail catastrophically, or during a time much longer than the average application response time, an appropriate metric of reliability is the

probability of successfully serving the application. Theorems 1 and 2 in [5] present the set of recurrence equations governing the dynamics of a DCS in the presence of this type of long-term failures. The DLB policies developed for this scenario employ Eq. (1) to determine the imbalances in the system. Unlike in the failure and recovery case, the $\Lambda_j$ parameters are defined also as the average failure time of the CEs, or alternatively, they can be defined as $\Lambda_j = \lambda_{d,j}\left(1 - \lambda_{f,j} \Big/ \sum_{l=1}^{n} \lambda_{f,l}\right)$. For this last definition, the $\Lambda_j$ parameters can be thought of as an *effective processing rate* of a CE, which penalizes the processing rate of a CE by its relative unreliability.

Figure 3 (extracted from Figure 2b in [5]) shows the probability of successfully serving an application, which we have denoted as $R^{\mathbf{I},\mathbf{F}}_{m_1,m_2}(t_b; \mathbf{C})$, as a function of the LB gains. We can observe again a remarkable agreement between theoretical, MC, and experimental results. We can see that the probability of successful completion seems to be convex as a function of the number of tasks to be reallocated. From our experience on the LB problem, we can say that the probability of successful completion (correspondingly, the average response time) has such concave (correspondingly, convex) shape when the communication network of the DCS exhibits notorious random transfer times.

Table 2 (extracted from Table 3 in [5]) lists the probability of success for different DLB policies. The policies differ in the balancing criterion used, that is, by the definition

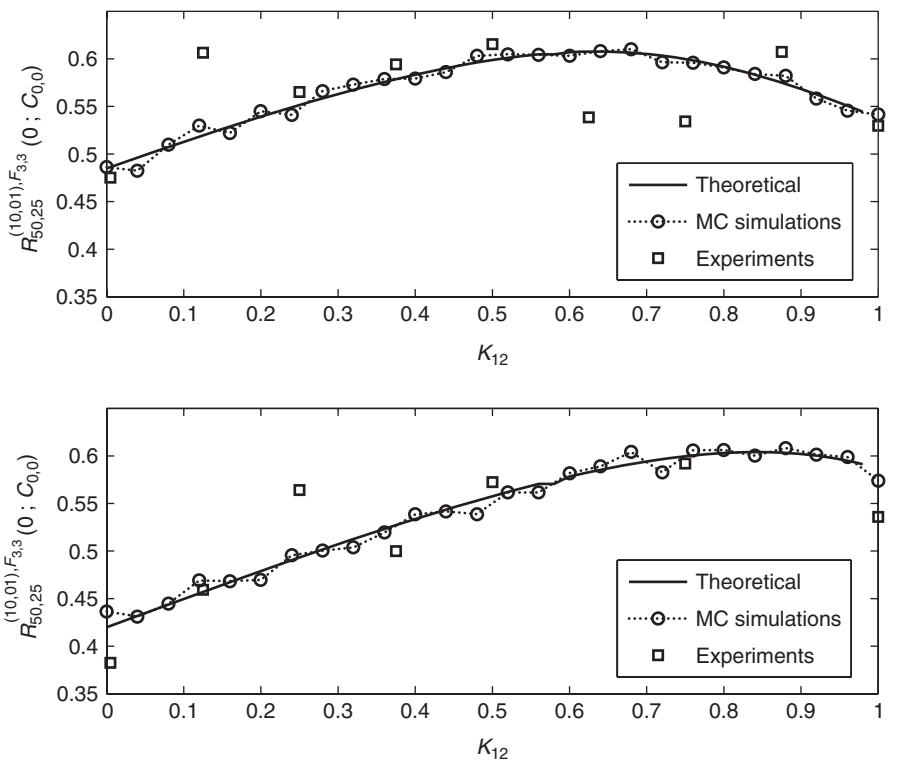



**FIGURE 3** The probability of successfully serving an application as a function of the LB gains. The example considers a DCS where CEs can catastrophically fail at any random time. Extracted from Figure 2b in [5].

**TABLE 2 The Probability of Successfully Serving an Application for Different Initial Workload Distribution**

| Initial Load ($m_1$,$m_2$,$m_3$,$m_4$,$m_5$) | Maximal-Service | Processing Speed | Complete | Optimum |
|---|---|---|---|---|
| (150,0,0,0,0) | 0.2338 | 0.1845 | 0.2223 | 0.2632 |
| (0,150,0,0,0) | 0.2853 | 0.2908 | 0.2653 | 0.2908 |
| (0,0,150,0,0) | 0.2868 | 0.2678 | 0.2760 | 0.2867 |
| (0,0,0,150,0) | 0.2915 | 0.2965 | 0.2978 | 0.2978 |
| (0,0,0,0,150) | 0.2545 | 0.2940 | 0.3125 | 0.3125 |
| (30,30,30,30,30) | 0.2953 | 0.3105 | 0.3045 | 0.3170 |
| (59,2,4,34,51) | 0.2579 | 0.2583 | 0.2868 | 0.3183 |
| (18,55,29,27,21) | 0.2943 | 0.3098 | 0.3053 | 0.3148 |
| (26,30,28,38,28) | 0.3185 | 0.2978 | 0.3040 | 0.3185 |
| (40,15,40,35,20) | 0.2860 | 0.2873 | 0.2845 | 0.2963 |

Different balancing criteria have been employed to balance the DCS. Extracted from Table 3 in [5].

of the $\Lambda_j$ parameters. The maximal-service policy defines the $\Lambda_j$'s in terms of the average failure time of the CEs, the processing speed policy defines the parameters in terms of the processing rate of the CEs, and the complete policy defines the parameters in terms of the *effective processing rate* of the CEs. In addition, we have considered an example where the fastest CEs are at the same time the less reliable ones. From the data given in Table 2, it can be concluded that a similar performance level can be achieved independently of the balancing criterion employed, thereby showing the strength of our approach. Finally, as shown in Figure 4 (extracted from Figure 2c in [5]), caution must

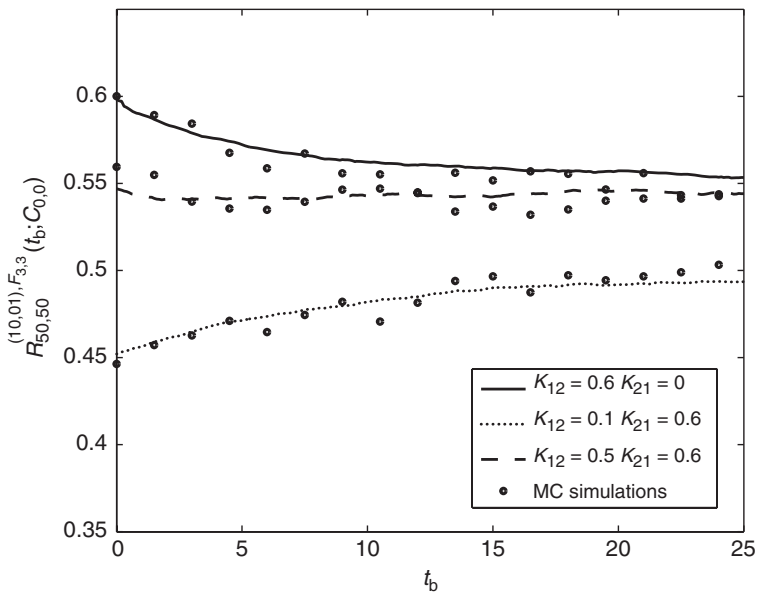



**FIGURE 4** The probability of successfully serving an application as a function of the balancing instant. The example considers a DCS where CEs can catastrophically fail at any random time. Extracted from Figure 2c in [5].

be exercised in the selection of the balancing instant and the LB gains; otherwise, the probability of successfully serving an application can be notoriously degraded, as in the LB policy where $K_{12} = 0.1$ and $K_{21} = 0.6$.

## 7 RESEARCH DIRECTIONS

More fundamental research on modeling complex computing infrastructures is needed, in order to predict and understand the response of such infrastructures in the presence of network and/or CE failures. Models must include the possibility of failures at different layers. For instance, models must consider long-term physical attacks such as those inflicted by WMDs, communication-layer attacks like network flooding, and application-layer attacks like those produced by malicious software. New models will significantly enhance the capabilities of homeland security to (i) optimize computing networks' performance and robustness in the presence of failures; (ii) warn users and operators about a system dysfunction and provide quantitative description of its magnitude; (ii) design modern computing networks that have superior resilience and robustness in the presence of failures.

There is also the need for developing models to characterize, from the point of view of a computing network, the environment and the extent of damage produced by severe attacks on a DCS. The random nature of these attacks demands for a statistical framework, where spatial and temporal correlations of the attacks must be considered. In addition, early detection mechanisms of infrastructure network attacks are also required. These detection mechanisms must be informed also about the spatiotemporal correlations associated with the attacks, so that we can develop smart detection systems capable of warning the users affected potentially by a certain attack.

## ACKNOWLEDGMENT

This work was supported by the Defense Threat Reduction Agency (Combating WMD Basic Research Program) and in part by the National Science Foundation (award ANI-0312611).

## REFERENCES

1. Shirazi, B. A., Kavi, K. M., and Hurson, A. R. (1995). *Scheduling and Load Balancing in Parallel and Distributed Systems*. IEEE Computer Society Press, Los Alamitos, CA.
2. Dhakal, S., Hayat, M. M., Pezoa, J. E., Yang, C., and Bader, D. A. (2007). Dynamic load balancing in distributed systems in the presence of delays: a regeneration-theory approach. *IEEE Trans. Parallel and Distrib. Syst*. **18**, 485–497.
3. Dhakal, S., Hayat, M. M., Pezoa, J. E., Abdallah, C. T., Birdwell, J. D., and Chiasson, J. (2006). Load balancing in the presence of random node failure and recovery. *Proceedings of IEEE IPDPS*, Rhodes, Greece.
4. Dhakal, S., Pezoa, J. E., and Hayat, M. M. (2007). A regeneration-based approach for resource allocation in cooperative distributed systems. *Proceedings of ICASSP*, Honolulu, HI, III-1261–III-1264.

5. Dhakal, S., Pezoa, J. E., and Hayat, M. M. (2008). *Maximizing Service Reliability in Distributed Computing Systems with Random Failures: Theory and Implementation*. Submitted to IEEE Trans. Parallel and Dist. Systems Paper available at http://www.ece.unm.edu/lb.

## FURTHER READING

Dhakal, S., Hayat, M. M., Elyas, M., Ghanem, J., and Abdallah, C. T. (2005). Load balancing in distributed computing over wireless LAN: effects of network delay. *Proceedings of IEEE WCNC*, New Orleans, LA.

Hayat, M. M., Dhakal, S., Abdallah, C. T., Birdwell, J. D., and Chiasson, J. (2004). Dynamic time delay models for load balancing. Part II: stochastic analysis of the effect of delay uncertainty. *Adv. in Time Delay Systems, LNCS* **38**, 355–368.

Dhakal, S., Paskaleva, B. S., Hayat, M. M., Schamiloglu, E., and Abdallah, C. T. (2003). Dynamical discrete-time load balancing in distributed systems in the presence of time delays. *Proceedings of IEEE CDC*, Maui, HI, 5128–5134.

*The Resource Allocation Group at the Electrical and Computer Engineering*, University of New Mexico, Albuquerque, NM. "The Resource Allocation GroupWebsite." Online since January (2003). Last update January 20th, 2009. http://www.ece.unm.edu/lb.

Sonnek, J., Chandra, A., and Weissman, J. (2007). Adaptive reputation-based scheduling on unreliable distributed infrastructures. *IEEE Trans. Parallel and Distrib. Syst*. **18**, 1551–1564.

Daley, D. J., and Vere-Jones, D. (1988). *An Introduction to the Theory of Point Processes*, Springer-Verlag Berlin, New York.

# PASSIVE RADIO FREQUENCY IDENTIFICATION (RFID) CHEMICAL SENSORS FOR HOMELAND SECURITY APPLICATIONS

RADISLAV A. POTYRAILO, CHERYL SURMAN, AND WILLIAM G. MORRIS
*General Electric Global Research Center, Niskayuna, New York*

## 1 INTRODUCTION

Development of new sensors is driven by the ever-expanding homeland security monitoring needs for the determination of chemical, biological, and nuclear threats

[1–4]. Over the last several decades, numerous principles of detection have been discovered, followed by the design and implementation of practical sensors and sensor arrays. New technologies for the detection of threats of importance to homeland security must be sensitive enough to detect agents below health risk levels, selective enough to provide minimal false-alarm rates, and rapid enough to enable an effective medical response [1]. This article provides a brief overview of chemical and biological threats, focuses in detail on modern concepts in chemical sensing, examines the origins of the most significant unmet needs in existing chemical sensors, and introduces a new philosophy in selective chemical sensing. This new approach for selective chemical sensing involves the combination of a sensing material that has different response mechanisms to different species of interest with a transducer that has a multivariable signal transduction ability to detect these independent changes. In the numerous laboratory and field experiments, the action of several response mechanisms in a single sensing film to different vapors was demonstrated, which resulted in the independent detection of these responses with a single sensor and correction for variable ambient conditions, including high levels of ambient relative humidity (RH).

## 2 BACKGROUND

Chemical sensors have found their niche among modern analytical instruments when real-time determination of the concentration of specific sample constituents is required. On the basis of a variety of definitions of sensors [5, 6], here we accept that a chemical sensor is an analytical device that utilizes a chemically responsive sensing layer to recognize a change in a chemical parameter of a measured environment and to convert this information into an analytically useful signal. In such a device (Fig. 1), a sensing material is applied onto a suitable physical transducer to convert a change in a property of a sensing material into a suitable form of energy. The obtained signal from the transducer is further processed to provide useful information about the concentration of species in the sample. The energy-transduction principles that have been employed for chemical sensing involve radiant, electrical, mechanical, and thermal types of energy [7]. As shown in Figure 1, in addition to a sensing material layer and a transducer, a modern sensor system often incorporates other important components such as sample introduction and data-processing components. A critical aspect of a modern sensor system is also its packaging design and implementation.

Compared to chemical sensing based on intrinsic analyte properties (e.g. spectroscopic, dielectric, and paramagnetic), indirect sensing using a responsive material expands the range of detected species, can improve sensor performance (e.g. analyte

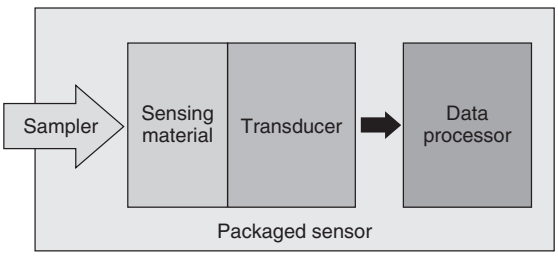



**FIGURE 1** Main components of a modern chemical sensor system.

detection limits), and is more straightforwardly adaptable to miniaturization (e.g. through micro-electro-mechanical system (MEMS) or self-assembly). However, a possible challenge of the indirect sensing approach is a trade-off between the selectivity of response to an analyte of interest in a multicomponent complex sample and sensor reversibility.

Innovative ideas for sensors originate from new technological capabilities in sample manipulation [8], sensing materials [6, 9–11], transducer designs [12, 13], micro- and nanofabrication of transducers [14], wireless and proximity communication [15], and energy scavenging [16]. Although the design of a sensor for a particular application will be dictated by the nature and requirements of that application, it is useful to set down the features, listed in Table 1, that one would wish of an ideal sensor for chemical species. In real-world applications, the qualities of an ideal sensor are often weighted differently according to application. For example, low false-alarm rate and high probability of detection are among the most important requirements for homeland security applications [1, 17, 18]. The most important respects in which existing chemical sensors require additional improvements include long-term stability, selectivity, detection limits, and response speed [1].

A known problem in chemical sensing is cross sensitivity of individual chemical sensors to chemical compounds other than compounds of interest. For example, Figure 2

**TABLE 1 Typical Requirements for an Ideal Sensor**

| | |
|---|---|
| Low false-alarm rate | Low initial cost |
| High probability of detection | Low operation cost |
| Broad dynamic range | Response reversibility |
| High sensitivity | Small size |
| High selectivity | Low power consumption |
| High long-term stability | Robustness |
| Maintenance simplicity | Self-calibration |
| High response speed | Ergonomic design |

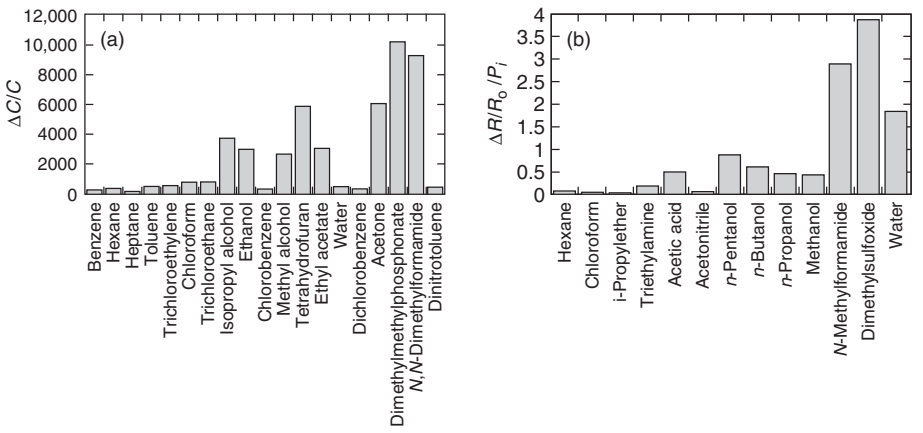



**FIGURE 2** Typical cross sensitivity of response of different types of sensing materials to a variety of vapors: (a) capacitance response pattern of single-wall carbon nanotubes and (b) resistance response pattern of $LiMo_3Se_3$ nanowires. (a) Adapted from Reference [19] with permission and (b) adapted from Reference [20] with permission.

illustrates typical cross sensitivity of response of different types of sensing materials to a variety of vapors [19, 20]. Design of sensing materials that are selective to small molecules is challenging [6, 9, 10]. A common approach to address this problem is to build an array of partially selective sensors and to process the array response using multivariate analysis [21]. In such sensor arrays, individual transducers are coated with sensing materials and one response per sensing material (e.g. resistance, current, capacitance, work function, mass, temperature, optical thickness, and light intensity) is measured. An example of such a response of a sensor array is presented in Figure 3, where four sensors were combined into an array for analysis of toxic vapors of chlorinated organic solvents [22]. Although individual sensors in the array were only partially selective, the operation of the sensor array made possible discrimination not only perchloroethylene (PCE), trichloroethylene (TCE), and vinyl chloride (VC) but also three isomers of dichloroethylene (DCE), such as *cis*-1,2-DCE, *trans*-1,2-DCE, and 1,1-DCE. Such discrimination was accomplished with multivariate analysis, such as principal components analysis (PCA) [21]. Using identical transducers in the array simplifies array fabrication, whereas combining transducers based on different principles or employing transducers that measure more than one property of a sensing film [13] could improve array performance through hyphenation. Minimization of the number of sensors in an array is attractive because of simplification of data analysis, reduction of data-processing noise, simplification of sensing materials deposition, and simplification of device fabrication [6, 10, 12, 14, 21].

In designing a chemical sensor system with a single transducer or an array of transducers, attention should be paid to specific design requirements of each system component (sampler, sensing material, transducer, and data processor) and how these components are packaged. Table 2 highlights some of the key challenges and sensor-design aspects for each system component and for the packaged chemical sensor system. Table 3 presents

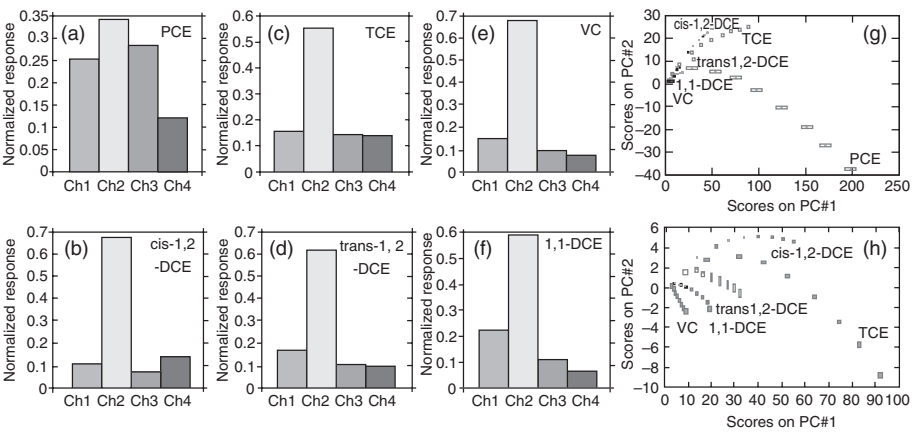



**FIGURE 3** Example of operation of a four-sensor array for the detection of toxic vapors of chlorinated organic solvents: (a–f) Partially selective responses of four sensors in the array to 100 ppm of PCE, *cis*-1,2-DCE, TCE, *trans*-1,2-DCE, VC, and 1,1-DCE. (g, h) Score plots of the first two principal components for the data set obtained from the response of the four-sensor array to (g) six and (h) five toxic vapors of chlorinated organic solvents at different concentrations ranging from 0 to 100 ppm. Each data point in (g, h) is the mean of three measurements, rectangles represent one standard deviation. Adapted from Reference [22] with permission.

**TABLE 2 Examples of Challenges and Sensor-Design Aspects Associated with Gas-Phase Chemical Sensing**

| Component | Challenges | Sensor-Design Aspects |
|---|---|---|
| Sampler | Particulate contamination<br>Lack of representative sample for trace analysis | Preconcentration for detection limit improvement<br>Integration into periodic self-cleaning sensor system |
| Sensing Material | Film poisoning<br>Film aging<br>Water condensation | Temperature-stabilized operation<br>Temperature, gas-flow modulation to facilitate more reversible and selective response |
| Transducer | Signal-to-noise decrease with reduced transducer size<br>Difficult readout from miniaturized transducer | Transducer design for higher order sensor response through hyphenated transduction techniques for selectivity, signal-to-noise, and stability improvement |
| Data processor | Reliable quantitation of multiple analytes in mixtures using partially selective sensing films and conventional sensor arrays<br>Detection of low levels of analytes in the presence of high levels of interferences | Analysis of dynamic signatures for selectivity and stability improvement<br>Analysis of multivariate signatures for selectivity, signal-to-noise, and stability improvement |
| Packaged system | Calibration drift<br>Relatively large system size with sampler, battery, and data communicator | Self-calibration<br>Power harvesting or wireless power |

several examples of existing available individual sensors and sensor array systems for the detection of vapors of interest in homeland security applications.

## 3 THREATS, CHALLENGES, AND NEW TECHNICAL SOLUTIONS

To respond to chemical and biological threats, in addition to available analytical instrumentation [2] and sensor systems for homeland security applications (Table 3), new technologies with previously unavailable capabilities are needed. New technologies for the detection of threats of homeland security importance must satisfy at least three goals. They must be sensitive enough to detect agent concentrations at or below health risk levels, selective enough to provide acceptable false-alarm rates, and prompt enough to enable an effective medical response [1]. Out of these goals, *high selectivity* of chemical detection using existing sensor systems represents the most significant challenge. Significant *sensor sensitivity* improvements were demonstrated using new transducer designs and high-surface area sensing nanomaterials, whereas a significant increase in the *response speed* was demonstrated using high-surface area sensing nanomaterials [6, 10].

**TABLE 3 Representative Examples of Commercially Available Individual Chemical Sensors and Sensor Array Systems**

| Individual Sensor or Sensor Array | Classes of Analytes | Company |
|---|---|---|
| Electrochemical sensors | Toxic industrial chemicals | City Technology Ltd, Portsmouth, Hampshire, UK www.citytech.com |
| Electrochemical and semiconductor sensors | Toxic industrial chemicals | Delphian Corp., Northvale, NJ, USA www.delphian.com |
| Metal oxide semiconductor sensors | Toxic industrial chemicals | Figaro Engineering Inc., Osaka, Japan www.figaro.co.jp |
| Array of interdigitated electrodes | Analytes of homeland security and defense relevance | Smiths Detection-Pasadena, Inc. (former Cyrano Sciences, Inc.), Pasadena, CA, USA www.smithsdetection.com |
| Array of surface-acoustic wave devices | Chemical warfare agents, toxic industrial chemicals | MSA, Pittsburgh, PA, USA www.msanorthamerica.com |
| Array of colorimetric sensing films | Toxic industrial chemicals | ChemSensing, Inc., Northbrook, IL, USA www.chemsensing.com |

An attractive technical solution to the insufficient selectivity of existing sensors is to implement a new recently contemplated and experimentally demonstrated sensing concept for selective sensing that requires only a single sensor rather than a sensor array [23, 24]. This new concept involves the combination of a sensing material that has different response mechanisms to different species of interest with a transducer that has a multivariable signal transduction ability to detect these independent changes. In the numerous laboratory and field experiments, the action of several response mechanisms in a single sensing film to different vapors was demonstrated, which resulted in the independent detection of these responses with a single sensor and correction for variable ambient conditions.

## 3.1 Threats

In the foreseeable future, the United States and other nations will face an existential threat from the intersection of terrorism and weapons of mass destruction. Chemical agents (CAs), toxic industrial materials (TIMs), and biological agents (BAs) are among those compounds that are expected, by homeland security experts, to be utilized in future terrorist attacks [18].

***3.1.1 Chemical Agents.*** Toxic chemical substances that are intended to kill, seriously injure, or seriously incapacitate people through their physiological effects are known

as *chemical agents* (*CAs*) or *chemical warfare agents* (*CWAs*) [2, 3, 25]. During the twentieth century, over 50 different chemicals in liquid, gas, or solid form have been used and stockpiled as CAs. CAs can be organized into several categories (which can slightly vary in different literature sources) according to the manner in which they affect the human body. *Nerve agents* disrupt the mechanism by which nerves transfer messages to organs. *Blister* (*vesicant*) *agents* cause severe skin, eye, and mucosal pain and irritation. *Pulmonary* (*choking*) *agents* attack lung tissue, primarily causing pulmonary edema. *Blood agents* prevent the body from utilizing oxygen. Representative examples of CAs are listed in Table 4 [2, 3]. Other types of less lethal CAs include riot-control agents (e.g. pepper spray with capsaicin as an active ingredient and tear gas with *ortho*-chlorobenzylidene-malononitrile or chloroacetophenone as an active ingredient) and incapacitating agents (e.g. 3-quinuclidinyl benzilate, fentanyl-based Kolokol-1).

***3.1.2 Toxic Industrial Materials.*** TIMs are industrial chemicals other than CAs that also have harmful effects on humans [2, 4]. TIMs are also often referred to as *toxic industrial chemicals* (*TICs*). They have a $LCt_{50}$ value (lethal concentration for 50% of the population multiplied by exposure time) less than 100 g min/m$^3$ in any mammalian species and are produced in quantities $>30$ ton/year at a given production facility. Although they are not as lethal as the highly toxic CAs, their ability to make a significant impact on the population is related to the amount of TIMs that can be released during a terrorist attack.

TIMs are ranked in three categories with respect to their hazard index ranking, indicating their relative importance. A *high hazard* ranking indicates a widely produced, stored, or transported TIM that has high toxicity and is easily vaporized. A *medium hazard* ranking indicates a TIM that may rank high in some categories but lower in others such as number of producers, physical state, or toxicity. A *low hazard* ranking indicates that this TIM is not likely to be a hazard unless specific operational factors indicate otherwise. Table 5 [2] summarizes TIMs by their hazard index. Many TIMs are toxic-by-inhalation (TIH) gases. The top four TIH gases that account for 55% of all highly hazardous chemical processes are listed in Table 6 [4].

***3.1.3 Biological Agents.*** BAs, on the basis of their potential harmful nature, are classified into three categories [18, 25, 26]. *Category A* agents are those that can be easily disseminated or transmitted from person to person, cause high mortality rates, and have the potential for major public health problems as well as disruption of social life. *Category B* agents are next in the priority and include those that are moderately easy to disseminate and result in moderate morbidity rates and low mortality rates. *Category C* contains the third highest priority agents that include emerging pathogens that are easily available and can be produced in large quantity without a significant laboratory setting and have the potential to be engineered for mass dissemination. Selected BAs are summarized in Table 7 [18, 25, 26].

## 3.2 Challenges in Chemical Sensing of Homeland Security Threats

High selectivity of chemical detection of homeland security threats using existing sensor systems is the most significant challenge. The fundamental reason for the cross sensitivity of individual sensors to different detected species is the need to meet two conflicting

**TABLE 4 Categories of Chemical Agents [2, 3, 25]**

| Nerve Agents | Blister (Vesicant) Agents | Pulmonary (Choking) Agents | Blood Agents |
|---|---|---|---|
| GA –Tabun | HD –Sulfur mustard | CG –Phosgene | CK –Cyanogen chloride |
| GB –Sarin | HN –Nitrogen mustard | DP –Diphosgene | AC –Hydrogen cyanide |
| GD –Soman | L –Lewisite | Cl –Chlorine | SA –Arsine |
| GF –Cyclosarin | MD –Methyldichloroarsine | PS –Chloropicrin | KCN –Potassium cyanide |
| VX –Methylphosphonothioic acid | PD –Phenyldichloroarsine | DM –Adamsite | NaCN –Sodium cyanide |
| Novichok | ED –Ethyldichloroarsine | BCME –*Bis*(chloromethyl) ether | |

**TABLE 5 TIMs Listed by Hazard Index [2]**

| High | Medium | Low |
|---|---|---|
| Ammonia | Acetone cyanohydrin | Allyl isothiocyanate |
| Arsine | Acrolein | Arsenic trichloride |
| Boron trichloride | Acrylonitrile | Bromine |
| Boron trifluoride | Allyl alcohol | Bromine chloride |
| Carbon disulfide | Allylamine | Bromine pentafluoride |
| Chlorine | Allyl chlorocarbonate | Bromine trifluoride |
| Diborane | Boron tribromide | *n*-Butyl chloroformate |
| Ethylene oxide | Carbon monoxide | sec-Butyl chloroformate |
| Fluorine | Carbonyl sulfide | *n*-Butyl isocyanate |
| Formaldehyde | Chloroacetone | *tert*-Butyl isocyanate |
| Hydrogen bromide | Chloroacetonitrile | Carbonyl fluoride |
| Hydrogen chloride | Chlorosulfonic acid | Chlorine pentafluoride |
| Hydrogen cyanide | Diketene | Chlorine trifluoride |
| Hydrogen fluoride | 1,2-Dimethylhydrazine | Chloroacetaldehyde |
| Hydrogen sulfide | Ethylene dibromide | Chloroacetyl chloride |
| Nitric acid, fuming | Hydrogen selenide | Crotonaldehyde |
| Phosgene | Methanesulfonyl chloride | Cyanogen chloride |
| Phosphorus trichloride | Methyl bromide | Dimethyl sulfate |
| Sulfur dioxide | Methyl chloroformate | Diphenylmethane-4,4'-diisocyanate |
| Sulfuric acid | Methyl chlorosilane | Ethyl chloroformate |
| Tungsten hexafluoride | Methyl hydrazine | Ethyl chlorothioformate |
| | Methyl isocyanate | Ethyl phosphonothioic dichloride |
| | Methyl mercaptan | Ethyl phosphonic dichloride |
| | Nitrogen dioxide | Ethyleneimine |
| | *n*-Octyl mercaptan | Hexachlorocyclopentadiene |
| | Phosphine | Hydrogen iodide |
| | Phosphorus oxychloride | Iron pentacarbonyl |
| | Phosphorus pentafluoride | Isobutyl chloroformate |
| | Selenium hexafluoride | Isopropyl chloroformate |
| | Silicon tetrafluoride | Isopropyl isocyanate |
| | Stibine | Nitric oxide |
| | Sulfur trioxide | Parathion |
| | Sulfuryl chloride | Perchloromethyl mercaptan |
| | Sulfuryl fluoride | *n*-Propyl chloroformate |
| | Tellurium hexafluoride | Tetraethyl lead |
| | Titanium tetrachloride | Tetraethyl pyroposphate |
| | Trichloroacetyl chloride | Tetramethyl lead |
| | Trifluoroacetyl chloride | Toluene 2,4-diisocyanate |
| | | Toluene 2,6-diisocyanate |

requirements, such as sensor reversibility and sensor selectivity. High reversibility of sensor response should be achieved *via low energy* of interactions between the analyte and the sensing film, whereas high selectivity of sensor response should be achieved *via high energy* of interactions between the analyte gas and the sensing film. As a result, individual sensors and sensor arrays often cannot detect minute analyte concentrations in the presence of elevated levels of interferences, for example water vapor in air. Figure 4 [27, 28] illustrates typical degradation of the ability to detect low concentrations of

**TABLE 6 Top Four TIH Gases that Account for 55% of All Highly Hazardous Chemical Processes [4]**

| TIH Gas | Percent from All Highly Hazardous Chemical Processes | Absolute Number Of Chemical Processes |
|---|---|---|
| Anhydrous ammonia | 32.5 | 8343 |
| Chlorine | 18.3 | 4682 |
| Sulfur dioxide | 3 | 768 |
| Hydrogen fluoride | 1.2 | 315 |

**TABLE 7 Biological Agents, Categorized Based on Their Potential Harmful Nature [18, 25, 26]**

| Category A | Category B | Category C |
|---|---|---|
| *Bacillus anthracis* (anthrax) | *Burkholderia pseudomallei* | Tickborne hemorrhagic fever viruses (*Crimean-Congo Hemorrhagic fever virus*, Tickborne encephalitis viruses, *Yellow fever virus*, Multidrug-resistant TB, *Influenza virus*, *Rabies virus*) |
| *Clostridium botulinum* | *Coxiella burnetti* (Q fever) | |
| *Yersinia pestis* | Brucella species (brucellosis) | |
| Variola major (smallpox) and other pox viruses | *Burkholderia mallei* (glanders) | |
| *Francisella tularensis* (tularemia) | Ricin toxin (from Ricinus communis) | |
| Viral hemorrhagic fevers (*Arenaviruses*, *Orthobunyavirus*, *Flaviruses*, *Filoviruses*) | Epsilon toxin of Clostridium perfringens | |
| | Staphylococcus enterotoxin B | |
| | Typhus fever (*Rickettsia prowazekii)* | |
| | Food and Waterborne Pathogens Bacteria (Diarrheagenic *Escherichia coli*, Shigella species, Salmonella, *Listeria monocytogenes*, *Campylobacter jejuni*, *Yersinia enterocolitica*), Viruses (*caliciviruses*, *Hepatitis A*), Protozoa (*Cryptosporidium parvum*, *Cyclospora cayatanensis*, *Giardia lamblia*, *Entamoeba histolytica*) | |

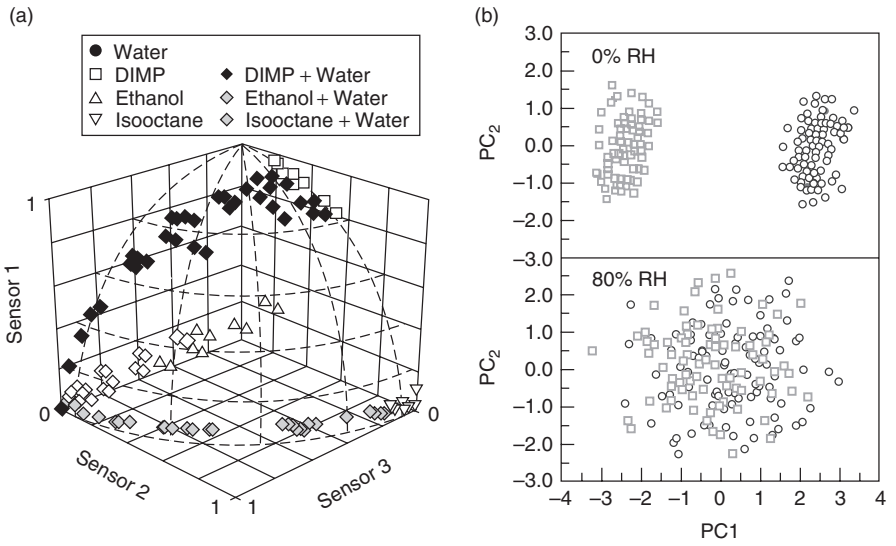



**FIGURE 4** Typical effects of water vapor in air on the ability to selectively detect analyte vapors using conventional sensor arrays. (a) Normalized responses of three polymer-coated chemiresistor sensors to diisopropylmethylphosphonate (DIMP), ethanol, and isooctane, mixed with water vapor at concentrations from 0 to 100%. The responses to binary mixtures of solvent and water vapor form "trails" on the surface of the sphere from pure water vapor to the pure solvent vapor. (b) Principal components score plots of an array of 10 chemiresistors coated with diverse surface-functionalized single-wall carbon nanotubes sensing films upon exposure to two types of vapor mixtures (squares and circles) at 0 and 80% RH. (a) Adapted from Reference [27] with permission and (b) adapted from Reference [28] with permission.

analyte vapors in the presence of relatively high levels of water vapor. Thus, it is critical that new sensors for homeland security applications will be not disappointingly affected by variable levels of water vapor in air, with concentrations up to 50–95% of its saturated $H_2O$ vapor pressure. There are also many other interferences of significance to homeland security applications in measured air. Some typical examples of additional interferences tested with sensors include vapors of diesel fuel, gasoline, floor stripper and polish formulations, disinfectant bleach, machine oil, and many others. However, concentrations of these interferences are much less, typically only up to 1–5% of their saturated vapor pressure [29]. Thus, the key successful phase in the development of new sensors is their ability to operate in the presence of high concentrations of water vapor in air.

### 3.3 Technical Solution—New Sensor Platform with Multivariable Signal Transduction

Over the years, wireless proximity-operated sensors have been reported based on diverse transducer designs such as resonant inductor–capacitor, magnetoelastic, thickness shear mode, and surface-acoustic wave transducers [24]. Radiofrequency identification (RFID) tags have been recognized as one of the disruptive technologies and are widely used ranging from the detection of unauthorized opening of containers to automatic identification of animals and to tracking of a wide variety of assets [30, 31]. Although usual RFID tags are ubiquitously employed as electronic labels and can cost only 5c in

large quantities [32], known approaches of RFID sensing typically require a battery or a proprietary-redesigned integrated circuit (IC) memory chip with typically a one-bit analog input [30, 33] preventing the wide adoption of RFID devices for sensing. Although battery-powered active RFID sensors transmit data over large distances, unfortunately, the battery adds to the system maintenance and complexity and reduces system's life. Passive devices are attractive when there is a need for the smallest sensor size, when a sensor is deployed for a long-term application, when a high power RF transmission is prohibited, or when the sensor should be disposable or low cost.

Recently, ubiquitous passive RFID tags were adapted for unusually selective chemical sensing [23, 24]. By applying a carefully selected sensing material onto the resonant antenna of the RFID tag and measuring the complex impedance of the antenna, the impedance spectrum response was correlated to the concentration of a chemical compound of interest in the presence of high levels of background interferences. The digital data were also written into and read from the IC memory chip of the RFID tag. This IC memory chip stored sensor calibrations and user-defined information. Using this attractive sensing platform, a new concept for selective vapor sensing has been contemplated and experimentally demonstrated. This new sensing principle requires only a single sensor and involves the combination of a sensing material that has different response mechanisms to different vapors with a transducer that has a multivariable signal transduction ability to detect these independent changes. In numerous experiments, the action of several vapor-response mechanisms in a single sensing film to different vapors was demonstrated and the independent detection of these responses with such single sensor was performed.

Compared to other sensor technologies (summarized in exemplary references [2, 10, 12–14] and Table 3), developed RFID sensors have a significantly improved response selectivity to analytes, are able to detect several analytes with a single sensor, and are able to reject effects from interferences.

***3.3.1 Principle of Chemical Sensing with RFID Sensors.*** The operation principle of chemical RFID sensors is illustrated in Figure 5 [24]. Reading and writing of digital information into the RFID sensor and measurement of complex impedance of the RFID sensor antenna are performed via mutual inductance coupling between the RFID sensor antenna and the pickup coil of a reader (Fig. 5a). A conventional digital RFID reader acquires digital data from an IC memory chip on the RFID sensor. This digital data have a unique factory programmed serial number (chip ID) as well as user-written data about the properties of the sensor (e.g. calibration curves for different conditions) and the object to which the sensor is attached (e.g. fabrication and expiration dates).

The origin of response of RFID sensor to chemical parameters is described in Figure 5 b and c. Upon reading of the RFID sensor with a pickup coil, the electromagnetic field generated in the RFID sensor antenna extends out from the plane of the RFID sensor (Fig. 5b) and is affected by the dielectric property of an ambient environment. When the resonant antenna of the RFID sensor is coated with a sensing film (Fig. 5c), the analyte-induced changes in the dielectric and dimensional properties of the sensing film affect the complex impedance of the antenna circuit through the changes in film resistance $R_F$ and capacitance $C_F$ between the antenna turns (inset of Fig. 5c). Such changes facilitate diversity is the response of individual RFID sensors and provide the opportunity to replace a whole array of conventional sensors with a single vapor-selective RFID sensor.

For selective analyte quantitation using individual RFID sensors, complex impedance spectra of the resonant antenna are measured as shown in Figure 5d. Several parameters

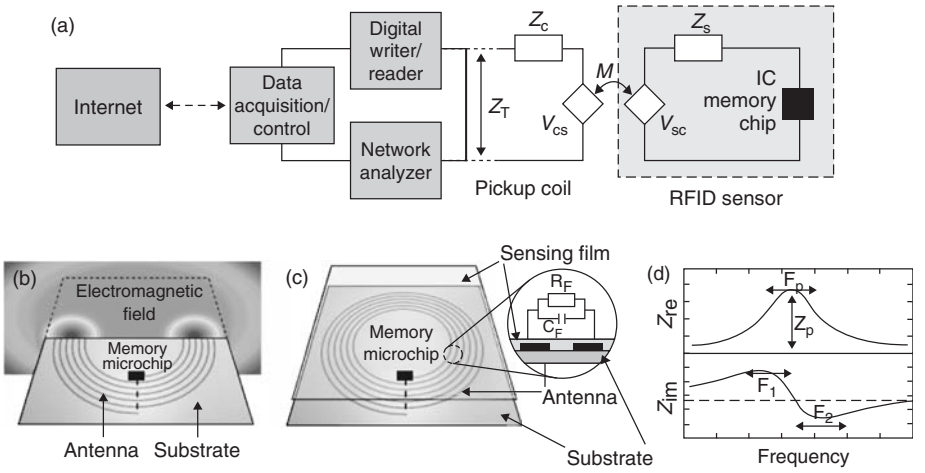



**FIGURE 5** Operation principle of passive battery-free RFID sensors. (a) System schematic of writing and reading digital information into the sensor IC memory chip and measuring complex impedance of the sensor antenna. $Z_C$ and $Z_S$ are intrinsic impedance of the pickup coil and sensor, respectively; $Z_T$ is total impedance; $V_{CS}$ and $V_{SC}$ are dependent voltage sources; and $M$ is mutual inductance coupling. (b) Visualization of the electromagnetic field in the resonant-sensing antenna that is generated upon excitation with a pick up coil of the sensor reader. (c) Origin of response of RFID sensors to chemical parameters via a sensing film deposited onto the resonant antenna. Inset, analyte-induced changes in the film affect the complex impedance of the antenna circuit through the changes in film resistance $R_F$ and capacitance $C_F$ between the antenna turns. (d) Measured complex impedance spectrum (real part $Z_{re}$ and imaginary part $Z_{im}$ of complex impedance) and representative parameters for multivariate analysis: frequency of the maximum of the real part of the complex impedance ($F_p$), magnitude of the real part of the complex impedance ($Z_p$), resonant frequency of the imaginary part of the complex impedance ($F_1$), and antiresonant frequency of the imaginary part of the complex impedance ($F_2$). Adapted from Reference [24] with permission.

from the measured real and imaginary portions of the complex impedance are further calculated. Examples of calculated parameters include frequency of the maximum of the real part of the complex impedance ($F_p$), magnitude of the real part of the complex impedance ($Z_p$), resonant frequency of the imaginary part of the complex impedance ($F_1$), and antiresonant frequency of the imaginary part of the complex impedance ($F_2$). Additional parameters can also be calculated (e.g. zero-reactance frequency and quality factor). However, the use of $F_p$, $F_1$, $F_2$, and $Z_p$ was found adequate for selective sensing. Upon a proper selection of a sensing film, the film-coated RFID sensor has responses different for each tested analyte or the analyte and interferences. By applying multivariate analysis of the full complex impedance spectra or the calculated parameters, quantitation of analytes and their mixtures with interferences is performed with individual RFID sensors. Examples of RFID tags adapted for sensing are presented in Figure 6.

***3.3.2 Comparison of Analog and Digital RFID Sensor-Data Transfer.*** Wireless sensors are under development as passive (battery-free) and active (battery-powered) devices for diverse applications, where a connection between the sensor and the reader without an electrical contact is important. Battery-powered sensors have an obvious advantage of data transmission over large distances [30]. At the same time, a battery adds to the system

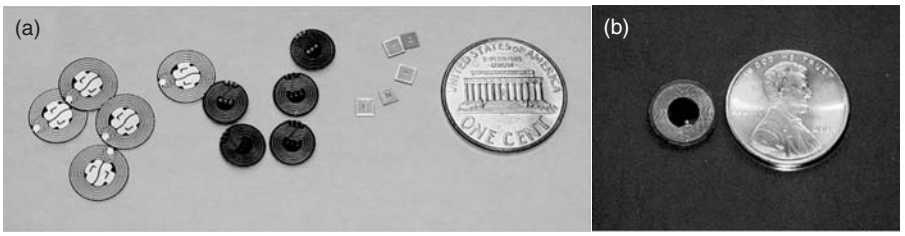



**FIGURE 6** Examples of different sizes and form-factors of conventional RFIDs adapted for sensing: (a) RFID tags from different manufacturers adapted for sensing and utilized in initial experiments and (b) RFID sensor with an antenna structure specifically developed for sensing application.

maintenance and complexity, reduces system life, and limits the temperature range of sensor applications. Although a possible alternative is scavenging of ambient energy (solar, mechanical, thermal, etc.) [16], at present, power scavenging is not mature enough for its wide applicability [34]. Passive devices are more attractive in situations when there is a need for the smallest sensor size, when a sensor is deployed for a long-term application, when a high power RF transmission is prohibited, or when the sensor should be of low cost or disposable.

In passive sensors, two broad approaches for sensor-data transfer include analog and digital data transfer as summarized in Table 8 [24]. In digital data transfer, sensor circuits are limited to very simple designs because of the need for enough available electrical power to operate. As a result, these sensors often have only one-bit resolution [30, 33] and, therefore, they only operate as threshold switches without capability to provide continuous sensing information. For example, RFID temperature-threshold sensors [35] last only for one measurement because they change their state irreversibly upon reaching a temperature threshold. Performance of such RFID sensor depends on the design of the IC memory chip with an analog input. Even with an increase in the resolution of an analog-to-digital converter of an IC memory chip, these digital sensors will measure only a *single parameter per sensor* and, thus, will suffer from environmental interference effects similarly to other reported sensors. The RFID readers of digital sensors typically operate with their own proprietary digital protocols but cannot affect the quality of sensor performance. In sensors with digital signal transmission, the mutual inductance coupling between the pickup coil and the sensor needs to be controlled in order to avoid possible bit errors. Operation of a sensor coupled to the analog sensor input of the IC memory chip also requires significant power. Thus, the read range of such sensors is significantly less.

In analog data transfer, the sensing capability resides in design of both the RFID sensor antenna and RFID sensor reader. The synergistic combination of the resonant antenna design of the RFID sensor and the sensing film deposited onto the antenna provides the foundation for the selective and sensitive sensor response. However, it is the RFID sensor reader that is responsible for the high resolution and signal-to-noise ratio of the acquired signal. Typical resolution of the sensor reader is 16 bit (vs. 1-bit resolution of available digital sensors). RFID sensors with analog data transfer measure the complex impedance of the resonant sensor antenna, combine *several measured parameters* from the antenna with multivariate data analysis, and deliver unique capability for multianalyte sensing and rejection of interferences using only a single sensor.

**TABLE 8 Key Features of Analog and Digital Sensors in Passive Inductively Coupled RFID Devices [24]**

| Sensor Performance Parameters | Capabilities of Analog Sensor-Data Transfer | Capabilities of Digital Sensor-Data Transfer |
|---|---|---|
| Opportunities in sensor–reader combination | Basis of RFID sensors is a standard low-cost RFID tag | Basis of RFID sensor is a custom IC chip with analog input on RFID tag |
| | Sensing performed by add-ons to standard RFID tag | Sensing performed by adding a separate sensor to IC chip |
| | Key monitoring capabilities are in RFID sensor reader that measures complex impedance of sensor | Key monitoring capabilities are in RFID tag with attached sensor |
| Measurement resolution | Typical 16-bit resolution provided by design of RFID sensor reader | Typical 1-bit resolution provided by design of IC chip |
| Multianalyte sensing and rejection of environmental interferences by a single sensor | Available by using multivariate analysis of measured complex impedance of resonant RFID antenna | Unavailable because only a single parameter per sensor is measured |
| Effects of variable mutual inductance coupling | Lead to sensor errors, however corrected using several methods | Lead to sensor bit errors, difficult to correct |
| Communication range | Several centimeters, limited to size of employed pickup coil | Several centimeters, limited by power for custom IC chip with analog input |
| Prospect as universal platform for physical, chemical, and biological sensing | Common sensor platform for measurements of physical, chemical, and biological parameters | Need for different separate sensors to be attached to RFID tag to detect different environmental parameters |

***3.3.3 RFID Dosimeter for Exposure to TIMs.*** Developed RFID sensors were tested for the detection of TIMs. Ammonia was selected as an analyte of choice based on its high hazard index (Table 5) and because ammonia tops the list of TIH gases (Table 6). As sensing materials, intrinsically conducting polymers (ICPs) were chosen for selective determination of vapors because of three key reasons [6, 9–11, 36]: (i) ICPs can exhibit several mechanisms of molecular recognition of gases that include changes in density of charge carriers, changes in mobility of charge carriers, polymer swelling, and conformational transitions of polymer chains. (ii) ICPs can be more sensitive than other sensing materials due to their inherent electrical transport property and energy migration. (iii) The inherent electrical transport property of ICPs is the material bulk transport property; thus, the readout of this material property can be more sensitive than potentiometric and amperometric methods that depend on local electronic structure.

As a sensing material in these experiments, polyaniline (PANI) was selected because it is a well-studied ICP for vapor sensing [11]. The response mechanism of PANI to $NH_3$ involves polymer deprotonation, whereas the response mechanism to $H_2O$ involves formation of hydrogen bonds and swelling [37]. Results of sensor exposures to $NH_3$ and $H_2O$ vapors are presented in Figure 7a–d. Deprotonation of the film upon $NH_3$

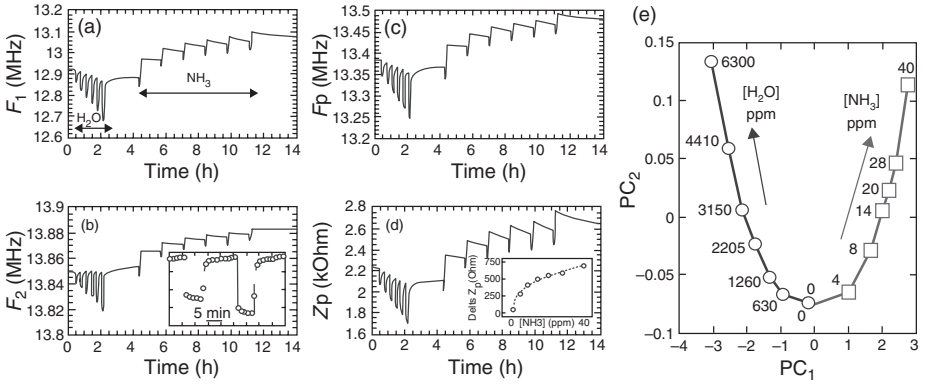



**FIGURE 7** Selective analysis of $NH_3$ and $H_2O$ vapors using a single sensor with the multivariable signal transduction. (a–d) Sensor responses $F_1$, $F_2$, $F_p$, and $Z_p$, respectively, upon ~10 min exposures of sensor to $H_2O$ vapor (630, 1260, 2205, 3150, 4410, and 6300 ppm) and to $NH_3$ vapor (4, 8, 14, 20, 8, and 40 ppm). Note reversible response to $H_2O$ vapor and nonreversible response to $NH_3$ vapor. Inset in (b), dynamic response to $H_2O$ vapor. Inset in (d), univariate calibration curve for $NH_3$ determinations. (e) Scores plot of $PC_1$ versus $PC_2$ demonstrates discrimination between $NH_3$ and $H_2O$ vapor responses.

exposures resulted in the increase in film impedance $Z_p$ and shifts of the sensor resonance $F_p$, $F_1$, and $F_2$ to higher frequencies. The formation of hydrogen bonds and swelling of the polymer upon $H_2O$ exposures resulted in the decrease in $Z_p$ and shifts of $F_p$, $F_1$, and $F_2$ to lower frequencies. Measurements of multiple output parameters from a single sensor revealed different recovery kinetics of responses $Z_p$, $F_1$, $F_2$, and $F_p$ during experiments with $NH_3$. Responses $Z_p$, $F_1$, and $F_p$ showed a partial recovery from $NH_3$, while $F_2$ response was irreversible with only 1.2–3.5% signal recovery. This irreversible $F_2$ response is attractive to take dosimeter readings at a later time, for example at the end of an 8-h work shift. Response to $H_2O$ vapor was reversible and at least 100-fold weaker over the response to $NH_3$. Univariate $Z_p$, $F_1$, $F_2$, and $F_p$ calibration curves to $NH_3$ showed relatively high response sensitivity at low concentrations. This nonlinear behavior is typical to PANI films [38]. The detection limit (based on $3\sigma$ criterion) was calculated to be 15–80 ppb of $NH_3$ from $Z_p$, $F_1$, $F_2$, and $F_p$ measurements. This achieved detection limit is much better over nanosensors with PANI nanowires [38] and single-walled carbon nanotubes [39].

For comparisons with earlier reported sensors, selectivity of developed RFID sensors was evaluated using PCA [21]. PCA is a robust tool for processing of multivariate signals that is used by 10 out of 13 surveyed electronic nose manufacturers [40]. As shown in the PCA scores plot (Fig. 7e), the action of several vapor-response mechanisms in a single sensing film was independently detected and quantified with a single multivariable signal transduction RFID sensor.

***3.3.4 Reliable Quantitation of Toxic VOCs in the Presence of Variable Humidity.*** The ability of RFID sensors to operate in the presence of variable ambient RH and to reject effects of ambient humidity was further evaluated in detail. In one such vapor sensor, individual measured parameters are affected by RH as shown in a PCA scores plot versus experimental time (Fig. 8a). However, critical to the sensor performance,

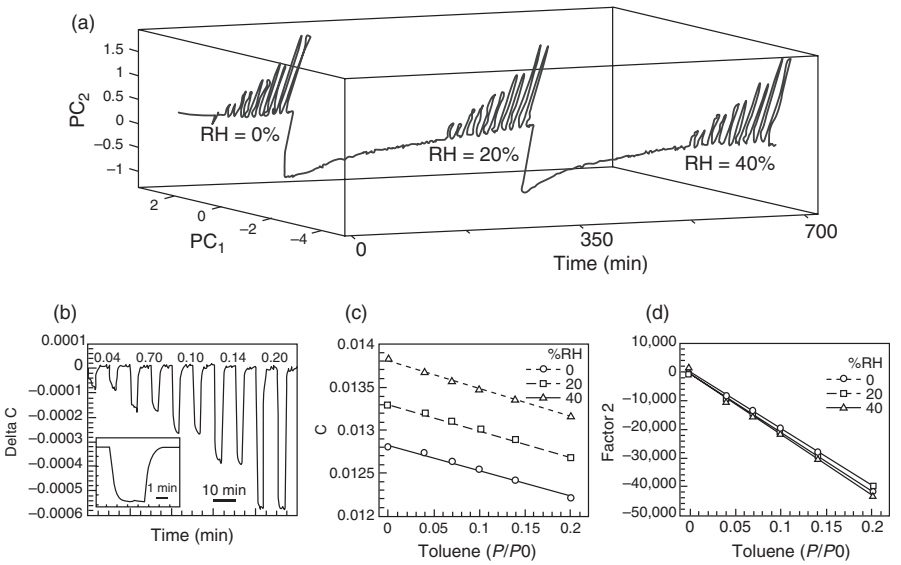



**FIGURE 8** Initial demonstration of humidity-independent operation using a single sensor with the multivariable signal transduction. (a) Plot of $PC_1$ versus $PC_2$ versus time illustrates sensor response to five concentrations of toluene vapor (0.04, 0.07, 0.10, 0.14, and 0.20 $P/P_o$, two replicates each) at three humidity levels. (b) Response reproducibility and dynamics. Univariate (c) and multivariate (d) calibration curves for toluene detection at 0, 20, and 40% RH. $P/P_o$ is partial vapor pressure during experiments.

sensing material applied onto the RFID antenna responds with the same magnitude to the model analyte vapor (toluene) in the presence of different humidity levels. The reproducibility and dynamics of the response to toluene at a single humidity level are presented in Figure 8b. Univariate calibration curves for toluene detection are presented in Figure 8c and show the preserved sensitivity and linearity of sensing film response at different humidity levels. A full correction of toluene response at different humidity levels was done using multivariate analysis of multiple responses from the single sensor. The resulting multivariate calibration curves at variable RH are identical (Fig. 8d) and provide a new capability to quantify vapors at different humidity. In these experiments, the detection of vapors was performed in the presence of up to 400-fold more concentrated water vapor. Measurements over extended period of time (45 h) were further performed to evaluate effects of even higher humidity levels, up to 76% RH where the sensor also did not change the response magnitude to the analyte at high humidity of the carrier gas.

Using the developed knowledge in the design of the sensing materials for RFID sensors, several types of new sensing materials were synthesized and determination of toxic vapors was performed down to 900 ppb detection limits and with eliminated humidity effects. Figure 9a illustrates an example of sensor response $F_p$ to variable concentrations of TCE, water, and toluene vapors, demonstrating that water vapor response was not only negligible but also opposite in its response direction. Further, stability of sensor response to toluene vapor was tested at variable humidity levels of the carrier gas (0, 22, 44, 65, and 76% RH) as shown in Figure 9b. It was found that from conservative estimations based on the multivariable sensor response, the detection of toxic gases can be performed in the presence of 27,000-fold more concentrated water vapor.

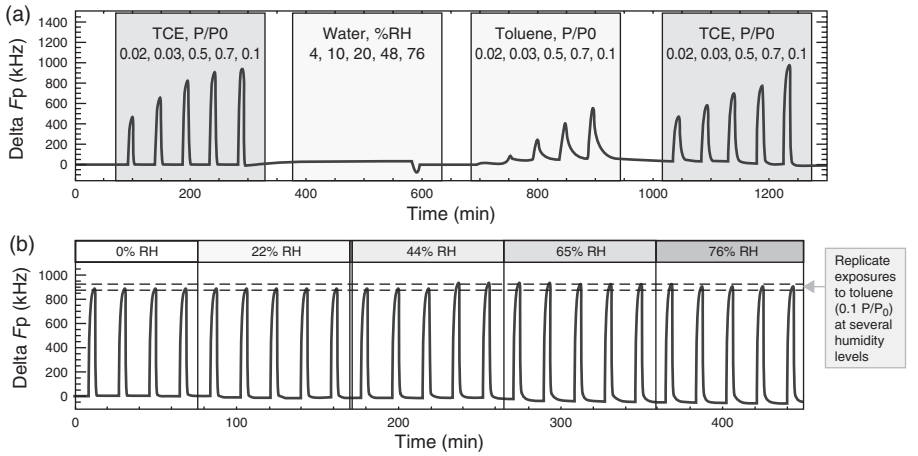



**FIGURE 9** Advanced demonstration of humidity-independent operation using a single sensor with the multivariable signal transduction. (a) Typical response to different concentrations of TCE (trichloethylene) vapor, water vapor, and toluene vapor. (b) Stability of sensor response to 0.1 $P/P_o$ of TCE vapor at variable humidity levels of the carrier gas.

***3.3.5 Selective Detection of CWA Simulants.*** Effects of different vapors on the response of the developed sensors were further evaluated by selecting a difficult combination of vapors such as methanol (MeOH), ethanol (EtOH), water ($H_2O$), and acetonitrile (ACN) [23]. Acetonitrile was selected as a simulant for blood CWAs [41]. Figure 10a demonstrates the measured $Z_p$ response for four analytes ($H_2O$, EtOH, MeOH, and ACN) for multiple concentrations and replicates ($n = 3$) [23]. Measurements of a single parameter of an RFID sensor, for example $Z_p$, cannot discriminate between different analytes. For example, if a signal $Z_p$ is changed by

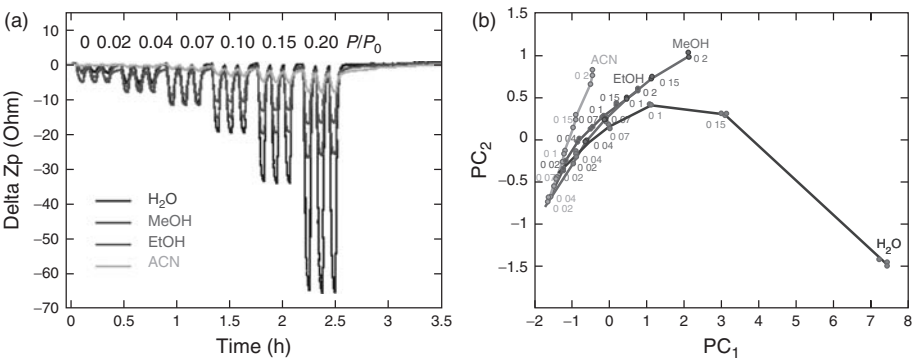



**FIGURE 10** Selective detection of ACN as a CWA simulant using a single sensor with the multivariable signal transduction. (a) Measured $Z_p$ response for four analytes ($H_2O$, EtOH, MeOH, and ACN), six concentrations (0, 0.02, 0.04, 0.07, 0.10, 0.15, and 0.20 $P/P_o$), and three replicates. (b) Results of the PCA multivariate analysis of measured parameters $F_1$, $F_2$, $F_p$, and $Z_p$ of the RFID sensor to the changes in $H_2O$, EtOH, MeOH, and ACN at six concentrations each, and three replicates per concentration. Numbers are $P/P_o$ values for individual vapors. Adapted from Reference [23] with permission.

~20 ohm, this change can be due to 0.1 $P/P_o$ of $H_2O$, 0.15 $P/P_o$ of MeOH, or 0.2 $P/P_o$ of EtOH. Thus, a single-parameter measurement of the RFID sensor cannot discriminate between different analytes and their concentrations. However, by applying the developed data-processing algorithm on the multivariable response of this single sensor, a good vapor discrimination has been achieved. Figure 10b illustrates that three out of four vapors were resolved using a selected sensing film and the complex impedance readout from the RFID sensor [23]. In particular, ACN vapor was well discriminated from $H_2O$, MeOH, and EtOH vapors. For detection of other analytes of interest to homeland security applications, diverse sensing materials can be applied [6, 9–11].

## 4 SUMMARY AND CONCLUSIONS

The detection of threats of importance to homeland security is needed with enhanced sensitivity for the detection of agents below health risk levels, with increased selectivity for operation in the presence of uncontrolled variable humidity and for providing minimal false-alarm rates and with expedited response rate for enabling an effective medical response. To meet these and many other new requirements, sensing technologies with previously unavailable capabilities are required.

These new capabilities will be difficult or even impossible to achieve using evolutionary improvements in existing sensing technologies. Thus, conceptually new technical solutions should be introduced in all key components of a sensor system as shown in Figure 1. Sensor systems with a sampler will benefit from new analyte preconcentrator concepts to rapidly collect and selectively release analyte species utilizing much less energy than is currently required. From the rigorous mathematical standpoint of data processing from a sensor, using a stable and high signal-to-noise multivariable response of a carefully designed sensor, it is possible to identify and quantify compounds that were not previously tested with the sensor [42]. To fully implement this capability, new sensing materials with more diverse response mechanisms to different species will be required, with well understood selection criteria [10]. These materials are under development using rational and combinatorial approaches [6, 10]. These sensing materials should be further coupled with new designs of multivariable transducers. Complete sensor systems will have more self-calibration and self-diagnostic abilities. At present, often the size of a transducer is much smaller than an associated battery needed for its operation. Thus, in sensors, too small to accommodate a conventional battery, power scavenging will become more important. This need will drive further the advanced packaging requirements to minimize needed power without degrading sensor performance. Of course, design, fabrication, and implementation phases of sensors will also be significantly impacted by progress in numerous disciplines and technologies as diverse as analytical chemistry, chemometrics, materials science, computer science, electrical engineering, artificial intelligence, and many others bound only by our imagination.

## ACKNOWLEDGMENTS

This work has been supported by GE Corporate long-term research funds. We are grateful to J. Cella, K. Chichak, and T. Sivavec for materials synthesis.

## REFERENCES


1. Fitch, J. P., Raber, E., and Imbro, D. R. (2003). Technology challenges in responding to biological or chemical attacks in the civilian sector. *Science* **302**, 1350–1354.
2. Fatah, A. A., Barrett, J. A., Arcilesi, J., Richard, D., Ewing, K. J., Lattin, C. H., and Helinski, M. S. (2000). *Guide for the Selection of Chemical Agent and Toxic Industrial Material Detection Equipment for Emergency First Responders, NIJ Guide 100-00*, Vol. 1, National Institute of Justice, Law Enforcement and Corrections Standards and Testing Program, Washington DC.
3. Shea, D. A. (2003). *High-Threat Chemical Agents: Characteristics, Effects, and Policy Implications*, CRS Report for Congress, Order Code RL31861, Congressional Research Service. The Library of Congress.
4. Hind, R. (2008). *Testimony before the Committee on Homeland Security on "Chemical Facility Anti-Terrorism Act of 2008"* http://www.greenpeace.org/raw/content/usa/press-center/reports4/chemsecuritytestimony.pdf.
5. Hulanicki, A., Glab, S., and Ingman, F. (1991). Chemical sensors: definitions and classification. Commission on General Aspects of Analytical Chemistry. *Pure Appl. Chem.* **63**(9), 1247–1250.
6. Potyrailo, R. A. (2006). Polymeric sensor materials: toward an alliance of combinatorial and rational design tools? *Angew. Chem. Int. Ed.* **45**, 702–723.
7. Middelhoek, S., and Noorlag, J. W. (1981/82). Three-dimensional representation of input and output transducers. *Sens. Actuators* **2**, 29–41.
8. Vilkner, T., Janasek, D., and Manz, A. (2004). Micro total analysis systems. *Recent Dev. Anal. Chem.* **76**, 3373–3386.
9. Hatchett, D. W., and Josowicz, M. (2008). Composites of intrinsically conducting polymers as sensing nanomaterials. *Chem. Rev.* **108**, 746–769.
10. Potyrailo, R. A., and Mirsky, V. M. (2008). Combinatorial and high-throughput development of sensing materials: the first ten years. *Chem. Rev.* **108**, 770–813.
11. Lange, U., Roznyatovskaya, N. V., and Mirsky, V. M. (2008). Conducting polymers in chemical sensors and arrays. *Anal. Chim. Acta* **614**, 1–26.
12. Röck, F., Barsan, N., and Weimar, U. (2008). Electronic nose: current status and future trends. *Chem. Rev.* **108**, 705–725.
13. Hierlemann, A., and Gutierrez-Osuna, R. (2008). Higher-order chemical sensing. *Chem. Rev.* **108**, 563–613.
14. Joo, S., and Brown, R. B. (2008). Chemical sensors with integrated electronics. *Chem. Rev.* **108**, 638–651.
15. Diamond, D., Coyle, S., Scarmagnani, S., and Hayes, J. (2008). Wireless sensor networks and chemo-/biosensing. *Chem. Rev.* **108**, 652–679.
16. Jiang, B., Smith, J. R., Philipose, M., Roy, S., Sundara-Rajan, K., and Mamishev, A. V. (2007). Energy scavenging for inductively coupled passive RFID systems. *IEEE Trans. Instrum. Meas.* **56**, 118–125.
17. Carrano, J. C., Jeys, T., Cousins, D., Eversole, J., Gillespie, J., Healy, D., Licata, N., Loerop, W., O' Keefe, M., Samuels, A., Schultz, J., Walter, M., Wong, N., Billotte, B., Munley, M., Reich, E., and Roos, J. (2004). Chemical and biological sensor standards study (CBS3). In *Optically Based Biological And Chemical Sensing For Defence*, Vol. 5617, J. C., Carrano, and A. Zukauskas Eds. SPIE—The International Society for Optical Engineering, Bellingham, WA, pp. xi–xiii.
18. Brower, J. L. (2006). The terrorist threat and its implications for sensor technologies. In *Advances in Sensing with Security Applications Amsterdam*, J. Byrnes, and G. Ostheimer Eds. Springer, The Netherlands, pp. 23–54.

19. Snow, E. S., Perkins, F. K., Houser, E. J., Badescu, S. C., and Reinecke, T. L. (2005). Chemical detection with a single-walled carbon nanotube capacitor. *Science* **307**, 1942–1945.
20. Qi, X., and Osterloh, F. E. (2005). Chemical sensing with LiMo3Se3 nanowire films. *J. Am. Chem. Soc* **127**, 7666–7667.
21. Jurs, P. C., Bakken, G. A., and McClelland, H. E. (2000). Computational methods for the analysis of chemical sensor array data from volatile analytes. *Chem. Rev.* **100**, 2649–2678.
22. Potyrailo, R. A., May, R. J., and Sivavec, T. M. (2004). Recognition and quantification of perchloroethylene, trichloroethylene, vinyl chloride, and three isomers of dichloroethylene using acoustic-wave sensor array. *Sensor Lett.* **2**, 31–36.
23. Potyrailo, R. A., and Morris, W. G. (2007). Multianalyte chemical identification and quantitation using a single radio frequency identification sensor. *Anal. Chem.* **79**, 45–51.
24. Potyrailo, R. A., Morris, W. G., Sivavec, T., Tomlinson, H. W., Klensmeden, S., and Lindh, K. (2008). RFID sensors based on ubiquitous passive 13.56-MHz RFID tags and complex impedance detection. *Wireless Commun. Mobile Comput.* DOI: 10.1002/wcm.711.
25. CDC (2008). *Emergency Preparedness and Response*. Centers for Disease Control and Prevention, Atlanta, GA, http://www.bt.cdc.gov.
26. Yadav, P., and Blaine, L. (2004). Microbiological threats to homeland security. *IEEE Eng. Med. Biol.* **23**, 136–141.
27. Patel, S. V., Jenkins, M. W., Hughes, R. C., Yelton, W. G., and Ricco, A. J. (2000). Differentiation of chemical components in a binary solvent vapor mixture using carbon/polymer composite-based chemiresistors. *Anal. Chem.* **72**, 1532–1542.
28. Peng, G., Trock, E., and Haick, H. (2008). Detecting simulated patterns of lung cancer biomarkers by random network of single-walled carbon nanotubes coated with nonpolymeric organic materials. *Nano Lett.* **8**, 3631–3635.
29. Meier, D. C., Evju, J. K., Boger, Z., Raman, B., Benkstein, K. D., Martinez, C. J., Montgomery, C. B., and Semancik, S. (2007). The potential for and challenges of detecting chemical hazards with temperature-programmed microsensors. *Sens. Actuators B* **121**, 282–294.
30. Finkenzeller, K. (2003). *RFID Handbook. Fundamentals and Applications in Contactless Smart Cards and Identification*, 2nd ed., Wiley, Hoboken, NJ.
31. Lehpamer, H. (2008). *RFID Design Principles*, Artech House, Norwood, MA.
32. Roberti, M. (2006). A 5-Cent breakthrough. *RFID J.* May, http://www.rfidjournal.com/article/articleview/2295.
33. Yang, C.-H., Chien, J.-H., Wang, B.-Y., Chen, P.-H., and Lee, D.-S. (2008). A flexible surface wetness sensor using a RFID technique. *Biomed. Microdevices* **10**, 47–54.
34. Philipose, M., Smith, J. R., Jiang, B., Mamishev, A., Roy, S., and Sundara-Rajan, K. (2005). Battery-free wireless identification and sensing. *IEEE Pervasive Comput.* **4**, 37–45.
35. Want, R. (2004). *Enabling Ubiquitous Sensing with RFID Computer*, pp. 84–86.
36. Sugiyasu, K., and Swager, T. M. (2007). Conducting-polymer-based chemical sensors: transduction mechanisms. *Bull. Chem. Soc. Jpn.* **80**, 2074–2083.
37. Nicolas-Debarnot, D., and Poncin-Epaillard, F. (2003). Polyaniline as a new sensitive layer for gas sensors. *Anal. Chim. Acta* **475**, 1–15.
38. Liu, H., Kameoka, J., Czaplewski, D. A., and Craighead, H. G. (2004). Polymeric nanowire chemical sensor. *Nano Lett.* **4**, 671–675.
39. Bekyarova, E., Davis, M., Burch, T., Itkis, M. E., Zhao, B., Sunshine, S., and Haddon, R. C. (2004). Chemically functionalized single-walled carbon nanotubes as ammonia sensors. *J. Phys. Chem. B* **108**, 19717–19720.
40. Snopok, B. A., and Kruglenko, I. V. (2002). Multisensor systems for chemical analysis: state-of-the-art in Electronic Nose technology and new trends in machine olfaction. *Thin Solid Films* **418**, 21–41.

41. Choi, N.-J., Kwak, J.-H., Lim, Y.-T., Bahn, T.-H., Yun, K.-Y., Kim, J.-C., Huh, J.-S., and Lee, D.-D. (2005). Classification of chemical warfare agents using thick film gas sensor array. *Sens. Actuators B* **108**, 298–304.

42. Grate, J. W., Wise, B. M., and Abraham, M. H. (1999). Method for unknown vapor characterization and classification using a multivariate sorption detector. Initial derivation and modeling based on polymer-coated acoustic wave sensor arrays and linear solvation energy relationships. *Anal. Chem.* **71**, 4544–4553.

## FURTHER READING

Bartelt-Hunt, S. L., Knappe, D. R. U., and Barlaz, M. A. (2008). A review of chemical warfare agent simulants for the study of environmental behavior. *Crit. Rev. Environ. Sci. Technol.* **38**, 112–136.

Chauhan, S., Chauhan, S., D'Cruz, R., Faruqi, S., Singh, K. K., Varma, S., Singh, M., and Karthik, V. (2008). Chemical warfare agents. *Environ. Toxicol. Pharmacol.* **26**, 113–122.

Eubanks, L. M., Dickerson, T. J., and Janda, K. D. (2007). Technological advancements for the detection of and protection against biological and chemical warfare agents. *Chem. Soc. Rev.* **36**, 458–470.

Kendall R. J., Presley S. M., Austin G. P., and Smith P. N. Eds. (2008). *Advances in Biological and Chemical Terrorism Countermeasures*, CRC Press, Boca Raton, FL.

Sadik, O. A., Land, W. H. Jr, and Wang, J. (2003). Targeting chemical and biological warfare agents at the molecular level. *Electroanalysis* **15**, 1149–1159.

Szinicz, L. (2005). History of chemical and biological warfare agents. *Toxicology* **214**, 167–181.

# PROTECTION, PREVENTION, RESPONSE AND RECOVERY

# PROTECTION AND PREVENTION: AN OVERVIEW

JOHN CUMMINGS
*Sandia National Laboratories, Albuquerque, New Mexico*

## 1 BACKGROUND

Much of what we currently consider part of "homeland security" has its origins in the late 1990s—especially in the work leading to the publication of Presidential Decision Directive 63 (PDD-63) Protecting America's Critical Infrastructures [1]. This Presidential Directive built on the recommendations of the President's Commission on Critical Infrastructure Protection. In October 1997, the Commission issued its report calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, banking and finance, energy, transportation, and essential government services. PDD-63 assigned lead agencies for specific infrastructure sectors and functions. In addition, the Office of Science and Technology Policy (OSTP) was assigned the responsibility to coordinate research and development agendas and programs for the federal government through the National Science and Technology Council (NSTC).

OSTP established the Critical Infrastructure Protection R&D Interagency Working Group (CIP R&D IWG) shortly after PDD-63 was issued as a subgroup to the NSTC Committee on National Security (CNS) and Committee on Technology (CT). In effect, the CIP R&D IWG was jointly placed under the CNS and the CT, and it reported to both. The CIP R&D IWG developed a database of existing federal government CIP R&D programs in conjunction with the Office of Management and Budget (OMB) and through data calls to the federal executive branch departments and agencies. The IWG also developed a set of CIP R&D agendas (strategies and road maps) that formulated the conceptual framework for a national level, strategic Infrastructure Protection Research and Development (R&D) Plan [2] to mitigate both cyber and physical threats. The agendas recommended R&D investments by type and agency, based on gaps between desired R&D and actual R&D reported in the database. The OSTP continued to encourage agencies to conduct research and development to protect the nation's critical infrastructure after PDD-63, but most efforts were limited in scope and funding [3].

All of that changed after the events of September 11, 2001 and the anthrax incidents that followed shortly thereafter. The formation of the Office of Homeland Security (OHS) provided renewed focus on the nation's infrastructure and expanded the sectors and assets of concern beyond those addressed in PDD 63. A series of national strategies was published by OHS or its affiliates including one that focused on the critical infrastructure of the United States [4]. The National Research Council formed a Committee on Science and Technology for Countering Terrorism that wrote a report that focused on the scientific and technological means by which we can reduce the vulnerabilities of our society to terrorist attacks, and mitigate the consequences of those attacks when they occur [5]. The RAND National Defense Research Institute sponsored a series of workshops involving industry, academe, and government officials that gathered information on physical protection of the nation's most critical infrastructure sectors. Finally, in March, 2003 the Department of Homeland Security (DHS) came into being and began the task of coordinating the national effort to protect critical infrastructure and key assets.

In December, 2003 the White House published Homeland Security Presidential Directive 7 (HSPD-7; "Critical Infrastructure Identification, Prioritization, and Protection [6]") which outlined the requirements for protecting the nation's critical infrastructure. HSPD-7 defined these critical infrastructure as consisting of the following sectors and key resources: agriculture and food, water, public health and healthcare, emergency services, the defense industrial base, information technology, telecommunications, energy, transportation systems, banking and finance, chemical, postal and shipping, national monuments and icons, dams, government facilities, commercial facilities, and nuclear reactors, materials and waste.

HSPD-7 also required the secretary of DHS, in coordination with the director of the OSTP, to prepare on an annual basis a Federal Research and Development Plan in support of the directive. In 2004, DHS and OSTP published "The National Plan for Research and Development in Support of Critical Infrastructure Protection [7]". The plan is structured around nine "themes": detection and sensor systems; protection and prevention; entry and access portals; insider threats; analysis and decision support systems; response, recovery, and reconstitution; new and emerging threats and vulnerabilities; advanced infrastructure architectures and systems design; and human and social issues. The long-term vision of the National Plan involves three strategic goals: a national common operating picture for critical infrastructure; a next-generation computing and communications network with security "designed-in" and inherent in all elements; and resilient, self-diagnosing, and self-healing physical and cyberinfrastructure systems. An updated National R&D Plan has been written but is not yet published (Note: updates to the plan have been published and coordinated with other Homeland Security plans that respond to other Homeland Security Presidential Directives.).

The focus of this article is on protecting assets, networks, systems, and humans by preventing and/or mitigating *physical* attacks/damage. The possibility of combined cyber and physical attacks is of concern, and it can be considered here by examining cases involving degraded communications and IT systems that support physical protection/prevention systems.

A number of terms are used to describe what "protection and prevention" mean for homeland security and defense. These terms are often used loosely without an agreed upon set of definitions. In order to provide some rigor it may be useful

to explicitly define these terms (definitions are from the Merriam-Webster online dictionary [8]):

*Protect.* To cover or shield from exposure, injury, damage, or destruction; to guard; to defend; to provide a guard or shield; to maintain the status or integrity of.

*Prevent.* To be in readiness for; to meet or satisfy in advance; to act ahead of; to go or arrive before; to deprive of power or hope of acting or succeeding; to keep from happening or existing; to hold or keep back; to hinder; to stop; to interpose an obstacle.

*Mitigate.* To cause to become less harsh or hostile; to mollify; to make less severe or painful; to alleviate; to extenuate; to relieve.

*Respond.* To say something in return; to react in response; to show favorable reaction; to be answerable; to reply.

*Recover.* To get back; to regain; to bring back to normal position or condition; to rescue; to make up for; to save from loss and restore to usefulness; to regain a normal position or condition.

*Robust.* Having or exhibiting strength or vigorous health; having or showing vigor, strength, or firmness; strongly formed or constructed; sturdy; capable of performing without failure under a wide range of conditions.

*Resilient.* Characterized or marked by resilience; capable of withstanding shock without permanent deformation or rupture; tending to recover from or adjust easily to misfortune or change; elastic.

Note that while the term *prevention* often means those efforts associated with intelligence and interdiction of terrorist plans, here it is focused on preparedness, deployment of defensive measures in advance of an attack, devaluation of targets, and so on.

The concepts of homeland security and homeland defense are often used interchangeably, but for our purposes we will align these terms with the agencies that are primarily accountable for them: DHS and the Department of Defense (DoD). Homeland security is focused on civilian and law enforcement areas of our national efforts to counter terrorist acts (including those complex issues associated with protecting our national borders). Homeland defense is focused on domestic use of military resources to defend the skies and seas (with some land-based actions focused on high-security events) and to provide assistance to other agencies in responding to and recovering from a major terrorist attack.

The threats and challenges from a homeland security and defense perspective range from relatively limited consequence suicide bombings to the possibility of weapons of mass destruction (WMD) being used to cause very large consequences. Threat actors range from radical Islamic fundamentalists to domestic extremist groups who support the use of violence—they are malevolent, intelligent, innovative, and dynamic. Challenges range from addressing root causes of unrest and support for violence to detecting WMD devices hidden in containers, vehicles, boats, and aircraft. There are literally millions of possible targets and thousands of miles of borders in the United States, so trying to protect and defend all of them is impossible. Terrorist acts focus on causing extreme fear in the civilian population so "hardening the will" of our citizens is a challenge. The primary goal of all our efforts is to maintain our core freedom and quality of life while providing an appropriate level of security. Understanding the dynamic risks from terrorism and deploying cost-effective solutions to address the highest risks is our

challenge. The recent release of a national strategy for DoD involvement in civilian disasters [9] ensures a much more organized and stronger response to situations such as WMD in a major city that could overwhelm civilian-only resources.

In addition to significant science and technology advances, we also require validated assessment methodologies for defense facilities, critical infrastructure facilities, port and coast guard facilities, government facilities, and privately owned facilities. Currently, there are many methods, tools, techniques, and processes being used. In addition, we need training to help prevent attacks on facilities and to protect facilities—this is an important element of preparing for terrorist acts as well as for accidents and natural disasters that disrupt our infrastructure. A variety of methods, tools, techniques, and processes are used.

There are scientific and technological solutions that can address many of the most difficult challenges. High priority scientific and technological solutions include sensor and detection systems for explosives and WMD, protection systems to defend against the effects of those threats, enhanced risk analysis and management tools, and techniques to address the "insider" problem. Work on these solutions is well underway but many of the challenges are very difficult especially when placed in the context of functioning infrastructure and real assets. The grand challenges that lie ahead involve developing advanced concepts for our infrastructure and physical assets that foster self-awareness, self-healing, and graceful degradation should they be attacked.

## 2 THREATS, CHALLENGES, AND SOLUTIONS

Threats can be decomposed into perpetrators and potential kinds of attacks. We must consider a range of perpetrators (not just Al-Qaeda)—both foreign and domestic terrorists with a variety of motivations, intents, and capabilities—and we must consider a spectrum of attacks from suicide bombs to WMD. Both elements of the threat pose challenges and some of those can be addressed with science and technology solutions.

Protection from insiders is an age-old problem. Insiders are within our defenses and they are trusted. They know about our security measures and plans. They know where vulnerabilities exist or can be created by them, in our systems. Defending against malevolent insiders can involve a number of approaches based on technology. Part of the vetting process for hiring employees and support contractors can include database searches using smart algorithms. Access control can limit the effectiveness of most insiders by not allowing them complete freedom of movement and action within our defensive perimeter. Tagging and tracking using radio frequency identification (RFID) devices can alert security personnel to insiders who are not where they should be or who are doing what they are not supposed/allowed to do. Document protection and control is used to limit the amount of information about critical components and processes that is available to general employees and contractors. Advanced concepts may include sensors that use noninvasive means to measure malevolent "intent" and new designs of systems that are "smart" in terms of self-protection from harmful actions. Some of these are already available and are termed *skeptical* systems.

Many forms of attack involve intrusion by a human or vehicle through (or around) a defensive perimeter. Protection from intrusion may involve detection, possible elements to delay the intruder, and then response (e.g. a security force or an automated action). Fences, gates, a security guard force, and closed circuit television (CCTV) systems are

fairly common elements of many systems. Physical intrusion detection may be by sensing motion, sound, or other parameters (temperature, human out-gassing, neuron activity, etc.). Metal and weapon detection systems are often employed at portals. Vehicles are often stopped or slowed using barriers and fences, bollards, serpentine roadway designs, architectural barriers, or vehicle traps. Access to a site or facility can be controlled with keys and locks, "smart" badges, passwords, biometric scans, and facial-recognition systems. Advanced designs and concepts for defense against intrusion are being developed and the use of advanced materials will improve the obstructing power of barriers. More intelligent and autonomous CCTV systems are under development and it is expected that they will provide significant improvements in cost-effective 24/7 detection of intrusion and attack.

Defense against explosive blasts is a growing concern. There are systems for detecting explosives as well as for disarming and deactivating explosive devices. Mitigation systems for buildings, windows, doors, and entry ways include blast design measures as well as debris and fragment shields. Defense against small arms fire, mortars, and rockets includes using barriers, shields, and armor, for body, buildings, and vehicles. Advanced designs and materials (e.g. carbon nanotubes) should reduce the cost of blast and fragment mitigation while improving performance. However, parallel advances in explosives and shrapnel technology of much higher performance make this area of R&D rather dynamic.

Chemical, biological, and radiological threats are generally manifested as airborne attacks with gases or aerosols. Heating, ventilation, and air conditioning (HVAC) systems can address these attacks on indoor facilities using detectors, filters, and alarms. There are HVAC systems with automated (smart) responses that can stop or redirect building airflows to mitigate effects. Drinking water and food are also possible vectors for these threats and current defenses involve detection and alarm. Future systems will employ new designs, concepts, and materials to detect, delay, mitigate, and possibly eliminate a broad range of these threats.

Less lethal and nonlethal force systems can be employed to delay or stop a physical attack on a facility. Common methods include the use of rubber and plastic bullets, beanbags, water cannons, tear gas, pepper spray, Mace spray, and stun guns. Newer concepts involve foams (sticky and slippery), slippery surfaces, acoustic devices, barometric and rapid gas exchange systems, laser dazzlers and microwaves. Many systems and techniques have been developed for use by law enforcement officers against criminals; evolutionary and revolutionary concepts are being developed and deployed constantly. An interesting observation in this area is the growing development and deployment of systems using robotic and automated response systems. These systems include those with lethal, less lethal, and nonlethal options. They offer the promise of cost-effective 24/7 response and are often used in combination with a guard force.

One of the methods of preventing an attack is to use cover, deception, and concealment systems so that the adversary is unaware of the location of the target. Techniques include camouflage and view-disruption systems. It is expected that nanotechnology may provide additional means of "hiding" systems and vulnerable components from view.

Water can be used as a weapon. This is clearly the case when considering major dams that are upstream of large population centers or important agricultural areas. Many of the methods, devices, techniques, and processes described previously to protect against intrusion and explosive blasts can be deployed to assist in defending such targets. There

are specific conditions that must be taken into account for defense of dams such as waterborne and underwater attacks using explosives. Water barriers and nets are commonly used approaches.

Fire can also be used as a weapon. Small quantities of flammable liquids and accelerants are easily concealed and can be used in indoor facilities and vehicles of mass transportation. Major wildfires are common natural threats but they can also be intentionally initiated to endanger metropolitan and agricultural areas or to distract emergency responders. Since indoor fires occur somewhat regularly, detection and extinguishment systems are common in areas where large numbers of people gather. Large wildfires require a lot of effort from emergency responders, especially when conditions are dry and windy. Advancements in firefighting equipment (including enhanced communications capabilities) and new materials for extinguishment will enable faster limitation of the effects of fires.

Electromagnetic, microwave, laser, and directed-energy devices can be used as weapons. While not commonly deployed today, their use may increase in the future. Lasers have been used to "dazzle" pilots in ways that cause temporary impairment of eyesight. A number of devices are commercially available today, which use a range of electromagnetic frequencies and effects to disrupt electronic circuits and systems. These devices could be used to disable security or response systems and then combined with physical assaults on key facilities and assets. A range of defensive measures (optical filters for laser beams, radiation shielding, and hardening of electronic circuits, etc.) are available today for these threats and it is anticipated that countermeasures will evolve if these methods of attack are deployed by terrorists.

Response and recovery are important elements of resilient infrastructure (as is redundancy, of course). If the timescale of recovery is short enough, one of the key goals of terrorism (economic damage) can be significantly mitigated. This section of the Handbook does not address the needs of first responders for enhanced science and technology solutions. The focus here is rather heavily on infrastructure systems. Protective materials, paints, coatings, and films are being developed to assist in the rapid decontamination of surfaces that have been exposed to toxic chemicals, biological agents, and radiological materials. For rebuilding damaged facilities and assets we will need to be able to rapidly provide temporary structures. Long-term recovery means rebuilding with new concepts and materials that have security "designed-in" at the start. A broad range of research and development is underway in the building and manufacturing industries to incorporate advanced designs, concepts, and materials into the next generation of critical facilities and assets.

*Critical infrastructure protection* is common terminology for much of what is discussed in this section of the Handbook. While this overview article focuses on protection from and prevention of terrorist attacks, much of the current discussion in conferences and workshops has shifted to resilience of the nation's infrastructure. This difference is really a matter of definition and perspective. Resilience can imply rapid response and recovery from a catastrophe—the assumption being that the nation cannot protect everything from attack. A cost-effective strategy may be to be prepared to rebuild facilities and reconstitute capabilities very rapidly. Redundancy is an important element of resiliency. On the other hand, protection and prevention can be broadly viewed as containing a range of elements from robustness (hardening to withstand attacks) to mitigation of effects (limiting damage and impact) to resiliency (rapidly recovering from attacks). Whatever be

the perspective, the science and technology base can and will provide solutions to many of the problems.

Information sharing and protection is a vital issue related to protection of the nation's critical infrastructure. The vast majority of the infrastructure is owned and operated by the private sector, cities, and municipalities. Most of the infrastructure is global in nature. Consequently, working together as partners to provide solutions that address the terrorism issue requires industry–government teams, US international teams, and openness in the science community to share research results while protecting sensitive information. Despite concerns about litigation and possible regulation, industry has often been reluctant to work closely with the government. Though this is not directly a science and technology issue, this area must be addressed in order to accelerate progress.

It is important to note that while this section of the Handbook is focused on research and development for solutions based primarily on the physical and engineering sciences, many of the solutions will come from the social sciences. In particular, terrorism is a violent form of action aimed at social, economic, cultural, ideological, and religious values. Addressing root causes of terrorism and removing some of the fear caused by it are extremely important for the ultimate solution for free and open societies.

## 3 FUTURE RESEARCH DIRECTIONS

Advanced designs, concepts, and materials for protection and prevention are areas of active research and development around the globe. New methods, devices, techniques, and processes are being developed every day. The key driver for many of these breakthroughs will be business continuity and reliability of infrastructure services. Another important driver for advancements will be protection from and prevention of criminal acts (including malevolent acts by insiders, theft, sabotage, and vandalism). Concerns about the impact of terrorist acts and natural catastrophes will drive much of the Federal investment in research and development for this area. Consequently, dual purpose R&D and multipurpose technology will help make future protection and prevention more cost-effective. It will also help increase the degree of deployment.

Information technology is one of the major contributors to current advancements and it will remain that way for the foreseeable future as well. Buildings and structures will contain significantly more embedded information technology that can sense the status of systems (and their constituent components) and provide automated responses. Designs will incorporate this capability into "smart" structures that will autonomously communicate with security and emergency officials, protect themselves, heal themselves, and degrade in ways that minimize loss of functionality and human casualties. Computer modeling and simulation tools will greatly aid in designing infrastructure systems that have security "built in" from the start and allow for cost-effective adaptability for the future.

Nanotechnology holds the promise of significant advancements in materials of all sorts. The construction of light-weight structures that are extremely strong is possible. Materials (e.g. based on carbon nanotubes) that can absorb blasts and contain fragments will be available at low cost. Special coatings, films, and surfaces that neutralize chemical and biological agents will be developed. Foams and sprays that can capture radiological particulates for removal and treatment may be manufactured. Materials with exotic properties will be developed that will provide new ways of protecting people, facilities,

and assets. Other new materials will allow us to design enhanced systems that prevent malevolent acts from taking place at all or mitigate their consequences.

Biotechnology will provide us with new ways of defending against attacks using chemical or biological agents by allowing people to be vaccinated or inoculated in advance. There will be new designs and concepts for protection developed based on biological processes and systems. Many of the new materials envisioned for the future will be created by mimicking naturally formed materials or by using biological processes to manufacture them. Humans, agricultural crops, and livestock will recover more rapidly and fully from injuries and attacks by using newly developed techniques based on our improved biotechnology capabilities.

The nature of terrorism is such that terrorists will employ new methods based on improved science and technology just as we use new methods to provide enhanced prevention and protection. As in warfare, the effort is dynamic. It has both evolutionary and revolutionary elements. Our primary aim must be to develop and deploy a range of tools and techniques that address the full spectrum of response to terrorist acts—from understanding root causes to increasing interdiction to providing protection and recovery.

## 4 CONCLUSIONS

The history of violence and war goes back to the earliest humans and tribal groups. Yet terrorism brings a strong emotional element of irrational fear associated with the randomness of attacks and the focus on innocent civilians, including women and children. Nevertheless, following the cold war, the United States felt reasonably secure from international violence until the attacks of September 11, 2001. The nation's response since then has involved major reorganization of federal agencies to address the operational and R&D elements, increased partnership with other countries, and significant changes in the way private industry and infrastructure owners deal with security issues.

Prevention of terrorist attacks and protection of our nation's critical infrastructure from such attacks are important elements of homeland security and defense. As a free and open society we are vulnerable to acts of terrorism, partly due to our inherent cultural values. Consequently we must exploit the advantages we have in science and technology to develop and deploy solutions that allow us to defend our way of life and increase the difficulties for those who seek to cause terror.

Many of the possible solutions to the threats and challenges that we face from terrorists can be used for additional purposes. From an infrastructure perspective, business continuity and reliable delivery of goods and services act as economic drivers for improved security, especially as new systems are designed and constructed. From a human perspective, measures that address crime and violence can also serve to counter terrorist acts. Accidents (e.g. chemical and radioactive material releases) and naturally emerging diseases [e.g. severe acute respiratory syndrome (SARS) and Avian Influenza] are also reasons to support research and development apart from providing solutions for the terrorism problem.

Research and development can assist us in addressing issues from insider threats to suicide attacks with conventional explosives to dealing with WMD. New designs, concepts, materials, tools, devices, and technologies can provide cost-effective solutions that not only make us more secure but also more resilient if a catastrophe occurs for any reason (natural, accidental, or intentional and malevolent). Systems that are automated

and built to be "smart" can defend, mitigate, and respond to attack and damage. Protection and prevention are important areas of homeland security and defense—they form part of the base of our science and technology response to acts of terrorism.

## ACKNOWLEDGMENTS

The submitted manuscript has been authored by a contractor of the US Government under Contract No. DE-AC04-94AL85000. Accordingly, the US Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for US Government purposes. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the US Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

## REFERENCES

1. The White House. (1998). *Presidential Decision Directive 63: Protecting America's Critical Infrastructures*, May 28 1998, http://www.fas.org/irp/offdocs/pdd-63.htm.
2. MacDonald, B., and Rinaldi, S. M. (1998). *Critical Infrastructure Protection Research & Development Interagency Working Group Blue Book*. Office of Science & Technology Policy.
3. Robert T. M. (1997). *Critical Foundations: Protecting America's Infrastructures, Report of the Presidential Commission on Critical Infrastructure Protection, Washington, Dc*, October 1997, http://www.pccip.gov/.
4. The White House. (2003). *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003, http://www.whitehouse.gov/pcipb/physical.html.
5. Committee on Science and Technology for Countering Terrorism. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, Washington, DC.
6. The White House. Homeland Security Presidential Directive 7 (HSPD-7), (2003). *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.
7. DHS and OSTP. (2004). *The National Plan for Research and Development in Support of Critical Infrastructure Protection*.
8. Merriam-Webster online dictionary; http://www.m-w.com/.
9. Department of Defense. (2005). *Strategy for Homeland Defense and Civil Support*. Department of Defense, Washington, DC, June 2005.

## FURTHER READING

Bullock, J., and Haddow, G. (2006). *Introduction to Homeland Security*, 2nd ed., Butterworth-Heinemann, Elsevier, Burlington, Mass, March 30 2006.

DHS. (2006). website: http://www.dhs.gov/dhspublic/.

DoD. (2006). website: http://www.defenselink.mil/.

Fay, J. (2007). *Encyclopedia of Security Management: Techniques and Technology*. Elsevier, Burlington, Mass, Butterworth-Heinemann.

Fennelly, L. J. Eds. (2003). *Effective Physical Security*, 3rd ed., Butterworth-Heinemann, Elsevier, Burlington, Mass.

Fischer, R. J., and Green, G. (2003). *Introduction to Security*, 7th ed., Butterworth-Heinemann, Elsevier, Burlington, Mass, November 2003.

Garcia, M. L. (2007). *The Design and Evaluation of Physical Protection Systems*. Butterworth-Heinemann, Elsevier, Burlington, Mass. February 23, 2001.

Homeland Security Institute. (2006). website: http://www.homelandsecurity.org/.

Howitt, A. M., and Pangi, R. L. Eds. (2003). *Countering Terrorism: Dimensions of Preparedness, BCSIA Studies in International Security*. The MIT Press, Boston, Mass, September 2003.

Kamien, D. (2005). *The McGraw-Hill Homeland Security Handbook*. McGraw-Hill, New York, NY, September 2005.

Lewis, T. G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley & Sons, Hoboken, NJ.

National Commission on Terrorist Attacks. (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, July 22, 2004, http://www.9-11commission.gov/.

National Infrastructure Protection Plan. (2006). Department of Homeland Security, http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

Sauter, M., and Carafano, J. (2005). *Homeland Security: A Complete Guide To Understanding, Preventing, and Surviving Terrorism*, *The McGraw-Hill Homeland Security Series*. McGraw-Hill, New York, NY.

Sennewald, C. (2003). *Effective Security Management*, 4th ed., Butterworth-Heinemann, Elsevier, Burlington, Mass.

# PROTECTION AND PREVENTION: THREATS AND CHALLENGES FROM A HOMELAND DEFENSE PERSPECTIVE

JEFFREY D. MCMANUS

*The Office of the Secretary of Defense, Washington, D.C.*

## 1 INTRODUCTION

We recently passed an important anniversary in the United States on September 11, 2008. It is 8 years since the al-Qaeda attacks against the World Trade Center and the Pentagon. Unfortunately, this attack in which almost 3000 people were killed in a single day, has been joined by other significant terrorist incidents against other countries. These attacks

have caused death to hundreds more innocent civilians in places like Mumbai, India (July 11, 2006); Bali, Indonesia (October 2, 2005); London, United Kingdom (July 7, 2005); and Madrid, Spain (March 11, 2004). A war has been declared upon our nation and waged against our people. The intent of transnational terrorists is to try to shape and degrade political will through extreme acts of violence in order to diminish resistance to their ideologies and agendas. Our future freedom and security depend on our efforts in meeting this challenge. It is imperative that we have a comprehensive preparedness strategy that focuses our combined national efforts on proactive prevention and protection activities *before* a terrorist incident occurs. This approach can greatly lessen the overall risk of both terrorist attacks as well as nonintentional hazards, and even assist the response and recovery efforts following those incidents that do occur.

## 2 BACKGROUND

It is the role of the Department of Defense and the US military to fight and win our nation's wars while protecting US sovereignty, territory, domestic population, and critical defense infrastructure against external threats and aggression. The structure and composition of military forces, built up during World War II and evolved over the 45-year Cold War, allowed for the detection, deterrence, or when necessary, defeat, of conventional threats to the United States. The principal threat was from the Soviet Union, capable of delivering nuclear weapons via missiles, bombers, or submarines, and having massive conventional forces poised in Eastern Europe for a strike west. The security of the US homeland depended on our nuclear deterrent and strong conventional forces. The Department of Defense and US military maintained a significant forward presence around the world that apart from providing a security shield, contained and deterred Soviet aggression, protected our allies and friends, and provided stability for the inevitable spread of personal and economic freedom.

The size, structure, and capabilities of US forces built up and maintained throughout the Cold War also provided key capabilities that could assist in specific situations here in the United States. These situations, called Defense Support to Civil Authorities (DSCA), allow for the use of US military forces within our homeland, under the direction of the President and the Secretary of Defense within the authorities provided by Title 10 U.S. Code (USC). However, the legal authorities and guidelines for DSCA are specific and limited. They preserve the spirit and intent of our founding fathers to limit the use of the military over our domestic population. Prior to any use of US military forces at home in a DSCA role, six criteria are assessed and evaluated:

- *Legality.* Is the activity compliant with existing law?
- *Lethality.* Is there no or very minimal potential for the use of lethal force by or against military forces?
- *Risk.* Is the activity safe for military forces?
- *Cost.* Is there an existing funding authority or reimbursement mechanism available to minimize impact to the Department of Defense budget?
- *Appropriateness.* Are military forces unique, capable, or necessary to provide the activity?
- *Readiness.* Will this activity not significantly interfere with other missions of the Department of Defense?

If answers to all of these questions are "Yes," then a DSCA mission can be approved and implemented.

These situations fall into four main categories. First is support following a civil disaster or emergency, such as a hurricane or an earthquake. These activities are governed under the Stafford Act (i.e. Title 42 USC, Sections 5121 and 5122). This allows utilization of military forces in response to a major disaster, whether natural or man-made. Second is support to counter drug operations, and is limited primarily to the detection and monitoring of drug traffickers attempting to cross US borders by air, sea, or land (i.e. authorities are outlined in Title 10 USC, Section 124). Third is support responding to either chemical or biological weapons emergencies, which is authorized under Title 10 USC, Section 382.

The final type of support would be that related to law enforcement functions, which is greatly restricted under the Posse Comitatus Act (i.e., 18 USC, Section 1385, also applicable is 10 USC, Section 375). This law prohibits US military forces from executing the civil laws of the United States, or stated another way, prohibits US military forces from performing direct law enforcement activities. These activities include interdiction of a vehicle, vessel, aircraft, or similar activity (with the exception of the specific drug detection and monitoring efforts described above); search or seizure; arrest or apprehension, such as stopping and frisking individuals; surveillance or pursuit of individuals; or undercover work, such as working as undercover agents, informants, investigators, or interrogators. The only exception from these restrictions would be if the President declares an emergency under the Insurrection Act (i.e. Title 10 USC, Sections 331–334). This would allow US military forces to respond to a civil disturbance and perform direct law enforcement functions.

## 3 CURRENT SITUATION

Following the terrorist attacks on September 11, 2001, the President working closely with Congress, created the Department of Homeland Security (DHS). *Homeland Security* is a concerted national effort to prevent terrorist attacks within the United States, reduce the vulnerability of the United States to acts of terrorism, and minimize the damage by and assist in the recovery from terrorist attacks that do occur. The DHS is the lead US federal agency for homeland security, with responsibilities for coordinating and integrating efforts related to homeland security, intelligence, law enforcement, and homeland defense. This environment is shown in Figure 1. It requires close coordination with other federal organizations which have critical roles in combating terrorism, such as the Directorate of National Intelligence and the intelligence community, the Department of Justice and the Federal Bureau of Investigation, and the Department of Defense. The DHS also has responsibilities beyond the prevention of terrorism, including leading the US government response to natural disasters and other emergencies.

There has been much progress made since September 2001. Many strategies, policies, and plans have been developed. New organizations have been established at the federal level, such as DHS, the Directorate of National Intelligence, the National Combating Terrorism Center, and US Northern Command. Each has consolidated authorities and functions that, while appropriate for the Cold War environment, were not meeting the requirements of the new security environment. It is important to recognize that we have more forms of protection in place than 8 years ago.

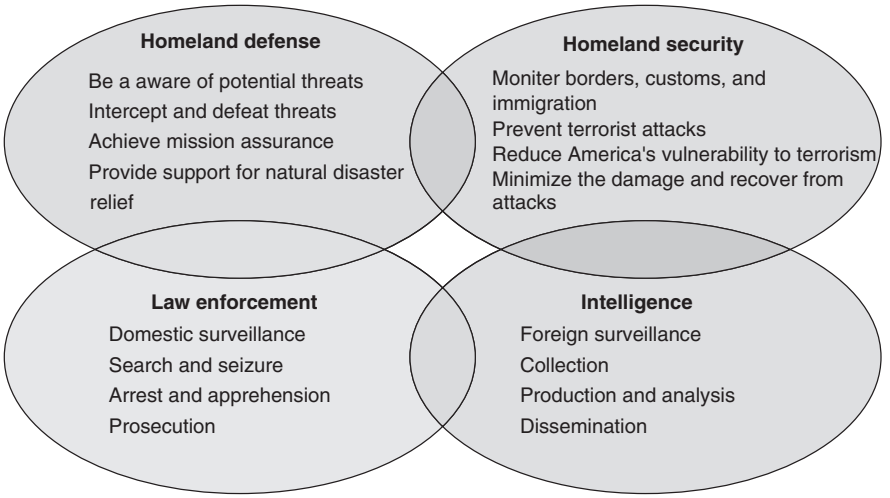



**FIGURE 1** The homeland security environment.

However, while much has been done, there is still room for improvement. We have many national strategies and plans, but we still seem somewhat mired in a stove-pipe structure. While national plans have been developed through interagency processes, they still reflect somewhat limited perspectives unique to their communities of interest. For example, our national protection plans primarily reflect a security or law enforcement perspective. Remediation activities are being appropriately driven by a budgetary perspective, but risk management appears inconsistent and is therefore ineffective in maximizing the resource priority trade-offs. Response plans reflect an emergency response or consequence management perspective, but do not account for the longer term, sustained activities necessary for true recovery. Five years since September 11, 2001, our national effort seems to be "reactive" and "federal", that is, focused mostly on postincident efforts, and limited to the functions and capabilities that can be provided by federal departments and agencies.

President Bush signed and released the *National Strategy for Homeland Security* in July 2002. (A revised version was released in October 2007.) This strategy highlighted the new threat environment, discussed our vulnerabilities, and outlined six critical mission areas necessary to meet the new security challenge:

- intelligence and warning;
- border and transportation security;
- domestic counterterrorism;
- protecting critical infrastructure and key assets;
- defending against catastrophic threats;
- emergency preparedness and response.

This national strategy provided the structure and framework for the establishment of the DHS, and documented several necessary foundations for success: law, science and technology, information sharing and security, and international cooperation.

There are, however, deficiencies in the *National Strategy for Homeland Security*. The first is in the area of risk management because the strategy does not provide a comprehensive risk management structure. Risk is a function of criticality, vulnerability, and probability of incident occurrence. While vulnerabilities are addressed in the strategy, as are the evolving means of terrorist attack, the elements of criticality (i.e. consequence of loss) and probability of incident occurrence are not. These elements must be included to enable true risk management, that is, the process by which decision-makers accept, reduce, or offset risk. Another related deficiency is that the strategy does not adequately address nonhostile hazards. Events such as accidents or natural disasters can also result in catastrophic damage; for example, incidents such as Hurricane Katrina and the subsequent levee breaches in New Orleans. This paper later outlines the full scope of threats and hazards that should be considered when addressing homeland security.

The 2002 strategy also does not differentiate between mission areas (i.e. *what* we need to do), the domain environment (i.e. *where* we need to do them), and the preparedness continuum (i.e. *when* we need to do them). To be fair, the strategy does discuss protection and response activities. However, it does not fully articulate the steady-state prevention functions that can be implemented preincident to minimize general risks. It also does not articulate the postevent actions necessary over the longer term (i.e. once immediate response functions are completed) to get people and infrastructure back to their preincident situation. This paper will later outline the preparedness continuum, and focus on the proactive activities and challenges faced in the pre-event functions of prevention and protection.

## 4 THREATS AND HAZARDS

As discussed above, a key element in the risk management equation is that of threats and hazards. These are the incidents, whether intentional and man-made, or unintentional accidents and natural disasters, that cause damage or loss. Figure 2 provides an illustrative example. Vulnerabilities occur when a specific asset or function is both susceptible to damage by the threat or hazard and there is a probability for damage to occur. For example, the human body is vulnerable to injury from a bullet or a bomb, but not directly vulnerable to a cyber attack. Conversely, a computer system is vulnerable to cyber penetration and attack, but not vulnerable to a biological agent. These distinctions become very important when risk is being assessed for management through remediation or mitigation.

Threats are incidents intentionally caused by an adversary who has the intent, capability, and opportunity to cause loss or damage. This definition is related closely with that of Carl von Clausewitz and his definition for war: acts of violence used to compel an adversary to do one's will. Traditionally, war and the violence it contains has been the domain of nation-states, with an evolved code of conduct and laws for war. Policy makers and military leaders are used to dealing with "traditional" threats within the nation-state environment. The clearest example is the development, structure, and operation of "conventional" US military forces (e.g. the Army, Navy, Air Force, and Marine Corps) in the implementation of deterrence and containment of the Soviet Union. By and large, this structure also applies to the conventional threats of other countries, such as China, North Korea, or Iran. Two relatively recent and clear demonstrations of

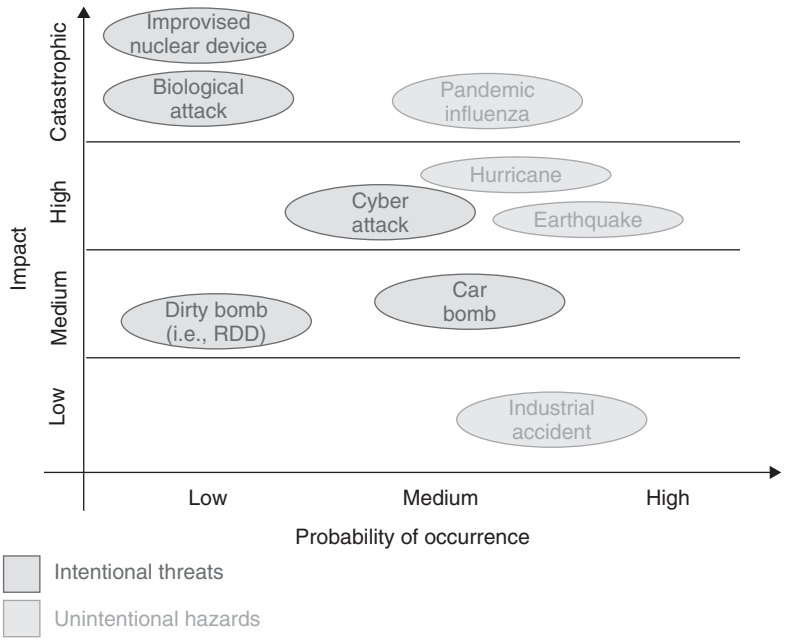



**FIGURE 2** The relative impacts of threats and hazards.

the power of US conventional military force against opposing conventional forces were Operation Desert Storm in 1990–1991 and the 2003 invasion and liberation of Iraq.

The growing threats we face today, at both home and abroad, are asymmetric in both type and means. "Type" implies their nonstate character, for example, transnational groups such as al-Qaeda, Hezbollah, and Hamas. "Means" signifies that our enemies are not seeking to build or deploy conventional military forces or capabilities to match against our own. The reasons why are not difficult to understand because we have clearly demonstrated that no conventional military force in the world is any match against ours. If the purpose of war is to do acts of violence to compel an adversary to do your will, then the acts of violence are only effective if they can be performed, and their results can have great impact.

The means-to-date for organizations such as al-Qaeda and Hamas, although unconventional in deployment, has been utilization of relatively small, conventional explosives against civilian populations and infrastructures. The attack of September 11, 2001, was an unconventional use of a nonmilitary capability, to achieve a significant explosive event. The attacks since have also been asymmetric, directed against innocent civilian populations, but have utilized relatively small explosives:

- Mumbai (July 11, 2006);
- Karachi (March 2, 2006);
- Bali (October 2, 2005);
- London (July 7, 2005);
- Cairo (April 7, 2005);
- Jakarta (September 9, 2004);

- Beslan (September 4, 2004);
- Madrid (March 11, 2004);
- Istanbul (November 20, 2003);
- Casablanca (May 16, 2003);
- Jerusalem (November 21, 2002).

These terrorist attacks have been conducted against civilian populations, with secondary infrastructure impacts, and have killed tens and hundreds. However, the defining characteristic of the security environment we now face is the growing threat of a more substantial and diverse asymmetric attack which could cause catastrophic loss of life and result in mass panic, through the use of a *weapon of mass destruction* (*WMD*) in Pentagon parlance.

In the past, WMDs have been the exclusive domain of nation-states. It is important to note that the United States spent nearly 45 years and billions of dollars to deter their use by the Soviet Union. It is clear that today's terrorists groups will continue in their attempts to obtain, deploy, and ultimately use a WMD involving chemical, biological, radiological, nuclear, or high yield explosive capabilities. They will attempt to use these capabilities against targets in the United States. The bottom-line: terrorists intend to kill more of our people. They have ominously said so, and it is important that we listen:

- Dr. Ayman al-Zawahiri, al-Qaeda's second most influential leader said on July 27, 2006, "All the world is a battlefield open in front of us . . . Our fight is a *jihad* [holy war] for the sake of God and will last until [our] religion prevails . . . from Spain to Iraq . . . We will attack everywhere . . . ";
- Shaykh al-Fahd, a jihadist legal authority, wrote in May of 2003 in his *Treatise on the Legal Status of Using Weapons of Mass Destruction Against Infidels*.: "If people of authority engaged in *jihad* determine that the evil of the infidels can only be repelled by the means of weapons of mass destruction, they may be used."

Asymmetric WMD attacks can be addressed in three general categories. First are those whose consequences would be physically localized and relatively limited in scope. This category would include the use of high explosives, such as a car or truck bomb. A graphic example is the domestic terrorist attack in Oklahoma City, Oklahoma, on April 19, 1995, where a truck bomb was used to destroy the Alfred P. Murrah Federal Building. This attack caused the death of 168 people, its effects were immediate, and physical damage was localized. This category would also include an attack with a chemical weapon, or intentional destruction of a chemical storage site. This type of attack could cause the death of tens to hundreds of people, depending on location and scenario. The effects of a chemical attack would also be relatively immediate, depending on the specific chemical and its properties for dissipation. Physical damage, again, would be localized.

The second category of asymmetric WMD attacks are those whose consequences would be regional and/or persistent. This category would include a cyber attack against a critical infrastructure network. This type of attack probably would not cause many deaths, but could be very disruptive depending on the infrastructure targeted. A successful cyber attack against the financial network could cause loss of assets, and have extremely negative effects on business, markets, and the economy. Another cyber example would be an attack on the electric power grid, that caused a massive regional power outage

similar in consequence to the power blackout of August 14, 2003, in the northeastern United States. This was the largest power blackout in US history, affecting an estimated 10 million people in the United States. and Canada; outage-related financial losses from this single event were estimated at $6 billion.

This category would also include a radiological weapon, also called a *dirty-bomb* or a radiological dispersion device ("RDD"). An RDD is a conventional explosive that is combined with radiological material. In physical damage this type of attack would be very similar to that of a high explosive. However, an RDD could also create additional panic and casualties, especially if used in a metropolitan area. Depending on the radiological material used, it could have contamination and radiation consequences. Therefore, recovery and cleanup could be extremely costly and time-consuming.

The last category of asymmetric WMD attack includes those whose consequences would be catastrophic and persistent. This category would include both biological and nuclear attacks. A biological attack, using something like the bacterial plague, could spread quickly if not contained and could kill thousands of people. The rate of spread would be amplified as a result of both, domestic and foreign travel. This type of attack would put a severe strain on the healthcare system, adversely impacting pharmacies, clinics, and hospitals. While this type of attack would not cause any physical damage to buildings or property, it could cause contamination that requires a costly cleanup.

This last category would also include a terrorist attack using an improvised nuclear device in a metropolitan city. It could kill tens to hundreds of thousands of people, cause incredible physical destruction over a 1–3 mile radius, further contaminate several thousand square miles, and displace more than half-a-million people. The economic impact would be hundreds-of-billions, with years for recovery. Impacts on the civilian population, healthcare system, economy, etc. are almost too grim to contemplate.

In addition to the threats outlined above risk management must also take into account hazards, which in many cases have a higher probability of occurrence than that of terrorist attack. Hazards are defined as nonhostile incidents, such as accidents, technological failure, or natural disasters, which cause loss or damage. Accidents can be due to negligence, bad maintenance, or truly bad luck, resulting in damage or death. A good example of an accident causing large-scale, regional impact was the electric power grid failure in the fall of 2003, mentioned earlier. This was the largest power blackout in US history, and it was caused when strained high voltage power lines shorted out after they came in contact with overgrown trees; it caused a cascading failure of the power network.

Another example of a hazard was the Bhopal disaster of December 1984, that killed at least 20,000 people and injured from 150,000 to 300,000 people. This incident followed the accidental release of 40 tons of a lethal chemical from a Union Carbide industrial plant in Bhopal, India. Later investigations showed that it was due to serious maintenance and safety problems at the plant. The situation degraded further when the transportation system of the city subsequently failed due to the overload and panic. People died when they were asphyxiated or trampled to death, or were seriously injured while trying to escape.

Natural disasters are also hazards that can cause significant death and physical destruction. The San Francisco earthquake of 1905, estimated at a magnitude greater than 7.5, killed at least several thousand people and left 300,000 people homeless. This earthquake and the resulting fire caused major damage to a principal US city and is remembered as one of the worst natural disasters in our history. Hurricane Katrina, and the subsequent levee breaches in New Orleans, is another example of a catastrophic natural disaster.

In August 2005, this Category 3 hurricane directly hit New Orleans, breaching levees and flooding 80% of the city. Over 1500 people were killed, hundreds of thousands displaced, and recovery from the storm is estimated to have cost $81 billion, making it the costliest natural disaster to date in US history. Tsunamis are another example of a natural disaster that can have devastating consequences. The Indian Ocean earthquake in December 2004, triggered massive tsunamis that killed an estimated quarter-of-a-million people and left millions homeless.

A final example of a hazard is an influenza pandemic, which the World Health Organization warns could occur in the next few years. The 1918 Spanish flu pandemic affected almost 25% of the population in the United States, with an estimated death toll of half-a-million. The ease and availability of both domestic and foreign travel would undoubtedly amplify the effect and speed of a pandemic. As with the biological attack scenario discussed previously, an influenza pandemic would add a significant strain on the healthcare system, medical personnel, hospital rooms, and medical supplies and distribution. It is unknown how much social disruption or panic could result, but it is clear that the effects of an influenza pandemic could be catastrophic.

## 5 ADDRESSING PRE-EVENT PREPAREDNESS

When addressing homeland security it is important to understand the relationship between missions, that is, what are the things we need to do, and the preparedness continuum, that is, when we need to do them. The preparedness continuum is a way of outlining the time elements of risk management. It can be articulated in three phases: the pre-event phase, the incident, and the postevent phase. This structure is shown in Figure 3.

The pre-event phase contains those activities and tasks that can and should be performed before an incident occurs. *Prevention* and *Protection* are both pre-event activities, and are discussed in detail below. The postevent phase contains those activities and tasks that can and should be performed after an incident occurs. *Response* and *Recovery* are both postevent activities. *Response* includes the actions taken immediately following an

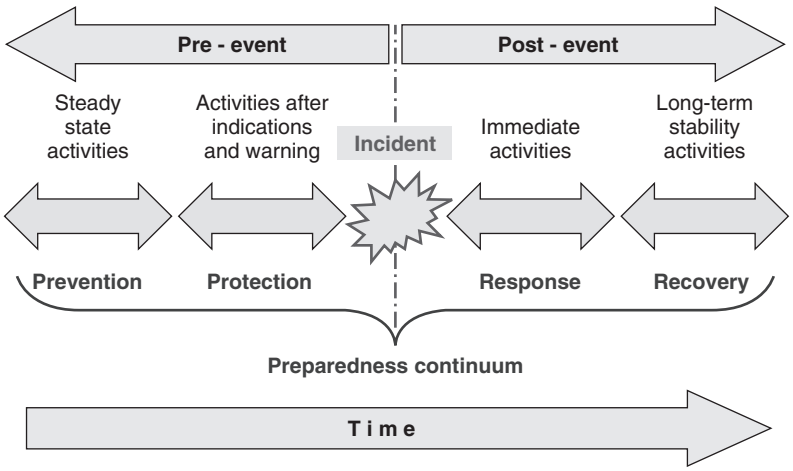



**FIGURE 3** The preparedness continuum.

incident, to save lives and minimize damage to property. *Recovery* includes the actions necessary over the longer term, once immediate response functions are completed, to get people and infrastructures back to their preincident situation.

*Prevention* is the first element in the preparedness continuum, and is the steady-state baseline effort which should be conducted preincident to minimize general risks. There are many activities that contribute to prevention. First is a risk assessment for overall awareness that is, the first step in any assessment should be a prioritization of those functions or activities that are most important. This differentiates between the "must have" and the "nice to have." Once the most important or critical functions have been identified, vulnerabilities can be assessed to determine which threats or hazards could cause damage or loss. Finally, a risk assessment is complete when the probability of occurrence for a threat or hazard is considered.

For those areas considered at risk through assessment, there are many activities that can remediate risk. Remediation includes the actions taken to lessen or correct known vulnerabilities or weaknesses. Maintaining simple awareness of routine situations and, taking note and reporting suspicious activity is a form of remediation. Another way to lessen risk is to add resiliency to a function or network. This can be done through redundancy, by either increasing the number of elements that can perform a function or by increasing the routes between the functioning elements. For example, if the ability of a worker to get to a certain place of business is critical to operations, then a prevention plan for remediation could include having multiple means of travel, or having multiple routes that could be taken, or some combination of both.

Another way to increase resiliency is through stockpiling or storage of critical elements. These can include many examples, such as purchasing and maintaining a power generator in case primary power is lost, or maintaining both landline and cellular phones, or storing water and food. Prevention activities can be performed by organizations, companies, and groups, or by families and individual citizens. As Benjamin Franklin said, "*an ounce of prevention is better than a pound of cure*."

Prevention efforts can also have deterrent effects on enemies contemplating an attack. Since the purpose of terrorism is to cause mass casualties and panic to degrade political will, visible prevention activities such as those discussed above increase overall preparedness and can, therefore, dissuade possible attackers. At the least, attackers have been known to shift target locations if preattack surveillance shows increased levels of prevention and preparedness.

There are many challenges, however, that can hinder the establishment of effective prevention efforts. For example, added awareness through increased surveillance can have civil liberty ramifications. The same cameras used by authorities to detect criminal behavior can also be misused against legitimate civil activities. Another consequence from the use of surveillance systems can be profiling, or the broad targeting of individuals from a specific race or ethnic background. Appropriate overseeing is necessary to avoid these potential misuses of surveillance.

There are challenges related to resiliency as well. As discussed above, added resiliency can be very effective, whether through redundancy or stockpiling, but these activities can have significant financial costs associated with them. An appropriate risk management process can greatly assist in determining which systems require more resiliency or defining the correct balance between active and passive systems for deterrence. The bottom-line challenge concerning overall financial costs of prevention activities is determining the financial risk or business benefit to an intangible like security.

Protection is the second element in the preparedness continuum, and is the additional actions that can be taken preincident to further lessen risks, given appropriate and timely indications or warning. Since protection activities can be linked to indications or warnings of specific threats or hazards, knowing where to focus efforts can be somewhat easier than with the general prevention activities discussed above.

Like prevention, there are many types of activities that contribute to protection. First is changing tactics, techniques, or procedures, called "TTPs" in the military. That is, normal procedures can be modified or altered to lower the risks from a known threat or hazard. A recent example was the changes in the UK and US airport screening and passenger carry-on-items in August 2006, following the discovery of the bombing plot and subsequent arrests of terrorists in London. Knowing the terrorists meant to use initially separate liquid chemicals that could later be mixed on board an aircraft to create explosives allowed changes in both, passenger security screening as well as prohibiting specific items from passenger baggage. Another example of this type of activity would be boarding windows and sandbagging areas following warnings for an approaching hurricane.

Another type of protection activity following a warning would be isolation of, or evacuation from, the targeted asset. These activities could range from disconnecting the asset from the surrounding network to hardening the asset by active guarding or increased physical security measures. Complete isolation could be achieved through a total security lock-out or a full personnel evacuation.

Selecting another asset to perform the function of a targeted asset is another protection activity. This assumes a form of redundancy, such that the selected unthreatened asset can do the work of the asset that is identified at risk. An example would be diverting aircraft to a safe airport from an intended airport under threat of hostile attack or bad weather.

As with prevention, there are many challenges that can hinder implementation of effective protection efforts. In order to implement effective changes in techniques or procedures, the warnings must be specific and credible. In the example discussed above, airline security authorities knew the terrorists intended to smuggle multiple liquid chemicals on board aircrafts to later mix to create explosives. This allowed select materials to be banned from carry-on luggage (e.g. liquids) and specific screening procedures to be implemented. Without this "actionable" intelligence, the subsequent protection efforts would have been greatly hampered.

There are also challenges related to isolation or evacuation. Significant or total isolation is difficult to maintain for extended periods, due to the need to stockpile key components and material, such as equipment, fuel, food, and water, to sustain independent operations. Evacuations can also be challenging, placing increased burdens on transportation systems and networks. The example from the Bhopal disaster, discussed previously, showed what can happen when the transportation system of a city fails due to overload and panic during an evacuation.

There are challenges related to out-sourcing from targeted assets, or hardening or guarding a threatened asset. As discussed above, added protection activities can have significant financial costs associated with them. This cost burden can be compounded if there is uncertainty in the potential duration of the threat, requiring sustained protection activities over an extend period of time.

## 6 ACHIEVING PREVENTION AND PROTECTION SUCCESS

Our country and governmental system are based on the fundamentals of democracy, enabling us to live our lives, enjoy the benefits of liberty, and pursue happiness. We have a long tradition of freedom, a tradition that has stood the test of time, and endured many challenges. There is an inherent tension between freedom and security, a tension that was clearly recognized by our founding fathers, and best articulated by Alexander Hamilton in The Federalist Papers, Number 8:

> "... the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civil and political rights. To be more safe, they at length become willing to run the risk of being less free."

It is important that we recognize this trade-off, and ensure that the efforts we put in place for prevention and protection to meet today's threat and hazard environment do not adversely degrade the very freedoms that are fundamental to our governmental system and our way of life.

Today's risks from terrorism and catastrophic hazards can be successfully managed if we implement a comprehensive approach. True risk management must consider three factors: consequence of loss, vulnerabilities, and probability of threat or hazard occurrence. These three elements must be combined and assessed to enable decision-makers to adequately accept, reduce, or offset risk.

An "all hazards" approach, one that addresses both threats and hazards as discussed above, must also be utilized to ensure we appropriately implement homeland security. The 15 National Planning Scenarios, developed by DHS in April 2005, for use in national, federal, state, and local homeland security preparedness planning, are structured using this all hazards approach. These scenarios span the spectrum of intentionally hostile threats, like chemical, biological, radiological, nuclear threats, or high yield explosives, to hazards like natural disasters and catastrophic accidents. They serve as an outstanding baseline for planning comprehensive prevention and protection activities.

A new updated strategic framework for homeland security must be implemented. This framework must address three areas. This paper discussed elements of one of them, that is, the prevention and protection activities of the broader preparedness continuum. However, the strategic homeland security framework must also include specific mission areas (i.e. what must be done for homeland security) and the domains environment (i.e. where the missions must be performed: on land, in the air, on the sea, and in cyber-space). This updated and comprehensive strategic framework for homeland security is shown in Figure 4.

This new Homeland Security Strategic Framework, based in large part on the preparedness continuum discussed in this paper, provides a context for synergy of effort between all levels of organizations in our country, from the largest government department down to the individual citizen and his respective community. It also places an emphasis on preincident activities, i.e., *prevention* and *protection*, which are proactive and can complement postevent planning. Our homeland security efforts can then be "powered down," meaning moving from the current "Top–Down" environment where large federal and state entities have the most responsibility, to a "Bottom–Up" environment where every

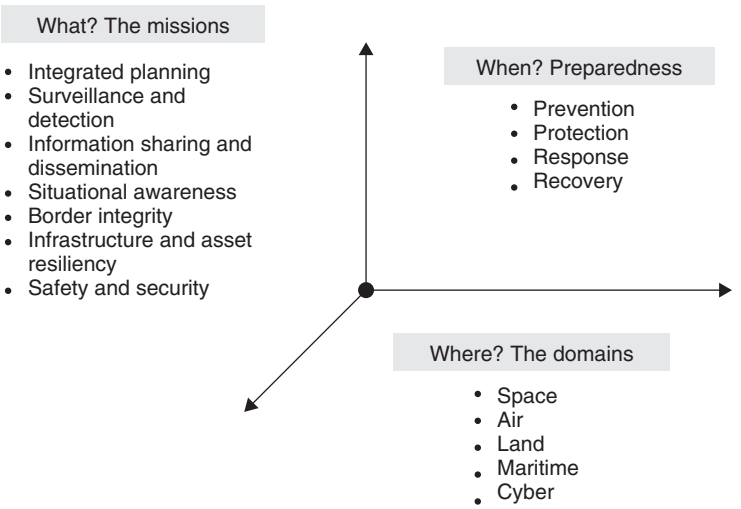



**FIGURE 4** A comprehensive homeland security framework.

citizen, community, and city is empowered to contribute to a truly national effort to enhance our homeland's security.

Frederick the Great, who ruled the Kingdom of Prussia in Europe from 1740 to 1786 and was known as a great military strategist and commander, is quoted as having said: " . . . *he who tries to defend everywhere defends nowhere*." This quote points out the inherent difficulties in defending against a determined enemy and highlights the significant challenges faced in attempting to implement a successful strategy for prevention and protection. However, if we can enlist every citizen as part of the effort, and engage them to actively participate in prevention and protection activities broadly and where possible, I believe we can achieve a level of security for our homeland that is unprecedented and successfully counter both the natural elements as well as those few that would attempt to do us great harm. In this we may be able to prove Frederick the Great wrong—when *everyone* fully participates in the common defense, we can be truly strong *everywhere*.

## FURTHER READING

Hamilton, A., Madison, J., and Jay, J. (1992). *The Federalist Papers*, specifically Numbers 8, 22–29, and 41. Buccaneer Books, Inc., Cutchogue, NY.

*Homeland Security Presidential Directive No. 5, "Management of Domestic Incidents," The White House*. (2003).

*Homeland Security Presidential Directive No. 7, "Critical Infrastructure Identification, Prioritization, and Protection," The White House*. (2003).

*National Infrastructure Protection Plan, the Department of Homeland Security*. (2006).

*National Response Network, the Department of Homeland Security*. (2008).

*National Strategy for Homeland Security, The White House*. (2002).

*Quadrennial Defense Review, the Department of Defense*. (2006).

*Strategy for Homeland Defense and Civil Support, The Department of Defense*. (2005).

# CONSEQUENCE MITIGATION

PO-CHING DELAURENTIS, MARK LAWLEY, AND DULCY M. ABRAHAM
*Purdue University, West Lafayette, Indiana*

## 1 INTRODUCTION

The 1998 President's Commission on Critical Infrastructure Protection identified telecommunications, energy systems, water supply systems, transportation, banking and finance, and emergency and government services as essential core infrastructures for our modern society. A later national plan for critical infrastructure protection developed jointly by the Executive Office of the President, Office of Science and Technology Policy (OSTP) and the Department of Homeland Security (DHS), identified other key infrastructures such as agriculture and food, the defense industrial base, national monuments and icons, dams, commercial facilities, nuclear reactors, and materials and waste [1].

The increase in terrorist activities around the world, the possible use of weapons of mass destruction, and acts of nature such as earthquakes and floods pose threats to the security of various civil infrastructure systems. Further, increasing population concentrations have significantly stressed many infrastructure systems [2]. These factors combined with the cascading effects of system failures in power grids, telecommunication networks, transportation systems, and so on, intensify the need for effective disaster response planning and mitigation strategies.

Many definitions have been proposed for disaster/hazard/consequence mitigation. In this article, consequence mitigation refers to response strategies performed on existing infrastructures after an attack or disaster has occurred. It uses existing resources to take effective actions in order to minimize damage and propagation of damage and loss of life and property. Consequence mitigation strategies include contingency plans, rapid recovery plans, and operational tactics. Examples of these include damage control, toxic agent confinement, first responder deployment, and resource reallocation [3]. Figure 1 illustrates the distinction between mitigation strategies for pre- and postdisaster planning and response.

## 2 SCIENTIFIC OVERVIEW

There is only limited research in consequence mitigation. Most existing work focuses on public policy and government planning issues, with little emphasis on operational issues. Researchers distinguish between the goals of disaster prevention and consequence mitigation. Prevention focuses on preparation activities that reduce the likelihood of adverse events. These may include security improvements, upgrades in topology, addition of redundancies, and/or resiliency enhancements. In contrast, mitigation involves alleviating disaster effects, responding to their impacts, and recovering from the consequences.

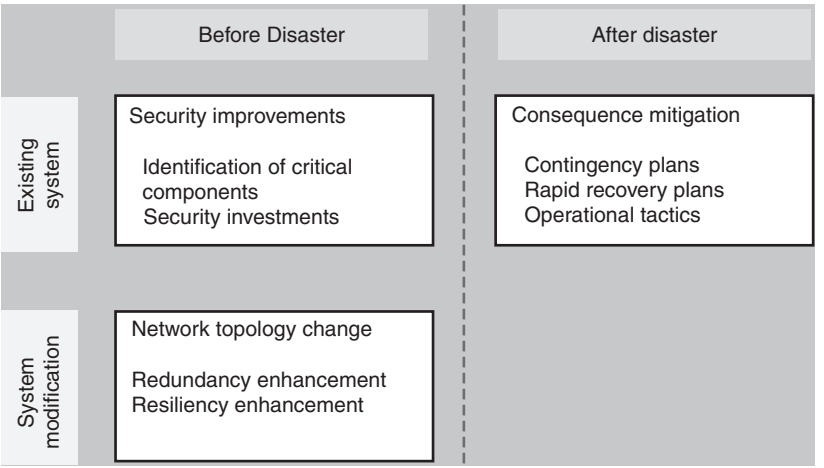



**FIGURE 1** Disaster response and planning for infrastructure systems (adapted from Qiao et al. [3]).

Recovery may involve reconstruction of damaged facilities, restoration of physical and social networks, rehabilitation (including psychological recovery), and restitution (such as return to a previous physical or societal state). Both prevention and mitigation depend on predisaster planning and preparation.

The following sections provide an overview of recent mitigation research, mitigation tactics and technologies, and effectiveness measures for mitigation efforts.

## 2.1 Active Research Work and Recent Accomplishments

The National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan was established in 2004 by the US DHS and the OSTP [1]. This plan identifies the critical R&D needs in securing the nation's infrastructures and key resources, and outlines several science, technology, and engineering themes that support all aspects of infrastructure protection.

The NCIP R&D Plan summarizes recent accomplishments in the development of strategies for consequence mitigation. It includes ongoing activities regarding protection of critical infrastructures undertaken by different agencies in the United States. Key highlights of consequence mitigation related efforts are listed in Table 1.

## 2.2 Mitigation Technologies and Tactics

There are different ways for mitigating disaster damages and potential hazards. One tactic aims at providing early detection and monitoring of the progression of a disaster so that damage control can be implemented at the earliest. Another method is the application of technologies that help minimize the damage caused by a disaster. Proper training for emergency workers who are called to respond to disasters is also deemed necessary for effective disaster mitigation.

***2.2.1 Communication.*** A commonly suggested means for consequence mitigation is reliable wireless information technology (IT) infrastructure [6] that can be deployed in

**TABLE 1 Ongoing and Recent Efforts of Consequence Mitigation by National Agencies in the United States**

| Agency | Highlights of Consequence Mitigation Effort |
|---|---|
| Department of Defense (DOD) | Development of technology for unexploded ordnance and dangerous materials detection inside assets and underground facilities |
| Department of Energy (DOE) | Development and deployment of a real-time global positioning system (GPS) with synchronized wide-area sensor network systems for electric grid monitoring and control |
| | Development of decontamination foam, which neutralizes chemical and biological agents in minutes |
| Department of Labor (DOL) | Developing protection, decontamination, and training guidance for hospital-based first receivers of victims of biological/chemical weapons of mass destruction |
| National Science Foundation (NSF) | Supporting research in nano- and biotechnology applications in protective materials and devices, new architectures for secure and resilient cyber and physical infrastructures, and sensors and sensor networks |
| US Department of Homeland Security, Federal Emergency Management Agency (FEMA) | *Best practice portfolio*—contains a collection of ideas, activities/projects, and funding sources that can help reduce or prevent the impacts of disasters, and is searchable by state, county, sector type, hazard, category/activity/project, and keywords [4] |
| US Environmental Protection Agency (EPA) and National Homeland Security Research Center (NHSRC) | Homeland security scientific research and technology development activities consist of the following: (i) threat and consequence assessment of human exposure to hazardous materials; (ii) decontamination and consequence management; (iii) water infrastructure protection; (iv) emergency response capability enhancement; (v) technology testing and evaluation [5] |

various scenarios as an independent and secured emergency communication system [7]. Emergency management and control and responders may rely heavily on such infrastructure to communicate during disasters particularly when the public communications infrastructure is destroyed or severely damaged by the disaster. Developing frameworks for coordinated chains of communication is essential to provide quick response to victims as well as to ensure the safety of the responders.

***2.2.2 Hazard Detection.*** Chemical/biological (C/B) or radiological attacks, in general, are difficult to detect and control especially in public spaces. The Program for Response

Options and Technology Enhancements for Chemical/Biological Terrorism in Subways (PROTECTS) is an initiative of the Department of Energy aimed at developing and applying technologies dealing with C/B terrorism. It covers both emergency planning and response phases of an incident and focuses on modeling and analyzing responses using engineering technologies [8]. A key technology developed by the PROTECTS program is the detection of the release of a C/B or radiological attack. Detection can be made by agent sensors, artificial intelligence, and video technologies. An artificial intelligence algorithm is used to recognize certain patterns of motion and sounds that are characteristics of a panicking crowd. The confirmation of a true incidence (not a false alarm) is then done by inspecting closed-circuit TV images. The use of this technology helps to keep casualties low since the situation can be observed remotely. Another frequently mentioned technology is sensor networks [9–11]. A sensor network is a collection of small, low-cost, and low-power devices with limited memory storage and wireless communication capabilities. One application is the personal digital assistant (PDA)-based multiple-patient triage device that can be used for on-scene patient triage, tracking, data recording, and monitoring of the physical environment. These data can help a medical facility prepare and appropriately allocate required resources (e.g. medical staff, beds, and operating rooms) before patients arrive, especially in a mass casualty scenario. Another sensor network application is the use of vital sign sensors that can be worn by disaster victims and first responders. These sensors can monitor a patient's physical condition and relay data to emergency medical personnel, enabling them to manage multiple patients simultaneously and be alerted if there are sudden changes in a patient's physiologic status [9]. Bioscience is another type of technology that can be used to detect hazards. For instance, the Sandia National Laboratories have been developing a state-of-the-art type of technology that uses special proteins to accurately and quickly detect specific bioterror threat agents [12].

***2.2.3 Mitigating Technologies.*** Several technologies can be applied in mitigating hazard from a C/B attack: (i) inflatable barriers for blocking the spread of agent, (ii) water curtains, air curtains, and water or foam sprays for containing and detoxifying contaminated air, (iii) support tools for first responders and incidence commanders, such as hand-held devices that can receive information on-site, and (iv) training and exercises [8]. The Sandia National Laboratories have been active in developing effective tools to counter C/B attacks. One technology is containment foam that can be rapidly applied around an explosive device in order to reduce the blast effects and to capture the hazardous material that may be further spread [13]. Special types of coating materials can be used to contain radioactive materials by binding them, thereby preventing them from spreading. The lab has also developed bomb disablement tools that can be deployed by first responders to disable improvised explosive devices (IEDs) safely and remotely while preserving forensic evidence [12]. Successful technology applications are adopted by various US government agencies such as the DHS, the National Institute for Occupations Safety and Health (NIOSH), and the US Army.

***2.2.4 Training.*** Emergency response/recovery technologies will not be effective without well-trained personnel [7]. Thus, organizations responsible for emergency or disaster mitigation tasks should provide proper training for first responders and incident management teams. Federal Emergency Management Agency (FEMA)'s Emergency Management Institute (EMI) provides a comprehensive list of training courses, both on-line

and on-site, for emergency management officials [14]. In addition to educational and knowledge-based training, scenario-based physical exercises, such as simulated fires in a subway system, can also be an effective way for first responders and the incident commander to respond and implement optimal ventilation control strategies [8]. The Technical Support Working Group (TSWG), a US interagency forum, dedicates itself to developing technologies and equipment for the needs of the combating terrorism community. TSWG's training efforts include the development of "delivery architectures" (e.g. knowledge management systems and software architectures), "advanced distributed learning" (e.g. tools and guidelines for developing standard training materials), along with "training aids, devices and simulations" (e.g. virtual reality and computer-based simulations) [15].

***2.2.5 Modeling and Simulation.*** Modeling and simulation tools can be used to understand what happens in disasters and thus what needs to be done in the mitigating and recovery stages. These tools can also be used as training exercises for the first responders, as well as the command and control personnel of Emergency Operations Centers (EOC) at all levels. In 2003 and 2004, the National Institute of Standards and Technology (NIST) held workshops on *Modeling and Simulation for Emergency Response* aimed at utilizing modeling and simulation technologies to better prepare for, mitigate, respond to, and recover from emergencies. Table 2 summarizes the range of emergency response modeling and simulation application tools discussed in the workshop. Details on the standard and related tools available can be found in Appendices A and B in NIST's report [16].

Bryson et al. [17] pointed out that there have been few studies in disaster recovery plan modeling in the management science (MS) and operations research (OR) community. They demonstrated an application of mathematical modeling techniques for decision-making support for disaster recovery planning, suggesting the need for dedicated efforts in integrating technical and MS/OR knowledge and techniques so that mitigation tactics and strategies can be more efficient and effective.

## 2.3 Effectiveness Measures

In addition to pursuing state-of-the-art technologies and techniques for disaster consequence mitigation planning and implementation, having precise and accurate methods for evaluating the effectiveness and efficiency of the mitigation actions is very important. Effectiveness measures can serve as a real-time feedback mechanism in the process of mitigating a disaster so that decision makers and responders can adjust plans and tactics accordingly. Examples of effectiveness measures include (i) public management—evacuation, restriction of entry, and quarantine; (ii) damage control—damage evaluation and pinpointing, agent confinement and elimination (e.g. toxic substance), and providing alternative sources of service; and (iii) recovery and rebuilding. However, the real challenge lies in defining and determining these effectiveness measures. Some methods that can help achieve the goals of effectiveness measures of consequence mitigation based on general emergency management include the following:

1. *Effectiveness measures developed from past experience*. After Hurricane Katrina devastated the New Orleans region in 2005, emergency response agencies began

**TABLE 2 List of Modeling and Simulation Applications for Emergency Response Talks in NIST 2003 Workshop**

| Purpose | Application Tool | Developer |
|---|---|---|
| Planning applications | Virtual reality (VR) modeling and simulation—using geographic information systems (GISs) data, drawings, building plans, and city maps are processed using terrain generation software | Institute for Defense Analyses (IDA) |
| | JWFC simulation toolbox—providing multiechelon simulation across federal, state, and local government agencies | Joint Warfighting Center (JWFC) |
| | 3D digital modeling, simulation, communication, and emergency response database (including facility models of high risk sites and libraries of the "best practice" processes) | Dassault Systems, Data Systems & Solutions (DS&S), Science Applications International Corporation (SAIC), and SafirRosetti |
| | Mass prophylaxis planning using ARENA simulation and queueing analysis in Excel | Department of Health and Human Services (DHHS), Agency for Healthcare Research and Quality (AHRQ) |
| Training | Top Officials (TOPOFF)—a national-level "real-time" weapons of mass destruction (WMDs) response exercise | The Department of Justice, the Department of State, and the Federal Emergency Management Agency (FEMA) |
| | 2D simulations for command and control exercises of fire incidents | National Fire Programs, US Fire Administration, FEMA |
| | Automated exercise and assessment system (AEAS)—for emergency response and emergency management practitioners from the infrastructure owner/operator and local and state jurisdictional levels specific to WMD terrorist attacks | National Guard Bureau (NGB) |
| Real-time response | Tools and services for atmospheric plume predictions—in time for an emergency manager to decide if taking protective action is necessary to protect the health and safety of people in affected areas | National Atmospheric Release Advisory Center (NARAC) |

to evaluate strategies for better evacuating and sheltering of residents and reducing loss of lives and properties. Whatever actions and plans were taken during that specific incident, for example, can serve as "the least effective" measure. Future mitigation plans and strategies for responses during hurricanes can then be improved by benchmarking against this measure.

2. *Use of risk and vulnerability assessment/mapping*. Risk and vulnerability assessment/mapping can be used for designing mitigation tasks and examining if current mitigation strategies and tactics are sufficient or effective. For example, matrices of multiple hazards can be used to analyze the relevance of different mitigation tools for responding to various hazards. Risk and vulnerability mapping can also be used as a tool to show the probabilities of disaster occurrences as well as the possible damage on physical properties, community infrastructure systems, and human lives [18].
3. *Simulation models*. Even though simulation may not provide the optimal solution, it can be useful as an effectiveness measure for disaster/hazard mitigation in integrating predisaster and postdisaster management and action plans and tactics to validate their effectiveness in a virtual environment. For example, the use of computer simulation for assessing the benefits of new technologies for disaster mitigation could reveal significant insight of such applications in a cost- and time-efficient manner [19]. Discrete event simulation and agent-based modeling, combined with human-in-the-loop and live simulation can provide significant insights on the effectiveness and efficiency of disaster responses.
4. *Use of detection device and remote sensing tools*. Detection devices such as sensors that can monitor or detect levels of C/B agents may be used after some hazardous material has been released. From these sensor readings, responders can determine the speed at which the agent is spreading or determine if the agent is confined where it was released. On the basis of this assessment they can plan their response. Then using real-time sensing, they can obtain feedback to assess whether their actions were effective in the situation.

## 3 ACTIVE RESEARCH AND FUNDING

Funding for research efforts in consequence mitigation has seen a surge since September 11, 2001. Table 3 lists several sources of funding for consequence mitigation.

## 4 CRITICAL NEEDS ANALYSIS

Consequence mitigation focuses on recovery after an attack or disaster has occurred. Technologies, such as those discussed above, support disaster mitigation efforts by providing more precise postdisaster information, such as pinpointing the location and amount of a toxic chemical released. Nevertheless, there is little discussion of the operational aspects of the disaster mitigation effort itself, that is, on the mitigation decision-making processes, triggering events, responder coordination, and so forth. Thus, research contributions in the following areas are essential for effective operational response after disaster.

### 4.1 Multiorganizational Coordination

In any disaster scenario, it is likely that multiple agencies across different jurisdictions in the affected area would participate in the mitigation effort. For example, if a C/B attack

**TABLE 3 Research Funding Available in the United States and Other Countries**

| Agency | Funding Interest |
|---|---|
| US Sources of Funding | |
| National Science Foundation (NSF)—Division of Civil, Mechanical and Manufacturing Innovation, Infrastructure Management and Extreme Events (IMEE) [20] | For scientists, engineers, and educators focusing on large-scale hazards on civil infrastructure and society, and on issues of preparedness, response, mitigation, and recovery. |
| National Science Foundation (NSF)—hazards mitigation and structural Engineering (HMSE) [21] | For scientists, engineers, and educators working on fundamental research such as the design and performance of structural systems, and new technologies for improving the behavior, safety, and reliability of structural systems and their resistance to natural hazards. |
| Centers for Disease Control and Prevention (CDC)—engaging state and local emergency management agencies to improve states' ability to prepare for and respond to bioterrorism (funding opportunity number: CDC-RFA-TP06-601) [22] | Preparing the Nation's public health systems to minimize the consequences associated with natural or man-made, intentional or unintentional, disasters. Funding is only available to the National Emergency Management Association (NEMA). |
| National Institutes of Health—Small Business Innovation Research (SBIR) E-learning for HAZMAT and emergency response (SBIR [R43/R44]) [23] | For small businesses concerning the development of advanced technology training (ATT) products for the health and safety training and hazardous materials (HAZMAT) workers, emergency responders, and skilled support personnel. |
| US Department of Homeland Security—FEMA Hazard Mitigation Grant Programs (HMGP) [24] | For states and local governments for implementation of long-term hazard mitigation measures after a major disaster declaration. |
| US Department of Homeland Security—Predisaster Mitigation Grant Program [24] | For states, territories, Indian tribal governments and communities for hazard mitigation planning and the implementation of predisaster mitigation projects. |
| US Department of Homeland Security Office of Grants and Training—2006 Homeland Security Grant Program (HSGP) [25] | For state and urban areas to obtain critical resources to achieve the interim national preparedness goal and implement homeland security strategies. |
| US Department of Homeland Security Office of Grants and Training—Emergency Management Performance Grant (EMPG) [25] | The objective of this program is to help states develop effective emergency management systems that encourage the cooperation and partnership among government, business, volunteer, and community organizations and thus strengthening their preparedness for catastrophic events and emergency management capabilities. |

**TABLE 3 (*Continued*)**

| Agency | Funding Interest |
|---|---|
| International Sources of Funding | |
| The European Mediterranean Disaster Information Network (EU-MEDIN)—applied multirisk mapping of natural hazards for impact assessment (ARMONIA) [26] | To provide the European Union (EU) with harmonized methodologies for producing integrated risk maps to achieve effective spatial planning in areas prone to natural disasters in Europe. |
| Disaster Hazard Mitigation Project Kyrgyz Republic [27] | To achieve (i) minimizing the exposure of humans, livestock, and riverine flora and fauna to radionuclides associated with abandoned uranium mine tailings and waste rock dumps in the Mailuu-suu area; (ii) improving the effectiveness of emergency management and response by national, local government agencies and local communities; (iii) reducing the loss of life and property in key landslide areas of the country. |
| Australian Government—the local grants scheme (LGS) and the national emergency volunteer support fund (NEVSF) [28] | For local governments to help communities develop and implement emergency management initiatives and enhance critical infrastructure protective measures, as well as to provide training of security awareness for local government staff. |

were to occur at a subway station in a city, the local jurisdiction levels involved would include the subway management team (e.g., the city transportation administration), the city government, and the county in which the city is located. Public, private, and nonprofit organizations would need to coordinate their actions with each other and across jurisdictions to create a dynamic emergency response system to ensure effective mitigation and response to a disaster. Since the most effective response processes and plans will transcend political and response agency boundaries, coordinated response plans must be developed through the collaborative efforts of all key responders.

### 4.2 Management Framework

A disaster response management framework is needed for supporting decision makers in a disaster scenario. Such an emergency management framework should include the use of real-time monitoring of the situation (such as the general environment, infrastructure systems, first responders, and victims) and real-time information and communication tools, both vertically in the organizational structure and horizontally among responders. Coordination of effective reporting from multiple sites (for instance, in an earthquake rescue effort) should also be incorporated in the framework so that mitigation decisions can be made to achieve effective and efficient actions taken to minimize negative impacts of a disaster [29]. Research on technology integration for real-time information exchange, decision-making support systems, and cross-infrastructure recovery efforts is very much needed. Furthermore, since response resources are likely to be limited or overwhelmed, it is important to prioritize response activities. Scarce resource allocation decisions need

to be modeled, analyzed, and optimized beforehand to ensure that the most effective priorities and trade-offs occur during response.

## 5 RESEARCH DIRECTIONS

Four major themes can be identified for future research.

### 5.1 Computing Hardware, Software, and Research Tools

In the current environment, network of computers and devices embedded in infrastructure systems are susceptible to crippling cyber attacks. Thus, there is a significant need for next-generation Internet architectures that are designed to have security and inherent protection features at all levels of hardware and software [1]. The NCIP R&D plans propose the designing of cyber infrastructures that are resilient, self-diagnosing, and self-healing. In addition, future research will need to focus on developing integrated systems architecture/framework so that management and responders across jurisdictions and hierarchical response organizations can be well coordinated.

### 5.2 Interdependencies between Civil Infrastructures

Since modern civilization relies heavily on basic civil infrastructures that are interdependent of each other, improving coordination of security precautions taken by different utility systems is also an important task. In other words, it is necessary to look beyond the effects of an incident on a single system. Instead, future technologies and practice should be able to understand the perturbed behaviors of a complex, "system of systems" [30], which includes the unexpected cascading effects of infrastructure damage and failure. A good example is the concept of "resilient cities" that focuses on strengthening physical and social elements of an urban area and on bridging natural hazard and antiterrorism predisaster mitigation and postdisaster response strategies [31]. More effective use of technology transfer and broader industry/government support are needed to achieve the effectiveness of consequence mitigation for the industry/society as a whole [7].

### 5.3 Sensing Technologies for Assessment

Advanced sensing technologies are essential for assessing the causes and effects of disaster events. Future infrastructures must be designed with more embedded sensing, diagnostic, and predictive capabilities. Integrated sensor networks with powerful computational and communication capabilities are now becoming a reality, and infrastructural planners, engineers, managers, and operators must develop fuller understandings of how these can be incorporated into design and decision processes. For instance, a real-time building damage sensing network could be used to assess the condition of a building after an extreme event, such as an earthquake. This type of information would greatly help disaster responders responsible for evacuation, search, rescue, and building reenforcement efforts. Further, remote sensing technologies, such as satellite images, are especially helpful in surveying a large affected area [32].

### 5.4 Modeling and Analysis of Disaster Scenarios, Mitigation Plans, and Response Efforts

Simulation modeling can be very useful in assessing the effectiveness of mitigation plans for different disaster scenarios. For example, scenario analyses of various types and/or severity of terrorist attack can be performed using simulation. This type of "what if" analysis serves as a virtual exercise test bed for identifying critical mitigation resources and improving mitigation plans and decisions. Furthermore, optimization techniques are very useful for analyzing decision problems where priorities must be considered and trade-offs must be made. For example, reconfiguring damaged infrastructures and prioritizing repair tasks to optimally meet a population's demand during repair can be addressed by using advanced optimization techniques from Operations Research and Management Science. Technical challenges associated with developing these types of simulation and optimization models include model abstraction, validation, data scarcity, computational requirements, identifying appropriate objective functions, and interpreting the results, among others. A significant practical challenge is engaging laypeople in the development of the models and in ensuring that users of the model have adequate confidence in the results obtained through the models. Although this type of analysis has a long history in other large-scale planning and operation efforts such as manufacturing and transportation, it is in its infancy in disaster mitigation and response planning. Thus, there are significant opportunities for researchers to make seminal contributions in this area. One example is the application of a computer interface that integrates an agent-based discrete event simulation model and a geographic information system such that real-time data exchange and communication can coordinate and facilitate large-scale disaster response efforts [33]. Stochastic programming technique can be applied to address the issue of transporting first aid commodities and response personnel in an earthquake scenario [34]. Other examples of this type of work can be seen in [35–37].

## REFERENCES

1. The Executive Office of the President Office of Science and Technology Policy (OSTP), and the Department of Homeland Security Science and Technology Directorate. (2004). *The National Plan for Research and Development in Support of Critical Infrastructure Protection*, US Department of Homeland Security, Washington, DC.
2. Hamilton, R. M. (2000). Science and technology for natural disaster reduction. *Nat. Hazard. Rev.* **1**(1), 56–60.
3. Qiao, J., Jeong, H. S., Lawley, M. A., and Abraham, D. M. (2006). Physical security aspects in water infrastructure. In *Advances in Homeland Security Volume 1, The Science of Homeland Security*, S. F. Amass, A. K., Bhunia, A. R., Chaturvedi, D. R., Dolk, S. Peeta, and M. Atallah, Eds. Purdue University Press, pp. 37–62.
4. FEMA. FEMA Mitigation Best Practices Search. (2008). http://www.fema.gov/mitigationbp/index.jsp.
5. U.S. Environmental Protection Agency. (2008). Homeland Security Research, http://www.epa.gov/nhsrc/index.htm.
6. Midkiff, S. F., and Bostian, C. W. (2002). Rapidly-deployable broadband wireless networks for disaster and emergency response. *The First IEEE Workshop on Disaster Recovery Networks (DIREN '02)*. June 24, 2002, New York.

7. Schainker, R., Douglas, J., and Kropp, T. (2006). *Electric Utility Responses to Grid Security Issues. IEEE Power and Energy Magazine*, March/April, 31–37.
8. Policastro, A. J., and Gordon, S. P. (1999). The use of technology in preparing subway systems for chemical/biological terrorism. *APTA 1999 Rapid Transit Conference*. Toronto, ON.
9. Lorincz, K., Malan, D. J., Fulford-Jones, T. R. F., Nawoj, A., Clavel, A., Shnayder, V., Mainland, G., Welsh, M., and Moulton, S. (2004). Sensor networks for emergency response: challenges and opportunities. Pervasive computing. *IEEE* **3**(4), 16–23.
10. ARC Research Network on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP) Applications. (2007). http://www.ee.unimelb.edu.au/ISSNIP/apps/index.html.
11. Zussman, G., and Segall, A. (2003). Energy efficient routing in ad hoc disaster recovery networks. *Proceedings IEEE INFOCOM 2003 Conference*. San Francisco, CA.
12. Sandia National Laboratories. (2006). *Defense Against Chemical and Biological Threats*. http://www.sandia.gov/mission/homeland/chembio/development/biotechnology/index.html.
13. Sandia National Laboratories. (2008). *Explosive Countermeasures*. http://www.sandia.gov/mission/homeland/programs/explosives/index.html/.
14. FEMA Emergency Management Institute. (2008). http://training.fema.gov/.
15. The Technical Support Working Group. (2008). http://www.tswg.gov/.
16. National Institute of Standards and Technology. (2008). *Modeling and Simulation for Emergency Response Workshops*. http://www.mel.nist.gov/div826/msid/sima/simconf/mns4er.htm.
17. Bryson, K.-M., Millar, H., Joseph, A., and Mobolurin, A. (2002). Using formal MS/OR modeling to support disaster recovery planning. *Eur. J. Oper. Res.* **141**, 679–688.
18. Godschalk, D. R., and Brower, D. (1985). Mitigation strategies and integrated emergency management. Public administration review. *Public Adm. Rev.* **45**, 64–71, Special Issue.
19. Robinson, C. D., and Brown, D. E. (2005). First responder information flow simulation: a tool for technology assessment. *Proceedings of the 37th Conference on Winter Simulation*, Orlando, FL.
20. NSF. *Infrastructure Management and Extreme Events (IMEE)*. (2008). http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13353&org=CMMI.
21. NSF. *Hazard Mitigation and Structural Engineering (HMSE)*. (2008). http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13358&org=CMMI&sel_org=CMMI&from=fund.
22. CDC Grant. (2007). http://www.grants.gov/search/search.do?oppId=10597&mode=VIEW.
23. Department of Health and Human Services. (2005). http://grants.nih.gov/grants/guide/rfa-files/RFA-ES-05-003.html.
24. FEMA. (2008). *FEMA Hazard Mitigation Grant Programs*. http://www.fema.gov/government/grant/hmgp/.
25. U.S. Department of Homeland Security, Office of Grants and Training (G&T). (2008). http://www.ojp.usdoj.gov/odp/about/overview.htm.
26. *ARMONIA –Applied multi Risk Mapping of Natural Hazards for Impact Assessment*. (2008). http://www.ist-world.org/ProjectDetails.aspx?ProjectId=46f1c981ed3b4821947cd3624b820fb4&SourceDatabaseId=7cff9226e582440894200b751bab883f.
27. Disaster Hazard Mitigation Project Kyrgyz Republic. (2004). http://web.worldbank.org/external/projects/main?pagePK=64283627&piPK=73230&theSitePK=40941&menuPK=228424&Projectid=P083235.
28. Australian Government. National Emergency Volunteer Support Fund (NEVSF). (2008). http://www.ema.gov.au/communitydevelopment.
29. Comfort, L. K., Dunn, M., Johnson, D., Skertich, R., and Zagorecki, A. (2004). Coordination in complex systems: increasing efficiency in disaster mitigation and response. *Int. J. Emerg. Manage.* **2**(1-2), 62–80.

30. Little, R. G. (2003). Toward more robust infrastructure: observations on improving the resilience and reliability of critical systems. *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*. Big Island, HI.

31. Godschalk, D. R. (2003). Urban hazard mitigation: creating resilient cities. *Nat. Hazard. Rev.* **4**(3), 136–143.

32. Adams, B. J., Huyck, C. K., Gusella, L., Wabnitz, C., Ghosh, S. and Eguchi, R. T. (2006). Remote Sensing Technology for Post-Earthquake Damage Assessment- A Coming of Age. *Proceedings of the 8th U.S. National Conference on Earthquake Engineering*. April 18–22, San Francisco, CA.

33. Wu, S., Shuman, L., Bidanda, B., Kelly, M., Sochats, K. and Balaban, C. (2007). Disaster policy optimization: a simulation based approach. *Proceedings of the 2007 Industrial Engineering Research Conference*. Nashville, TN.

34. Barbarosoglu, G., and Arda, Y. (2004). A two-stage stochastic programming framework for transportation planning in disaster response. *J. Oper. Res. Soc.* **55**, 43–53.

35. Friedrich, F., Gehbauer, F. and Rickers, U. (2000). *Optimized Resource Allocation for Emergency Response after Earthquake Disasters, Safety Science 35.*

36. Altay, N., and Green, W. G., III. (2006). OR/MS research in disaster operations management. *Eur. J. Oper. Res.* **175**, 475–493.

37. Lee, E., Maheshwary, S., Mason, J., and Glisson, W. (2006). Large-scale dispensing for emergency response to bioterrorism and infectious-disease outbreak. *Interfaces* **36**(6), 591–607.

## FURTHER READING

### Disaster Planning and Public Policy

Berke, P. R., Kartez, J., and Wenger, D. (1993). Recovery after disaster: achieving sustainable development, mitigation and equity. *Disasters* **17**(2), 93–109.

Comfort, L., Wisner, B., Cutter, S., Pulwarty, R., Hewitt, K., Oliver-Smith, A., Wiener, J., Fordham, M., Peacock, W., and Krimgold, F. (1999). Reframing disaster policy: the global evolution of vulnerable communities. *Env. Hazard* **1**, 39–44.

Godschalk, D., Beatley, T., Berke, P., Brower, D. J., and Kaiser, E. J. (1999). *Natural Hazard Mitigation Recasting Disaster Policy and Planning*, Island Press, Washington, DC.

Freeman, P. K., Martin, L. A., Linnerooth-Bayer, J., Mechler, R., Pflung, G., and Warner, K. (2003). *Disaster Risk Management: National Systems for the Comprehensive Management of Disaster Risk and Financial Strategies for Natural Disaster Reconstruction*. Inter-American Development Bank, Sustainable Development Department, Environment Division, Integration and Regional Programs Department, Regional Policy Dialogue, Washington, DC.

### Technical Research

Jacobson, S. H., Kobza, J. E., and Pohl, E., Eds. (2007). *IIE. Trans.* **39**(1), Special Issue on Homeland Security.

### General Research for Natural Disasters

Cruz, A. M. (2008). *Engineering Contribution to the Field of Emergency Management*. http://training.fema.gov/EMIWeb/edu/docs/Engineering%20Contribution.pdf.

Heaney, J. P., Peterka, J., and Wright, L. T. (2000). Research needs for engineering aspects of natural disasters. *J. Infrastruct. Syst.* **6**(1), 4–14.

# SECURITY ASSESSMENT METHODOLOGIES FOR U.S. PORTS AND WATERWAYS

D. Brian Peterman, Joseph DiRenzo III, and Christopher W. Doane
*United States Coast Guard*

## 1 INTRODUCTION

The challenge of securing critical infrastructure within the US Maritime Domain is daunting. With over 95,000 miles of maritime border, 361 maritime ports, thousands of critical maritime facilities, and millions of recreational and commercial maritime users, the US Maritime Domain is too vast to be completely protected. Compounding the problem is the Maritime Transportation System that provides over $700 billion a year to the nation's economy; a system that is highly sensitive to interruption. The only feasible solution to this maritime security dilemma is to prioritize maritime security efforts using a rigorous process to assess risk at the national, regional, and port levels. Since the horrific attacks of September 11, 2001, the US Coast Guard has developed, refined, and continuously updated maritime risk assessment tools and methods to inform maritime security operations against the ever-changing worldwide asymmetric terrorist threat. Settling upon the equation, risk = threat × vulnerability × consequence, the capability to assess maritime risk is now several iterations ahead of where the country was after the attacks. This assessment process will remain a "living process" requiring constant modification to stay apace of changes in maritime use and terrorist adaptations to security measures.

## 2 BACKGROUND

The attractiveness of the US Maritime Domain to terrorists is captured in the US National Strategy for Maritime Security, "the infrastructure and systems that span the maritime domain ... have increasingly become both targets of and potential conveyances for dangerous and illicit activities" [1, p. 2]. The challenge of protecting the US maritime is daunting for multiple reasons. The country's maritime borders, rivers, and waterways are extensive; the maritime border alone is over 12,400 miles [2, p. 6; 3]. These shorelines are host to thousands of facilities either critical to the national economy and/or processing highly volatile or toxic materials dangerous to nearby populations. The waterways also contain other critical infrastructure, such as locks and dams, whose damage or destruction would have dire effect on the Maritime Transportation System in addition to population. "The challenge is immense as it involves nearly 13 million registered US recreational vessels, 82,000 fishing vessels and 100,000 other small vessels" [4, p. i]. The potential

security challenge posed by recreational boats is made even more complicated with each state maintaining vastly different databases that do not electronically connect or share information easily or by automation.

The only solution for reducing risk to such a vast and complex system as the US Maritime Domain without undermining the Maritime Transportation System is to employ a risk-based strategy, identifying and focusing security efforts on high risk targets while preparing to minimize the consequences of attacks that do occur. This concept is clearly stated in the country's National Strategy for Homeland Security, "We accept that risk—a function of threats, vulnerabilities, and consequences—is a permanent condition. We must apply a risk-based framework across all homeland security efforts in order to identify and assess potential hazards (including downstream effects), determine what levels of relative risk are acceptable, and prioritize and allocate resources among all homeland security partners, both public and private, to prevent, protect against, and respond to and recover from all manner of incidents" [5, p. 41].

### 2.1 Risk Assessment Methods

An understanding of "risk" and its associated components of "threat," "vulnerability," and "consequence" is essential to any discussion of risk assessment methods. Defining these four critical terms is not easy, nor has there been agreement within academic, law enforcement, or military circles as to their meaning. Adding to this difficulty is the issue of "real risk" versus "perceived risk" (public perception is an additional reality that must be respected). Assessing risk is a process that involves as much art as it does science. The art element is driven by the high degree of uncertainty created by questions such as the following: What is acceptable risk? What is the enemy's true capability? What is the enemy's intent? In simple terms, the terrorists hold every one of the controlling factors in the successful accomplishment of an attack. They can pick the time, place, location, and method of the attack. Terrorists also have the ability to call off or delay an attack if security forces are in position to disrupt their attack knowing that these forces cannot remain at high alert indefinitely.

The analysis of risk informs several critical decisions: determining how limited resources and capabilities will be deployed; identifying what security actions offer the greatest risk reduction for the least investment; and what new technologies or capabilities offer the best investment for limited funds. The same discussion occurs as mitigation strategies are developed, analyzed, and selected. In selecting a specific course of action, risk models help quantify potential results. What also must be evaluated are unintended consequences of the action.

The RAND Corporation's team of Dr. Henry Willis, Dr. Andrew Morral, Terrence Kelly, and Jamison Jo Medby presented one of the definitive papers regarding the "risk" equation at the Society for Risk Analysis' Annual Meeting in 2004. Dr. Henry Willis, who is an Associate Policy Research at RAND's Pittsburgh's office, expanded on this equation on February 7, 2007 in testimony before the Committee on Appropriations Subcommittee on Homeland Security, United States House of Representatives. Willis noted at the very beginning of his testimony that, "There is no single correct method for measuring terrorism risk ... Terrorism risk is a function of three factors: a credible *threat* of attack on a *vulnerable* target that would result in unwanted *consequences*. Risk only exists if terrorists want to launch an attack, if they have the capability to do so successfully in a way that avoids security and compromises the target, and if the attack

results in casualties, economic loss, or another form of unwanted consequences" [6] (*see* Risk Analysis Framework for Counterterrorism).

The US military uses very specific processes to evaluate potential targets that can be invaluable to an overall discussion of risk. "Target analysis is the detailed examination of potential targets to determine their military importance, priority of attack, scale of effort, and the lethal or nonlethal weapons required to attain a specified effect. It is a systematic approach to establishing the adversary vulnerabilities and weaknesses to be exploited. This is accomplished through the methodical examination of all information pertaining to a given target" [7, p. A-1]. This target analysis examines vulnerability to attack and what the overall effect would be if an attack occurred.

To conduct this analysis, US Special Forces use a method called CARVER. The name is an acronym for the variables the method uses for evaluation. The use of this method is applicable to infrastructure evaluation as part of an overall approach to risk evaluation. A numerical value/rating scheme is applied to each of the following CARVER variables.

C = Criticality. "Criticality or target value is the primary consideration in targeting. Criticality is related to how much a target's destruction, denial, disruption, and damage will impair the adversary's political, economic, or military operations, or how much a target component will disrupt the function of a target complex" [7, p. A-3].

A = Accessibility. "In order to damage, destroy, disrupt, deny or collect data on a target, Special Operations Forces (SOF) must be able to reach it with the necessary equipment, either physically or via indirect means" [7, p. A-4].

R = Recuperability. "In the case of Direct Action (DA) missions, it is important to estimate how long it will take the adversary to repair, replace, or bypass the damage inflicted on a target. Primary considerations are spare parts availability and the ability to reroute production" [7, p. A-4].

V = Vulnerability. "A target is vulnerable if SOF has the means and expertise to attack it. At the strategic level, a much broader range of resources and technology is available to conduct the target attack" [7, p. A-4].

E = Effect. "The target should be attacked only if the desired military effects can be achieved. These effects may be of a military, political, economic, informational, or psychological nature" [7, p. A-4].

R = Recognizability. "The target must be identifiable under various weather, light, and seasonal conditions without being confused with other targets or components" [7, p. A-4].

For each CARVER element a criterion provides a value that is included in the overall assessment of either the ease or difficulty in attacking a particular target and achieving the desired effect. For example, under "Critically" a score of "5" might equal "significant damage to overall mission capability." However, an assigned score of "1" could mean "loss would not effect overall mission performance." [Note: These types of notional factors are applied across all six criteria listed for CARVER]

But CARVER is only a process, or some would say a "tool," in an overall evaluation regime. An even more critical factor in any maritime risk assessment process is the *capability* of a terrorist group to use and exploit the maritime environment for an attack. This is an important component discussion above the standard risk = threat × vulnerability × assessment. It is often overlooked because it is extremely difficulty to judge. But when you think about it, is it not the most basic question—what are terrorist groups, both national and international truly capable of? (*see* Vulnerability Assessment).

## 2.2 Assessing Maritime Risk

The capability and intent for some terrorist groups to exploit the maritime environment has been well documented. Certainly the Tamil Tigers have conducted their bold maritime attacks, including use of the underwater environment, and tactical acumen rivaling many of the world's military and security forces. What is debated in both government and academic circles is the ability of a terrorist group to obtain a chemical, biological, radiological, or nuclear (CBRN) weapon of mass destruction (WMD). What is truly available on the black market? Do terrorists groups have the technical expertise to assemble, deploy, and trigger a WMD inside a port? These are the true questions of risk that should be part of any overall discussion.

So what has been and is being done to assess maritime risk due to terrorism?

Primary responsibility for conducting these assessments falls on the US Coast Guard as the Department of Homeland Security's Executive Agent for Maritime Security [1, p. 23] and the Federal Maritime Security Coordinator in the port [8, p. 7]. Before entering into a detailed discussion of the Coast Guard's use of risk assessment methods for analyzing port security requirements, an understanding of the service's historic role in securing US ports and employing risk management is necessary.

At the start of World War I the Coast Guard was assigned the responsibility for the security of US ports under the Magnuson Act of 1917. For both World Wars and the Korean War, the service expanded its numbers significantly to meet the tremendous demands of securing the nation's 12,400 miles of maritime border and hundreds of ports. During World War II, the Coast Guard grew to more than 240,000 active duty personnel with more than 53,000 assigned to port security duties [9] (the current strength of the Coast Guard is just over 40,000 active duty personnel) [10].

After the Korean War, the port security threat to the United States steadily diminished and the port security program essentially became a contingency mission assigned to the Coast Guard Reserve. The perception was that port security operations would only be needed in support of the Department of Defense. Planning centered around two functions: securing a limited number of domestic ports conducting military out load operations (ports of embarkation) and providing port security at foreign ports to support military offload operations (ports of debarkation). By September 11, 2001 the Coast Guard had been reduced to a force of just over 35,000 active duty personnel who had little to no involvement in port security.

During the 18 months preceding the September 11th attacks the Coast Guard had gone on record stating that it lacked the resources necessary to meet all of its missions; a resource demand that essentially did not include port security [11, p. 11]. Following the attacks, port security suddenly became a primary mission of the active duty force. This resurgence of port security as a primary mission significantly exacerbated the already sizeable resource shortfall within the Coast Guard.

On September 11, 2001 the port security task facing Coast Guard planners and operators was formidable. As previously discussed, the vastness, complexity, and economic importance of the US Maritime Domain and the Maritime Transportation System are truly immense. Protecting everything was clearly not an option. In addition, the nearly 12,000,000 recreational boaters operating on US waters created ideal camouflage for terrorists seeking to disguise preparations for small boat attacks.

To add to the maritime security difficulty, industry had shifted to a "just-in-time" inventory system, maintaining minimum inventory and counting on being resupplied just in time with the critical supplies and material needed to continue operations. As

much of these materials are transported through the Maritime Transportation System, any inordinate delay in the flow of commerce due to security measures would have a telling effect on the economy. It was clear to Coast Guard planners that, barring a significant force increase to the levels of World War II, maritime security operations would have to be focused, efficient, and effective in order to maximize the use of existing security forces while minimizing the impact on legitimate users; their solution, risk management. The greatest risks in the maritime relative to security needed to be identified and effective risk mitigation measures implemented.

Fortunately, the Coast Guard had been using risk management principles for almost a decade prior to 2001. To inform its Marine Safety and Environmental Protection programs, the service had employed Risk-Based Decision Making [12, p. 4-1] and was using Operational Risk Management [13, p. 1] to assist field commanders in assessing the risks associated with a specific action or activity. These two initiatives created a risk management culture within the Coast Guard that significantly facilitated the service's adoption of risk-based operations to meet the new demands of maritime security following the 2001 attacks.

The Operational Risk Management model follows a seven-step task-oriented process: identify mission tasks, identify hazards, assess risks, identify options, evaluate risk versus gain, execute decision, and monitor situation. This model calculated risk using the equation

$$\text{Risk} = \text{Severity} \times \text{Probability} \times \text{Exposure}$$

Severity is the potential consequences in terms of degree of damage, injury, or mission impact. Probability is the likelihood of the potential consequence. Exposure is the amount of time, number of occurrences, number of people, and/or equipment involved in the task [13, p. 4]. Coast Guard commanders were taught to assess risk associated with specific actions or missions using this Operational Risk Management model (*see* Terrorism Risk: Characteristics and Features).

The service's Risk-Based Decision Making model contains five major components: decision structure, risk assessment, risk management, impact assessment, and risk communication. Decision structure includes the concept of obtaining input from external stakeholders in the risk analysis process to determine available options and influencing factors. Risk assessment uses the equation:

$$\text{Risk} = \text{Probability} \times \text{Consequence}$$

The assessment also looks at factors such as: reasons for the assessment; type of results needed; available resources; complexity of the assessment; type of activity or system analyzed; and type of incidents targeted. Risk management recognizes that the benefit of action to manage or reduce risk must outweigh the cost, be acceptable to other stakeholders, and not cause other significant risk. Impact assessment requires tracking of the risk mitigation actions taken to ensure that the desired benefits are realized. Risk communications incorporates two-way communication with stakeholders to identify key issues, provide information, and obtain consensus [12, p. 4–5].

## 3 POST-9/11 MARITIME RISK ASSESSMENT

With this background in risk management, Coast Guard leadership and planners readily accepted risk-based decision making as the means to solve the maritime security challenge. Shortly after the 2001 attacks the Coast Guard developed its first security risk assessment tool called the *Port Security Risk Assessment Tool*s (PSRAT) [14, p. 16]. This tool used the risk equation:

$$\text{Risk} = \text{Threat} \times \text{Consequence} \times \text{Vulnerability}$$

The tool was provided to Coast Guard Captains of the Port to assess maritime risk in their areas of responsibility. Individual facilities, infrastructure, and waterways seen as potential terrorist targets were assessed for risk using the tool. The tool generated a dimensionless Risk Index Number (RIN) for the target based upon the assessed values for threat, consequence, and vulnerability; the higher the RIN, the greater the risk.

The RIN scores for the various facilities and other infrastructure were compiled and ranked at the national level. This allowed the service to develop its first list of nationally critical maritime infrastructure based upon risk. Coast Guard security forces and those of other agencies then focused their security operations in support of these critical infrastructures.

While PSRAT was a good start, it had shortcomings. The level of effort put into the analysis varied depending upon staff availability and workload at each port. As a result, consistency in the analysis between ports was not ideal. In addition, the vulnerability and consequence analysis was conducted primarily by law enforcement personnel, not scientist and engineers, creating inaccuracies. A significant weakness was poor linkage between attack methods and resulting consequences. A second run of the PSRAT model was conducted with modified guidelines, improvements in the results were noted, but significant inconsistencies were still apparent.

Coast Guard planners gathered to improve their port security risk assessment and developed the Maritime Security Risk Analysis Model (MSRAM) in 2006 [14, p. 16]. Although based upon the same risk equation, this tool offered improved threat information including potential damage information, target classification, more rigorous training, and data treatment. Still, the 2006 MSRAM analysis produced results with some clear errors. The problems were addressed and a second MSRAM analysis was conducted in 2007 with much improved result [14, p. 16].

In MSRAM, threat is treated as the probability a certain type of terrorist attacks, such as explosive-laden small boats, standoff attacks, sabotage, and so on might occur [14, p. 19]. This threat analysis includes concepts, such as terrorist intent, terrorist capability, and timeframe in which terrorists will acquire the capability. In addition to terrorist competency and possession of necessary material for a given attack method, the assessment of capability also considers the ability of the terrorists to produce that capability in a given geographic region. For example, terrorists have proven their ability to conduct suicide attacks with explosive-laden small boats in the Middle East; but do they have the infrastructure in place to conduct such attacks in the United States? (*see* Risk-Based Prioritization).

The consequence assessment looks at both primary consequences and secondary economic impacts that might result from a selected attack method. Primary consequences include factors such as: death, injury, primary economic impact, national security impacts, symbolic effect, and environmental impact that would probably result from a successful attack of a given type. Secondary economic impacts consider factors such as: recoverability, redundancy, and secondary economic impacts [14, p.19].

Primary economic impacts include direct factors such as the value of the infrastructure that would be lost in the attack. Secondary economic impacts consider factors such as the monetary impact through lost revenue if the attacked target remains inoperable. Recoverability is an assessment of how quickly an attacked function can be restored at the site of the attack. Redundancy looks at how many of the same type facility or infrastructure exist [14]. For example, the consequences of losing the only bridge in a region may be far more significant that a region with several bridges spanning the same waterway.

A significant difficulty in calculating consequence stems from equating the consequence values associated with different factors. Equating economic value or national security value to lives lost is not an exact science, but requires objective analysis and stakeholder consensus. Overtime, the Coast Guard worked with a variety of other agencies and entities to develop these equivalencies.

Vulnerability is the likelihood that a selected attack method will succeed in producing the consequences feared. Vulnerability considers factors, such as achievability, security systems in place, and target hardness. Achievability considers attack aspects such as whether the depth of water surrounding a piece of infrastructure would support a small boat attack. Security systems include the security capabilities at the selected facility as well as the security capabilities of local law enforcement and the Coast Guard. Target hardness evaluates the ability of physical barriers, such as wall material and thickness, to resist a given attack type.

### 3.1 Maritime Risk Assessment Challenges

In calculating risk, it is critical that the consequence and vulnerability values used are those associated with the selected attack method. Consider an explosive-laden small boat attack on a waterfront chemical facility. The degree of physical destruction, subsequent chemical release, and resulting death and injury must be those resulting realistically from the amount of explosive a small boat can carry and the proximity to the facility a small boat can achieve; not necessarily a worse case release.

The accuracy of the risk assessment is wholly dependent upon the accuracy of the inputs to the tool. Accurately establishing the values for each of the risk factors requires expert and deliberate analysis. For the explosive-laden small boat attack on a waterfront chemical facility example: the blast effect of various explosive loads must be calculated, the ability of the facility's wall to withstand the blast also must be calculated, and the effect of the blast energy that reaches the chemical needs to be understood; Will the chemical ignite? If so, with what thermal or blast effect? Will the chemical be released in a toxic plume? If so, in what concentration, for what duration and distance? Answers to these questions require in-depth analysis by scientists and engineers

(*see* High Consequence Threats: Chemical and High Consequence Threats: High-Grade Explosives).

### 3.2 Application of Maritime Risk Assessment

As a result of the risk analysis supported by MSRAM, the national maritime critical infrastructure list was significantly refined. This in turn allowed port-level security forces to prioritize their security operations with increased confidence. Although inconsistencies and need for improvements were still apparent, the Coast Guard has developed enough confidence in the tool to require its use in developing Area Maritime Security Plans as required in the Maritime Transportation Security Act of 2002 (MTSA) [15, p. 36].

### 3.3 Opportunities for Improving Maritime Risk Assessment

Perhaps the most significant opportunity for improvement in the Coast Guard's port security risk analysis does not reside with the risk analysis tool, but with the input values. As noted earlier, the need for accurate inputs is critical; however, the inputs for vulnerability and associated consequences continue to be provided by port-level operators with little expert analysis by scientist and engineers. This more in-depth expertise is needed to accurately calculate risk. Given the size and complexity of the US Maritime Domain, and the limited size of maritime security forces and the national budget, an accurate risk assessments is a must to ensure the most effective and efficient use of these resources.

Identification of effective risk mitigation activities is another use for the MSRAM. Once the areas of greatest security risk are identified, the obvious next step is to determine how to best reduce vulnerability. Although it is possible to reduce potential consequences (move the facility away from populated areas, dilute the chemical concentration, institute a robust response organization, etc.), the current focus is to reduce the vulnerability. Ideally, port planners should be able to use the risk assessment tool to "plug in" various security options and measure the risk reduction gained to determine the best returns on investment.

Unfortunately, in its present form, the MSRAM tool is too cumbersome and lacks sufficient sensitivity for effective use as a risk mitigation assessment tool. As currently configured, the ranges for consequence values are essentially orders of magnitude [14], whereas, in many cases, the ability of available security forces to mitigate potential consequence is far smaller. Therefore, the risk changes created by different force employment operations cannot be discerned with the tool.

## 4 CONCLUSION

Risk assessment is not a one time effort, rather it is an ongoing process that identifies initial risk and adjusts risk as new threat information is received, risk is reduced through security activities, infrastructure is added or removed, and new technologies emerge. The ever-changing nature of risk demands that risk assessment be dynamic and responsive.

For example, in the absence of intelligence of specific attack planning for a port, we must use default analysis of previous targeting choices and the stated strategic objectives of our enemy to make our best guess at the "threat" value for our risk equation. The risk mitigation activities developed with the resultant risk assessment forms the core of our steady state maritime security strategy.

But what happens when attack planning intelligence is received for a port? The natural tendency is to put as many prevention resources around the intended target as possible to deter or defend against the specified threat. This would be a good response if there were adequate strategic law enforcement reserves to do targeted point defense while regular forces continue steady state protection, but unfortunately this is rarely the case. As a result, more risk is assumed throughout the system as we rush to protect a specific target (*see* Emerging Terrorist Threats).

If time is available, it would be useful to enter specified threat information into the risk assessment tool to reassess how the entire port security system might be impacted. This analysis may show that it is prudent to focus all protection resources against the threat, but it may also show that it might be worth absorbing a lower consequence attack than dropping our guard around higher consequence infrastructure. The thought of our enemy using operational deception to draw us away from high value targets must never be ignored. Whatever risk mitigation strategy is selected, the risk tool should again be employed to measure the expected effects on risk throughout the port security system.

A fundamental premise of port security is that we will never be able to eliminate risk. The adaptive threats posed by our enemies and limited resources available to counter those threats requires that we work toward reducing, not eliminating the threat. The risk assessment tool is critical in helping to assess where we will achieve the greatest risk "buy down" through applied security activities. While we can use the risk assessment tool to inform the budget process for increasing security capabilities and capacities were the investment is warranted, we cannot and should not try to protect everything with our limited resources. If we do, we expose the highest risk infrastructure to greater risk while spreading precious resources thin in the process of protecting lower risk areas. Deciding where to focus security efforts is one of the most difficult problems faced by a Captain of the Port. MSRAM is one of the few tools available to the operational commander to help make those decisions. It is therefore critical that MSRAM be a robust, agile tool that not only assesses risk, but also assesses the effects of security measures. The current tool is capable in the former task, but needs more work on the latter (*see* Risk-Based Prioritization).

It is important that local operational commanders have maneuvering room to develop locally focused security plans because all ports have fundamental differences. As noted previously, the MTSA designated the Coast Guard Captains of the Port as the Federal Maritime Security Coordinator for the ports in their areas of responsibility. They are supported by an Area Maritime Security Committee for each port that includes representatives from interested federal, state, and local governments as well as the private sector. Each Area Maritime Security Committee has helped to develop a comprehensive Area Maritime Security Plan tailored to the security requirements of the individual port. MSRAM assessment plays a role in developing this Plan. The Plan is exercised at least once a year and modified as needed. The Plan is required to be reviewed and reapproved by the Coast Guard once every five years.

Through the Area Maritime Security Committee and resultant partnerships, the Coast Guard Captain of the Port seeks as many resources as possible to bolster port security.

Maritime resources from State and local law enforcement agencies play a large role in supplementing Coast Guard resources. Nationally, about 25% of the port security effort comes from non-Coast Guard law enforcement agencies [16]. Some state and city governments have passed local laws making violation of federal security zones a state/local offense as well, thus allowing nonfederal law enforcement officials to enforce federally designated security zones. This not only improves patrolling but also facilitates prosecution because violators can be held accountable in federal, state, or local courts.

### 4.1 Consequence Management

Although this article is about port facility protection and prevention, a brief discussion of consequence management is prudent. Much of the Coast Guard's counterterrorism efforts to date have focused on protection and prevention. More effort is now going into consequence management and the reason is clear from the risk equation. Our enemies wish to attack us in order to achieve a certain serious consequence. If we can reduce the consequences of an attack, we reduce the effects our enemy can achieve. By building a robust consequence mitigation capability, we get into our enemy's planning cycle and can potentially prevent an attack by showing the enemy that his desired effects will not be achieved. If we show the enemy that even a tactically successful attack on a port will only have limited consequences, it might deter our enemy from attacking. Thus, post-attack consequence mitigation planning and capacity building can have a powerful deterrent effect and must be a key part of our overall counterterrorism strategy. MSRAM and future risk assessment tools must include the capability to assess the power of consequence mitigation to help Captains of the Port plan consequence management (*see* High Consequence Threats: Chemical).

### 4.2 Summation

The challenges faced by those responsible for US port security are daunting and the ability to accurately assess risk at the national, regional, and port levels are critical to deterring and preventing attacks as well as mitigating the consequences of an attack. Current assessment tools are well ahead of where we started, but much more must be done to improve their scope, make them more agile, enhance their display, and make them available to the people who need to know.

## REFERENCES

1. U.S. President (2005). *National Strategy for Maritime Security*. White House, Washington, DC, pp. 1–27.
2. Allen, T. W. (2008). *Statement of Admiral Thad W. Allen Commandant on the Fiscal Year 2009 President's Budget Before the Committee on Appropriations Subcommittee on Homeland Security U.S. House of Representatives*, pp. 1–18.
3. U.S. Coast Guard (2007). *The U.S. Coast Guard Strategy for Maritime Safety, Security and Stewardship*. Headquarters U.S. Coast Guard, Washington, DC, p. 34.
4. Department of Homeland Security (2008). *Small Vessel Security Strategy*. SECDHS, Washington, DC, pp. 1–31.
5. U.S. President (2007). *National Security Strategy for Homeland Security*. White House, Washington, DC, pp. 1–53.

6. Willis H. RAND Corporation (2007). *Testimony before the Committee on Appropriations Subcommittee on Homeland Security, United States House of Representatives*, pp. 1–7.
7. U.S. Office of the Chairman of the Joint Chiefs of Staff (2003). *Joint Tactics, Techniques and Procedures for Special Operations Targeting and Mission Planning*. CJCS, Joint Publication (JP), Washington, DC, pp. I-1–IV-18.
8. U.S. Congress (2002). *An Act to Amend the Merchant Marine Act, 1936, to Establish a Program to Ensure Greater Security for United States Seaports, and for Other Purposes: Maritime Transportation Security Act of 2002*. 107th Congress, 2002, Public Law 107–295, pp. 1–71.
9. Doane, C., DiRenzo J. III (2004). The history of port security: A coast guard mission since 1917. *Maritime Reporter and Engineering News* 8, 28–47.
10. U.S. Coast Guard Fact Sheet (2008). Available from http://www.uscg.mil/top/xabout/
11. Loy, J. M. (2000). *Statement of Admiral James M. Loy before the House of Representatives, Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure*, U.S. Congress, Washington, DC, p. 8–32. Available from http://commdocs.house.gov/committees/trans/hpw106-95.000/hpw106-95_1.HTM.
12. U.S. Coast Guard. Office of the Commandant (2004). *Contingency Preparedness Planning Manual, Volume I: Planning Doctrine and Policy*, COMDTINST M3010.11C, Headquarters U.S. Coast Guard, Washington, DC, pp. 1-1–10-2.
13. U.S. Coast Guard. Office of the Commandant (1999). *Operational Risk Management*, COMDTINST 3500.3, Headquarters U.S. Coast Guard, Washington, DC, pp. 1–13. Available from http://www.uscg.mil/directives/ci/3000-3999/CI_3500_3.pdf.
14. Downs, B. (2007). Balancing resources to risk. *Presentation to SCOTS/NCHRP 20–59*, August 2007, Irvine, CA, pp. 1–57. Available from www.transportation.org/sites/security/docs/Downs—USCG%20Balancing%20Resources%20to%20Risk.pdf.
15. General Accounting Office (2007). *Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery*, GAO Report GAO-07-412, Washington, DC, pp. 1–53. Available from www.gao.gov/new.items/d07412.pdf
16. U.S. Coast Guard Atlantic Area (2008). *Operation Neptune Shield Scorecard for June 2008 (Security Sensitive Information).*

## FURTHER READING

Daniels, W. and DiRenzo, J. III (2005). *Maritime Anti-Terrorism at the Crossroads of National Security and Homeland Defense, National Defense*, http://nationaldefense.ndia.org/issues/2005/feb/Maritime_Anti-Terrorism.htm.

DiRenzo, J. IIII and Doane, C. (2007). *Small Vessel Security Summit Initiates Constructive Dialogue, Maritime and Border Security News*, http://www.imakenews.com/ejkrause/e_article000864979.cfm?x=b11,0,w.

Linacre, N. A., Koo, B., Rosegrant, M. W., Msangi, S., Falck-Zepeda, J., Gaskell, J., Komen, C., John, M. J., and Birner, R. (2005). *Security Analysis for Agroterrorism: Applying the Threat, Vulnerability, Consequence Framework to Developing Countries*.

Parfomak, P. W. and Frittelli, J. (2007). *Maritime Security: Potential Terrorist Attacks and Protection Priorities.* Congressional Research Service, Washington, DC.

Willis, H. H., Morrall, A. R., Kelly, T. K., and Medbey, J. J. (2004). Risk-based allocation of counterterrorism resources. *RAND. Presented at the Society for Risk Analysis Annual Meeting Palm Springs.* Palm Springs, CA.

Willis, H. H., Morrall, A. R., Kelly, T. K., and Medbey, J. J. (2005). *Estimating Terrorism Risk.* RAND, Santa Monica, CA.

# DEFENDING AGAINST MALEVOLENT INSIDERS USING ACCESS CONTROL

DALE W. MURRAY

*DoD Security System Analysis Department, Sandia National Laboratories, Albuquerque, New Mexico*

BETTY E. BIRINGER

*Security Risk Assessment Department, Sandia National Laboratories, Albuquerque, New Mexico*

## 1 INTRODUCTION

The greatest challenge to any security system is protecting against the malevolent insider because the he or she may be authorized to own 'the keys to the kingdom'. An insider is defined as anyone with knowledge of operations, sensitive information, and/or security systems and who has unescorted access to the facilities or critical assets. A malevolent insider is an insider who has decided to become an adversary. Protecting against the malevolent insider threat requires an integrated security system that minimizes the potential for hiring an adversary and deters the on-staff employee from becoming an adversary. The security system must integrate such protection functions as personnel security, physical security, cyber security, and operations security to *make it easy for the insider to do the right thing and very difficult for the insider to do the wrong thing*. If the insider decides to do the wrong thing, the security system should be able to protect against the adversarial acts or, if the malevolent insider is able to overcome the security system, the system should photograph, record, or otherwise document the event in order to provide evidence for prosecution. The physical security system prevents the malevolent insider from causing an undesired event by detecting the action early enough and delaying the insider adversary long enough so that an appropriate response can interrupt the scenario before the undesired event is caused. Access control is an important element of defending against the malevolent insider because it supports the detection, delay, and response functions of the physical security system. The current state of access control technology, as applied to the insider adversary, focuses on identity verification, contraband detection, and tamper indication.

## 2 PROTECTION AGAINST THE MALEVOLENT INSIDER

The determination of how much security is enough cannot be made without some judgment about the level, access, and sophistication of the threat that the system must protect against. A description of the insider threat spectrum must be completed in order to design or assess the effectiveness of a security system. An insider is defined as anyone with knowledge of operations, sensitive information, and/or security systems who

has unescorted access to the facility or security interests. The passive insider adversary commits no overt acts; he or she only provides information. The active insider adversary may be nonviolent, unwilling to use force against personnel, or he or she may be violent, willing to provide active, violent participation including force against personnel. The active, violent insider is a very difficult adversary to protect against. More than one insider adversary is possible but emphasis is placed on addressing the single insider adversary, the most probable insider threat. Another underlying assumption is that the nonviolent insider will give up if detected.

### 2.1 Insider Threat Analysis

The motivations for the insider adversary can be the same as those for the outsider adversary. Motivation is an important indicator for both the level of malevolence and the likelihood of insider attack. Motivations might be ideological (the insider holds a fanatical conviction), financial (the insider wants or needs money), vengeful (the insider is a disgruntled employee, contractor, or customer), egotistical ("Look what I can do"), psychotic (the insider is mentally unstable but capable), voluntary (the insider is a volunteer), or coercive (the insider or the insider's family is threatened).

Insider adversaries have advantageous characteristics that distinguish them from other adversaries:

- Operational/system knowledge that can be used to advantage
- Authorized access to the facility, information system, sensitive information, and security systems, without raising the suspicion of others
  - Can conduct tests and rehearsals
  - Can test the system with normal "mistakes"
- Opportunity to choose the best time to commit an act or extend acts over a long period of time
- Capability to use tools available at work location
- Recruitment/collusion with others, either insiders or outsiders [1]

All employment positions at a facility should be included in the insider threat analysis. Any employee may pose a potential insider threat, even trusted managers and security personnel. Insider positions at a typical building might include managers, staff, information system administrators, security personnel, administrative staff, contractors, custodians, maintenance personnel, vendors, and past employees. Visitors hold some, but not all, of the advantages of an insider.

A higher level of protection may be required for high risk positions. High risk positions are those that afford employees access to the most sensitive information or critical assets as a part of the normal job assignment. The insider threat analysis describes general personnel job categories in terms of *knowledge, access*, and *authority* related to each of the undesired events or related critical assets. Efforts should be made to assure that all appropriate personnel assignments are included. The purposes are to identify the job categories that could provide the greatest advantage for the insider adversary to cause the undesired events, and to understand the potential capabilities of an insider adversary. The types of insider knowledge that provide a significant advantage to the insider adversary include knowledge of security/control features, work schedules and assignments, locations

and characteristics of critical assets, specific details of facility operations, and known weaknesses and gaps in protection. Insider access that can be used to cause an undesired event includes the usual authorized work access, special temporary access to other areas, and the access to other employees as a source of expanded information. Insider authority that the insider adversary can exploit is described as management authority over others, personal influence over others, the authority to do assigned tasks, and the ability to get temporary authority to do any task.

### 2.2 Role of Access Control in Protecting against the Insider Threat

Protection features from personnel security, physical security, cyber security, and operations security must be integrated to mitigate the insider threat. Usually, these protection features function independently and are not integrated towards a common objective, but not a single one of these functions, acting alone, can answer the insider threat. The physical security features must function together to detect, delay, and appropriately respond to the insider threat to prevent the undesired event.

Access control plays a prominent role in the physical protection system because it supports all three functions of detection, delay, and response. Access control can detect insider noncompliance with procedures, insider attempts to access areas for which he or she is not authorized, and insider attempts to enter an area with contraband (weapons, explosives, or any restricted item) on his or her person, or in packages. Access control can delay the insider adversary by denying access to unauthorized areas or locking doors to areas he or she is not authorized to enter, thus forcing the insider either to switch to an overt method of attack or be deterred from becoming an adversary.

An important objective for the physical protection system is to minimize the opportunity for malevolent insider acts. A common method of achieving this objective is to compartmentalize the facility. Compartmentalization can be achieved by limiting access to sensitive information or actual assets to only those needing it for job duties, further restricting access to the assets that could result in a high consequence undesired event, enforcing a multiperson presence in critical areas, and monitoring activities to detect potential malevolence and identify who is responsible for the act. Entry/exit control can be used to enforce compartmentalization and access. Entry control enforces authorization checks with a picture-badge inspection, electronic credential, personal identification number (PIN), or a biometric check, such as fingerprints, eye-retinal pattern, and the like. Entry control schemes might include contraband detection to prevent the introduction of weapons, explosives, or other tools that could be used in a malevolent attack. Exit control is used to detect the unauthorized removal of high value assets.

## 3 ACCESS CONTROL TECHNOLOGY

Access control is the function performed by the security system to allow authorized individuals into a secured area while preventing entry by unauthorized individuals. Other functions that are performed by an access control system are enforcing a two- (or more) person rule, antipassback (*passback* refers to entry credentials being passed back by the first user to a second person for use), contraband detection, and tamper indication. Some of these functions are related directly to addressing the outsider while some address the

insider adversary. Before discussing the way in which the access control points address insider issues, some general background on access control is required.

### 3.1 Balancing Intrusion Detection and Access Control Portals

Perimeter and building security can be extremely effective at detecting persons attempting to penetrate a security area through the detection layers, but authorized persons and materials must still have access to the area. Thus it is very important to have portals in the security area that meet the same level of security as the intrusion detection system. In order to accomplish that, the access control and contraband detection system must be capable of accurately verifying the identity and determining the authorization of persons attempting to enter via the portal. It also has to be able to determine that authorized persons are not carrying materials and objects that are prohibited in the area.

The portal should not be so secure that it greatly exceeds the security of the intrusion detection system. It is a waste of money and resources to create a highly secure portal that can be easily bypassed by entering covertly through the intrusion detection layers. In addition to wasting money and resources, very high security portals are more time-consuming to pass through and have a higher likelihood of falsely rejecting an authorized individual than lower security portals. Depending on the application and the need for very high security, additional time to enter and a higher probability of falsely rejecting authorized persons may be acceptable trade-offs.

### 3.2 Verifying Identity

In the process of access control it is important to verify the identity of an individual seeking access before granting entry into the security area. There are three criteria used for identity verification. These criteria are not limited to electronic identity verification; they are the means we all use to recognize each other and have been used throughout human history so it is not surprising that they have been carried over into electronic security systems. These criteria are easily remembered as something you know, something you have, or something you are.

The most common means of verifying identity in an electronic access control system based on “something you know” is the PIN. At access control portals for physical access to a security area, it is usually difficult to provide a full alphanumeric keyboard; typical access control systems use keypads for numeric entry of PINs. But, PINs used alone to verify identity does not provide a high level of security since there is often nothing to prevent an adversary from guessing PINs. If an adversary is allowed an unlimited number of guesses, it is simply a matter of time until an enrolled PIN is guessed. One means of reducing the chance of success at guessing a PIN is to make the number of possible combinations greatly exceed the number of PINs actually enrolled and used. For instance, a four-digit PIN allows only 10,000 unique combinations. If there are 1000 PINs enrolled, an adversary has a 1-in-10 chance of guessing correctly with each attempt. By simply increasing the number of digits in the PINs to five, there will be 100,000 possible combinations, thereby reducing the chance of correctly guessing on a single try to 1 in 100.

There are a number of examples of “something you have” used for identity verification. Keys and credentials are the most frequently used objects for gaining access into secured areas and systems. In the case of electronic security systems, the coded credential is required. Coded means that there is some way to store information on the

credential—usually a card—that can be easily read by an electronic interface. Coded credentials include bar codes, magnetic strips, proximity badges, and smart cards. As with keys, anyone in possession of the credential can use it to gain entrance to a security area if the credential is the only criterion used by the system. For this reason a coded credential combined with a PIN is considerably more secure. Guessing the correct four-digit PIN for the credential is a 1 in 10,000 probability event; thus the adversary's task when both are used is to gain an individual's coded information and the associated PIN in order to gain entry.

Electronic systems currently in use can make measurements of some physical or behavioral feature of humans—in other words, "something you are". The measurements obtained by the electronic interface are called a *biometric*; the electronics that make and analyze the measurements are called *biometric systems*. Physical features used for identification include (but are certainly not limited to) height, weight, finger print, blood vessel pattern on the retina, iris structure, facial structure, or shape of the hand. Behavioral features include speech patterns (speaker recognition systems can be physical; some work on tones that are determined by dimensions of the vocal tract), signature dynamics, typing dynamics, and walking gait. The security of the biometric technique used to identify the individual depends on how unique the feature is to the individual. Obviously a person's height or weight is not unique to the individual; many people have the same height or weightwhereas the structure of the human eye and fingerprints are unique to the individual.

In very high security applications the highest level of security is provided by combining all three criteria into a single application. Figure 1 shows one such system. This combination of all three identification criteria creates a very high confidence that the identity of the individual can be verified.

### 3.3 Detecting Contraband

Nearly anything that can be used by an adversary to perform a malicious act can be considered to be contraband. Sometimes materials like drugs and alcohol that are simply detrimental to production or safety are considered contraband. Guns and other weapons

**FIGURE 1** A magnetic stripe card reader used in combination with a PIN pad and a hand geometry biometric system.

**FIGURE 2** An automobile door handle being swipe-sampled for explosives detection.

are an obvious class of contraband items. For the protection of sensitive information, cell phones, cameras, and recording devices are often considered contraband. Tools that can be used by an adversary can also be considered contraband. Contraband detection is a clear example of using technology to counter the insider because only persons who are authorized into a security area are screened for contraband. Not all contraband is readily detectable by technology. Examples of contraband that can be detected by modern contraband detection equipment include explosives, metallic objects like tools and weapons, and radiological materials. Systems are in development for the detection of chemical and biological agents. Figure 2 shows a contraband detection tool in use.

### 3.4 Tamper-Indicating Devices

Another means to counter the insider with an access control technology is the use of tamper-indicating devices (TIDs). These devices, commonly known as *seals*, have been used to authenticate documents and other items since the earliest records in history.

The purpose is to indicate unauthorized access by insiders, into secure containers or rooms. The role of a TID is to provide an indication of an unauthorized covert opening of a container, package, door, or other object to which a TID has been affixed. Seals are broadly divided into two categories: passive and active. A passive seal requires an inspection to determine whether an unauthorized entry has occurred between inspection intervals. Passive seals may or may not be operated electronically. Passive seals are further divided into groups based on the way they are applied. These groups are pressure-sensitive (or tape) seals, loop seals, and bolt seals. Pressure-sensitive seals are sheets of tamper-indicating materials with adhesive backing, as shown in Figure 3. These are applied like masking tape to a closed container or room. Any attempt to open the space will cause the seal to tear, stretch, or become detached. Loop seals, as shown in Figure 4, are used in conjunction with a hasp so that the container lid or room door cannot be opened without removing the loop seal. The loop is designed to become damaged and cannot be reapplied after removal. Bolt seals are similar in operation to loop seals in that they are also used in conjunction with a hasp. The bolt is designed to become damaged and is very difficult to reapply after removal. Figure 5 shows examples of bolt seals.

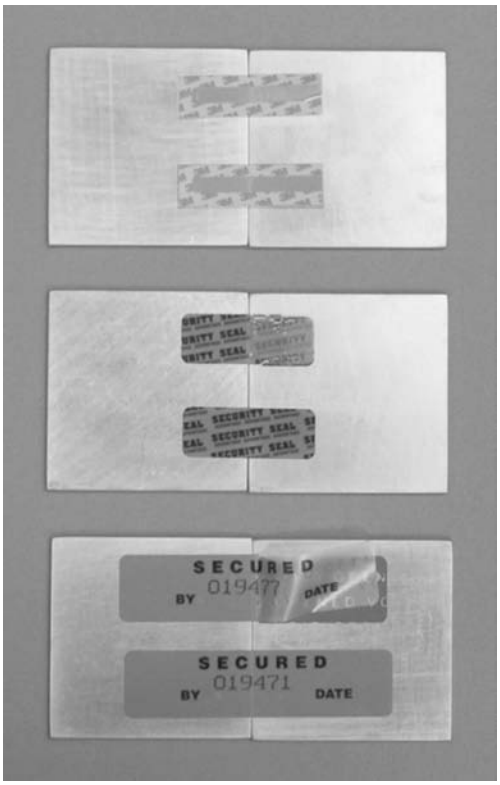



**FIGURE 3** Examples of tape or pressure-sensitive seals.

An active seal is electronically operated and provides a near-real-time indication, or alarm, of an unauthorized access or entry. Most active seals are in development at this time.

## 4 ACCESS CONTROL FEATURES APPLIED AGAINST THE INSIDER THREAT

Because the process of access control is designed to identify individuals for the purpose of separating those authorized to enter (insiders) from those not authorized (outsiders), the process is primarily intended to address the outsider threat. However, there are some features of access control systems that can be used to counter the insider threat.

### 4.1 Entry/Exit Logs

Entry control systems can provide detailed logs of all entries into all security areas. If the system uses exit readers, a complete log of the comings and goings of all personnel is maintained. While this feature cannot prevent an insider from performing a hostile act, it may act as a deterrent. Knowing that the system can identify personnel at the scene of a hostile act may deter insiders who consider the chance of being apprehended too great a risk. Determined insiders who do not fear being caught will not be deterred.

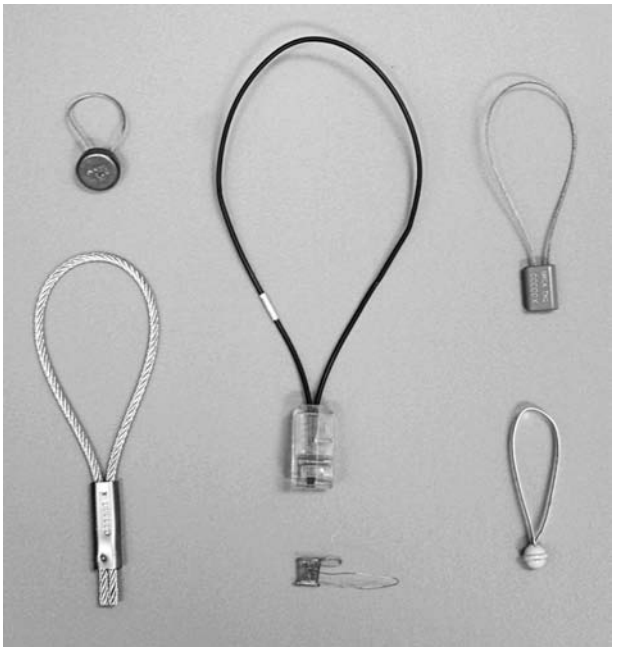


**FIGURE 4** Examples of loop seals.

### 4.2 Antipassback Features

The antipassback feature is used to make the job of an insider acting in collusion with one or more outsiders more difficult. In a collusion scenario an insider may use his or her credential and PIN to allow outsiders to enter a security area. The insider shares the PIN with an outsider and either creates a counterfeit of the coded credential or passes back the real credential to the outsider. The outsider can thus gain entry and join the insider in the secure area to perform a hostile act.

Antipassback is a feature that is often standard on commercial access control systems. This feature prevents the same credential codes and PINs from being used in tandem. This is intended to prevent an insider from assisting an outsider by "passing back" his or her credential to the outsider for use in defeating the access control system and entering the secured area. The insider must first exit the system for the codes and PINs to be valid for another entrance. This can be accomplished through either a timed antipassback feature, which prevents the coded credential and PIN from being used for some programmed period of time after it is used for entry, or an absolute antipassback feature, in which the credential and PIN must be used in an exit reader before being used for another entrance into the area. These antipassback features can be useful for complicating the task of an insider allowing an outsider accomplice into the area, but do not address the insider acting alone.

Another factor in determining the effectiveness of antipassback features is the portal that the access control system is controlling. Simple one-door portals will not be very effective because the insider can just hold the door open while one or more outsiders enter. More effective is a turnstile that is sufficiently small to make the introduction of more that one person at a time difficult and obvious. Electronic sensors developed to detect the entrance of more than one person through a portal at a time show varying degrees

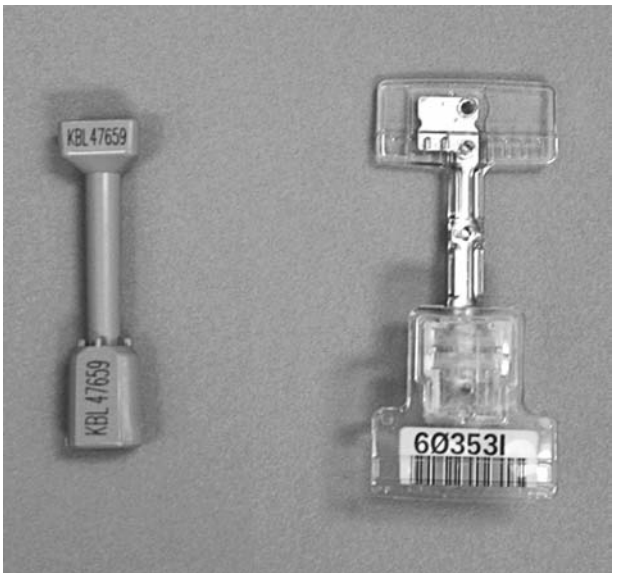



**FIGURE 5** Examples of bolt seals.

of success. The best portal design for use with antipassback features is the two-door portal or mantrap. This system requires the insider to enter the portal and close the door behind him or her, before using the access control system to gain entrance through the second door into the secure area. Electronic sensors can be used to determine that a single individual is inside the portal while it is in use or the portal can be equipped with scales to weigh the contents to ensure that only a single individual is inside.

### 4.3 Two-Person Rule Enforcement

The two-person rule is a security technique used to address the insider acting alone. A two-person rule specifies that no individual is allowed into a security area alone. This technique is typically reserved for the most secure areas. A two-person rule can be implemented either as a procedure or, in an electronic system, the entry control point can be programmed to force the implementation. In the electronic system approach two authorized persons must submit credentials and enter the associated PINs within a short period of time to open the portal. The system must also be equipped with out-bound or exit readers. The system keeps track of how many persons are inside the area and can prevent the exit of a person if that exit violates the two-person rule. Alternatively, the system can be programmed to allow the exit and transmit an alarm to the monitoring station to alert the guard force that a two-person rule violation has occurred. This powerful technique is highly effective at addressing the insider acting alone.

### 4.4 Compartmentalization Feature

Another feature of access control systems that is helpful in countering the malevolent insider is the use of compartmentalization. This feature is simple to implement using electronic access control systems. These systems are fully capable of developing compartments (security areas) within a facility that prevent unauthorized access. Access

control systems in wide use today can control access to interior security areas at the individual cardholder level. The system can be programmed to permit (or deny) access to individuals for specified days of the week and/or a certain time of day at a particular location. Combined with a two-person rule this feature is effective in preventing any single malevolent insider from gaining sufficient information to do significant damage.

## 5 RESEARCH DIRECTIONS

While these features and techniques provide varying degrees of effectiveness, they cannot prevent all malevolent acts by insiders. Neither antipassback nor the two-person rule can guarantee that the insider does not have free movement once inside the area. Antipassback effectiveness can be greatly enhanced by the use of two-door portals capable of detecting the presence of others when the insider is operating the access control system. Advances in sensor technology are required to enable high confidence decisions that a single individual is present inside the portal. One way to increase the effectiveness of the two-person rule would be to develop a system that can actively track all individuals inside a secure area. Alarms could be generated if either there are no longer two persons inside the area (a strict two-person rule violation) or if the personnel are no longer in direct line-of-sight with each other (a violation of the spirit of the two-person rule). Continued development of active seals that can generate an alarm when tampering occurs is recommended to detect the insider who defeats the access control system.

Currently there is little direct funding being invested in the effort to counter the insider with access control. However the considerable investment in improving access control technologies carries a side benefit of helping counter the insider threat. Substantial funding is currently used to develop reliable facial recognition techniques. Facial recognition holds the potential for not requiring cooperation from the person whose face is being captured and analyzed. This ability is dependent on further development and the use of multiple and covert cameras. Without covert coverage the insider adversary can take actions to avoid having his face seen by the cameras. Alternately an alarm could be generated when a sufficiently advanced image analysis detects someone who is actively avoiding having his face imaged. There are systems currently in development for detecting suspicious behavior and these algorithms could be modified for this purpose. Advances in video camera coverage inside a facility include a potential for insider tracking to identify and counter malevolent insiders. Past interior tracking designs relied on radio frequency (RF) tags and had only limited success, due to failed reads and the required cooperation from the potential insiders.

Improved contraband detection is another area where funding is strong. While metal detectors and X-ray package search systems are mature technologies, explosives detection equipment can be improved in such performance areas as sensitivity, reliability, and materials detected. Technologies for the detection of chemicals and biological agents are still in their infancy and will require time and funding to mature.

As with any security system there is no silver bullet that will solve all insider access control problems. Overall system effectiveness will be enhanced by integrating features. Just as using more than one of the three identity verification methods increases effectiveness, the use of access control techniques to counter the insider threat will be most effective when several features are combined. However effective it is, access control is the primary detection system for the malevolent insider threat.

## ACKNOWLEDGMENTS

The submitted manuscript has been authored by a contractor of the US Government under Contract No. DE-AC04-94AL85000. Accordingly, the US Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for US Government purposes. Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the US Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

## REFERENCE

1. James, P. (2006). Chapter 22, Insider Analysis. *The Nineteenth International Training Course for the Physical Protection of Nuclear Facilities and Materials*. Sandia National Laboratories and the International Atomic Energy Agency, Albuquerque, NM.

## FURTHER READING

Turner, J. T., and Gelles, M. G. (2003). Chapter 12, insider threat: risk management consideration. *Threat Assessment, A Risk Management Approach*. Haworth Press, Binghamton, NY.

# LESS-LETHAL PAYLOADS FOR ROBOTIC AND AUTOMATED RESPONSE SYSTEMS

HOBART RAY EVERETT, GREG KOGUT, LARRY DRYMON, BRANDON SIGHTS, AND KELLY GRANT

*Space and Naval Warfare Systems Center, San Diego, California*

## 1 BACKGROUND

The numerous types of less-lethal weapons developed over the past several decades represent a natural application payload for the growing number of unmanned ground vehicles (UGVs) now being employed in military, security, and law-enforcement scenarios. For the most part, however, these UGVs are all teleoperated, and thus suffer from real-time control problems because of communication latencies, poor situational

awareness, and unacceptable burden imposed upon the operator. The incorporation of teleoperated lethal/less-lethal weapons on such systems further exacerbates the situation, resulting in unacceptable performance in all but the most simplistic cases.

In 1996, US Department of Defense Directive 3000.3 defined nonlethal weapons as follows [1]: "Weapons that are explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment." When it later became apparent that many of these so-called nonlethal systems could under certain circumstances prove fatal, the more appropriate terminology "less lethal" was generally adopted instead.

A large number of less-lethal munitions have evolved over the years [2], most of which can generally be classified as either ballistic projectiles or directed energy. The most well known of the ballistic category is the kinetic energy (i.e. blunt force) variety, typical examples being rubber balls, plastic bullets, paint balls, bean bags, sponges, rings, and dowels. Ballistic incapacitants include nets that can be fired at human targets to ensnare and entangle (Fig. 1), and what is known as "sticky foam", extremely tacky and tenacious materials, are also used to entrap or impair. Examples of ballistic area-effect weapons are malodorants such as tear gas (CS) and pepper (OC), as well as flash-bang grenades that emit both a blinding flash (several thousand candela) and deafening sound (170 dB).

The most familiar of the directed-energy category is the taser, a ballistically delivered trailing-wire pair of barbs, which administers an incapacitating electric shock. A more

**FIGURE 1** A would-be intruder and his weapon are temporarily entangled by FMI's Snare Net munition during 1999 tests in Waltham, MA.

recent enhancement of this concept uses a laser-induced plasma channel (LIPC) to eliminate the need for wires, ionizing the air to form a conductive path for the electrical charge. Acoustical directed-energy systems such as the long range acoustic device (LRAD), on the other hand, focus debilitating high-intensity sound waves toward the target. Optical versions, such as strobe lights and laser dazzlers, employ intense beams of visible light to cause temporary blindness and disorientation. The radar-based "pain ray" active denial system similarly projects millimeter-wave radio-frequency (RF) energy, generating an extremely uncomfortable burning sensation on the surface of the skin.

Pursuit of weapon payloads for military UGVs initially involved the adaptation of conventional (i.e. lethal) ballistic munitions in a force-projection role, allowing the remote operator to maintain a safer standoff distance from the enemy. In 1983, for example, the Hawaii Laboratory of the Naval Ocean Systems Center (NOSC) incorporated an M-16 machine gun on a teleoperated dune buggy for the US Marine Corps [3]. The PROWLER (Programmable Robot Observer with Logical Enemy Response), developed in 1983–1985 by Robot Defense Systems (RDS) of Thornton, CO, featured two turret-mounted M-16s on a six-wheeled standard manufacturing all-terrain-vehicle chassis. In 1986, NOSC installed a 0.50-caliber M-2 machine gun on a high mobility multi-wheeled vehicle (HMMWV)-based UGV for the Marines under the Ground/Air TeleRobotic Systems (GATERS) program [4].

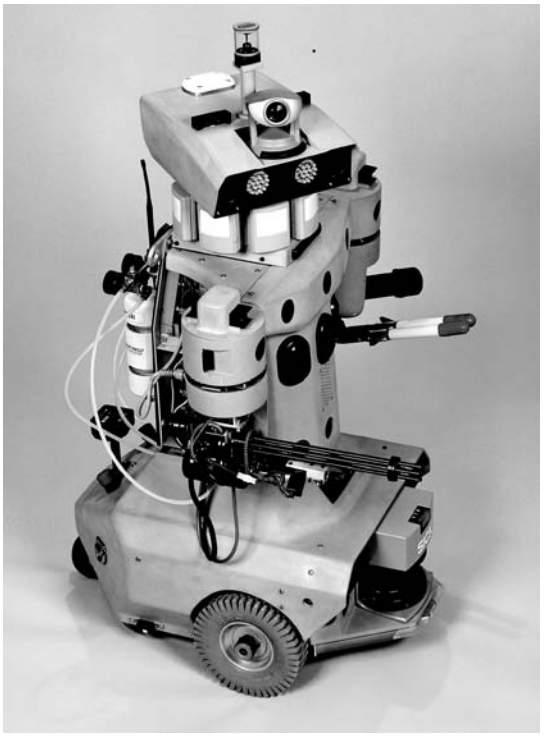


**FIGURE 2** ROBART III is a laboratory surrogate used by the Space and Naval Warfare Systems Center San Diego (formerly NOSC) to develop automated nonlethal response capabilities for security and force-protection missions.

**FIGURE 3** The FMI Snare Net ballistic incapacitant deploys after launch from a less-lethal payload mounted on the company's Lemming man-portable robot in 1999.

When a negative public reaction began to surface in the late 1980s, followed by Congressional direction prohibiting the incorporation of lethal weapons on robots, attention shifted to nonlethal systems. In 1992, for example, the NOSC laboratory robot ROBART III (Fig. 2) featured a pneumatically powered Gatling-style weapon that could fire either tranquilizer darts or rubber bullets [5]. Other less-lethal payloads included 130-dB acoustic disrupters and high-intensity xenon (later light-emittins-diode (LED)) strobes. The principal focus of this research effort was to pursue a more automated force-projection capability, as is further discussed later.

One of the first robotic implementations of a ballistic incapacitant was a net launching payload developed by Foster-Miller, Incorporated (FMI), funded in part under the DARPA Tactical Mobile Robot (TMR) program. Figure 3 illustrates a fully deployed net immediately after being fired from a laser-sighted payload on the front of an FMI Lemming man-portable robot. Interfaced via a 12-V power connection and an RS-232 serial link, the modular launch payload could be adjusted in elevation, with training in azimuth a function of robot heading. The FMI Snare Net round was originally designed for a standard 37-mm grenade launcher, the short-range version of which was effective from 1.5 to 8 m. For longer distances out to 150 m, an optical proximity-fuzed fire-and-forget variant could be used to delay net deployment until within 3 m of the target.

With the proliferation of man-portable UGVs supporting coalition forces in Iraq and Afghanistan, considerable interest has been recently expressed in the addition of nonlethal means for protecting the robot from tampering and sabotage. A more futuristic application scenario currently under consideration involves an autonomous UGV protecting its human partner during proximal human–robot teaming. Under this Warfighter's Associate concept [6], the robot infers to a large degree what its behavior should be by evaluating the perceived threat and observing the actions of its human partner.

## 2 TECHNICAL CHALLENGES

The technical challenges associated with the use of less-lethal weapon payloads on mobile robotic systems can be subdivided into two general categories: (i) controlling the robot and (ii) controlling its weapon.

### 2.1 Robotic Control

From a mobility perspective, the type of control strategy employed on a UGV runs the full spectrum defined by teleoperated at the low end through fully autonomous at the upper extreme. A teleoperated machine of the lowest order has no onboard intelligence and blindly executes the drive and steering commands from a remote operator. A fully autonomous system, on the other hand, keeps track of its position and orientation and typically uses some type of world modeling scheme to represent and avoid perceived objects in its surroundings. The most common form of control employed in robotic systems used by military and law enforcement today is teleoperation, for the simple reason that it is the least complex and therefore the least expensive.

An unfortunate trade-off, however, is that teleoperated systems require continuous high-bandwidth communications links, which not only are difficult to maintain in practice, but also introduce unwanted latencies into the control loop. This situation is further aggravated by other end-to-end systemic delays that can arise from video digitizing, compression, encoding and decoding, as well as operator and vehicle response times [3]. Collectively these various sources can contribute to overall latencies ranging anywhere from several hundred milliseconds to tens of seconds, the effects of which are well documented [7]. Elliott and Eagleson reported " . . . latencies as small as a few hundred milliseconds will prevent the operator from controlling a device in a natural way" [8]. Held et al. noted that feedback delays cause operators to consistently overcompensate in their joystick movements [9], while Day concluded latency typically generates oscillation in the operator's control responses [10].

Another drawback to teleoperated systems is significantly reduced situational awareness on the part of the remote operator, relative to a human performing the same task directly. In a comprehensive study, Drury et al. concluded that robot operators exclusively devote an average of 30% of their time to acquiring situation awareness, sometimes ignoring performance-critical feedback in the process [11]. In the late 1980s, many researchers were attempting to address this problem through a technique known as *remote presence* [3], employing helmet-mounted stereo displays and binaural hearing (Fig. 4). A robotic head–neck assembly in the driver's seat, for example, was slaved to the operator's helmet, allowing him or her to view whatever the robot was seeing from the vehicle perspective [12].

While indeed providing operators with a 3-D sense of immersion in the remote environment, this telepresence approach introduced a new set of problems that often outweighed its advantages. For starters, the use of stereo cameras drove the communication bandwidth requirements even higher than that for monocular vision. Even worse, the previously mentioned systemic latencies induced adverse physiological effects in a large percentage of users, since camera motion was no longer controlled by a joystick but now slaved to the motions of the operator's head. This problem arises due to the vestibulo-ocular reflex that actively stabilizes our eyes in response to accelerations sensed by the inner ear. Any unexpected disparities in feedback from our visual and vestibular systems can quickly lead to headache, disorientation, sweating, fatigue, and even nausea. If the remote cameras do not immediately mimic the operator's head movements, the effect is much more noticeable than the equivalent lag of a joystick-commanded camera motion.

A third negative aspect of teleoperation is the driving burden imposed upon the operator. Even the very best video cameras are no match for the human eye in terms of acuity

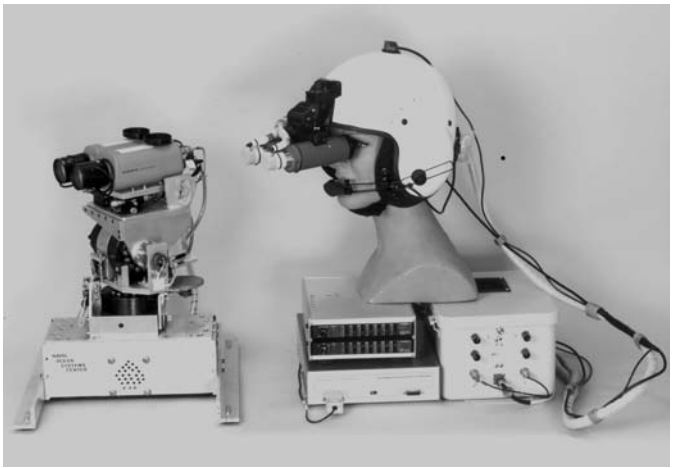


**FIGURE 4** The ground air telerobotic system (GATERS) helmet-mounted display employed an electromagnetic Polhemus sensor (top of helmet) to track the operator's head movements.

and dynamic range, and improved resolution is often achieved by zooming in the camera. The subsequently reduced field of view drastically restricts the operator's peripheral vision, however, down from somewhere around 180° (both eyes) to perhaps 40° or less. This "tunnel-vision" perspective forces operators to drive in an unnatural manner, with increased reliance on foveal vision relative to normal "manned-vehicle" driving, which is supported more by our subconscious perception.

Early NOSC attempts to reduce operator's burden through the application of onboard intelligence led to the reflexive-teleoperated control scheme developed on ROBART II [13]. The robot's sonar and optical collision-avoidance sensors, originally intended only for autonomous navigation, were also employed during manual operation to minimize the possibility of operator error. In this telereflexive mode, the control inputs for drive and steering still originate from a human operator as before. Both the speed and direction of the platform, however, are automatically altered as needed by the onboard software to keep the robot traveling at a safe speed without running into surrounding objects. A good analogy here is that of riding a horse versus riding a motorcycle: pointing the latter at a tree will result in a collision, whereas most horses will instinctively alter course to avoid contact.

In summary, the four fundamental shortcomings of teleoperated control include the following: (i) requires a continuous high-bandwidth communications link; (ii) suffers from feedback and control latencies; (iii) provides limited situational awareness; and (iv) imposes an excessive burden upon the human operator.

## 2.2 Weapon Control

While manually driving a remote vehicle is a very tedious and potentially fatiguing operation just by itself, adding a teleoperated weapon payload makes a bad situation even worse. Unless firing at a relatively motionless target from a static platform, the degree of accuracy and responsiveness required for effectively aiming a weapon is significantly greater than that needed for driving. Introducing any target or vehicular motion further

exacerbates the situation to the point where precise fire control is for the most part impossible. In addition, weapon-payload tasks are often complicated by potential time constraints and the need to follow definitive rules of engagement. If the remote operator has to simultaneously manipulate three different joysticks (i.e. one for drive and steering, another for camera pan and tilt, and yet a third for the weapon), the chances of successfully performing coordinated actions in a timely and effective fashion are minimal.

For this reason, work was begun in 1993 on ROBART III to extend the concept of reflexive-teleoperation into the realm of sensor-assisted camera and weapon control [5]. As a near-term strategy, the surveillance-camera pan-and-tilt axes could optionally be slaved to those of the weapon, so the camera automatically looked wherever the operator was aiming. The mobility base could similarly be slaved, causing the robot to turn and face the direction toward which the weapon was pointed. If a forward drive speed was commanded at this point, the operator merely had to keep the weapon trained on the intruder, and the robot would automatically give chase. Although this was clearly a step in the right direction in terms of reduced operator burden, it did nothing to address improved situational awareness or communication latencies. The most difficult task of all, controlling the weapon payload, was still teleoperated.

A more effective approach involves applying local sensor-assisted automation to those control tasks that can be off-loaded from the human operator. A breakdown of potential weapon-payload tasks is as follows:

*Target detection.* The two most distinguishing human characteristics that can be exploited by automated detection systems are that humans tend to move around and also give off heat. For this reason, the most common sensors employed in an initial detection role are Doppler radar, conventional video, and thermal imagers. Appearance cues such as skin temperature, color, texture, and aspect ratio are often taken into account as well to filter out nuisance alarms.

*Target acquisition.* The process of selecting a specific target from the set of all detected possibilities, and then aiming the weapon accordingly. A variety of factors come into play here, such as the perceived threat level, proximity to high-value assets, distance from the UGV, and likelihood of escape [7].

*Target tracking.* Maintaining a valid fire-control solution as the acquired target and/or UGV continue to move, which is a bit more complicated than simply pointing the weapon at the last observed target location.

*Target discrimination.* Rejecting inappropriate targets based on a variety of distinguishing features (i.e. noncombatant and unarmed), currently one of the biggest challenges for automated systems.

*Target prosecution.* The arming and firing of the weapon itself.

In the human-supervised sensor-assisted control scheme of ROBART III, the first three tasks of detection, acquisition, and tracking are automated, freeing the operator to focus on target discrimination and prosecution [6]. Since all detection and tracking functions take place locally, the debilitating effects of communications latency are eliminated, and any secondary systemic delays can be explicitly modeled for optimal performance. Two field-ready examples of more recent automated targeting systems are presented in the next section.

## 3 CURRENT LESS-LETHAL IMPLEMENTATIONS

The Force Protection Joint Experiment (FPJE) is a focused series of four technology-integration assessments to identify, scope, and mitigate risk for the Joint Force Protection Advanced Security System (JFPASS) Joint Capability Technology Demonstration (JCTD). Orchestrated by technical representation from the Army, Navy, and Air Force, the Joint Experiment serves as an effective venue for the evaluation of emerging force-protection technologies. A specific focus area is to integrate and assess automated response capabilities using lethal/nonlethal means to include semiautomated unattended weapons and semiautonomous security robots.

### 3.1 Unattended Weapon System

The network-integrated remotely operated weapon system (NROWS) is a stand-alone weapon platform designed to provide a remote lethal/less-lethal response to intruders (Fig. 5). The system employs autonomous surveillance, detection, and automated target tracking to enable timely response to hostile activity, but target prosecution remains

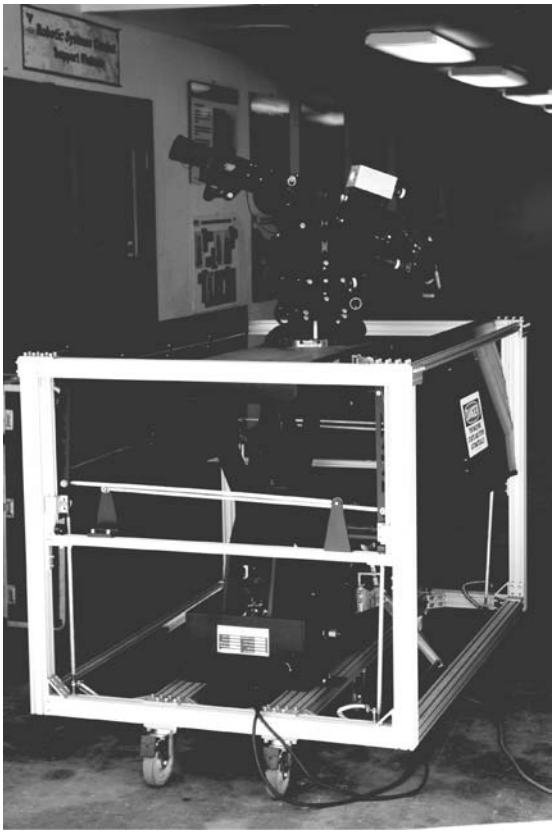


**FIGURE 5** The NROWS unattended weapon, shown here in the deployed position, can be housed in a protective "pop-up" enclosure until needed.

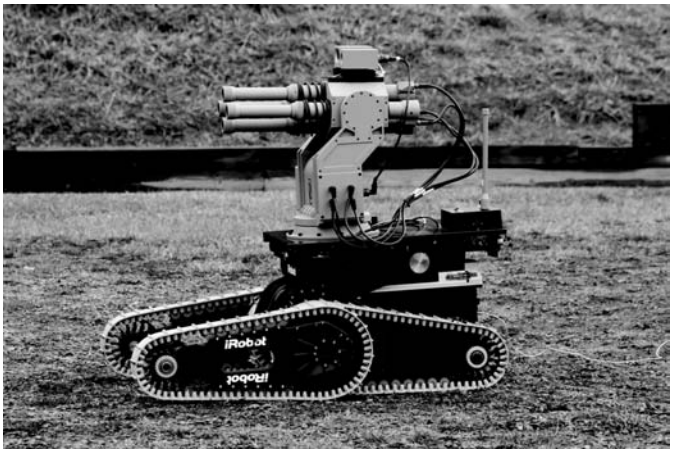



**FIGURE 6** Shown here on an iRobot Warrior, the multibarrel Metal Storm weapon can electronically fire (i.e. no moving parts to jam) a variety of lethal/less-lethal rounds.

under operator control. A transmission control protocol/internet protocol (*TCP/IP*) network architecture allows for flexible integration and operation of multiple platforms from a single control station. Communications between the remote unit and its command-and-control (C2) station can be established over a direct land line or via wireless link, providing a real-time unattended weapons pod that effectively extends delay/denial response capabilities.

On the basis of a precision weapon-aiming platform built by TeleRobotics Corporation (TRC) of Sausalito, CA, the system can apply a variety of small and medium automatic weapons in support of security or combat operations. These weapons require no modifications of any kind, facilitating use of standard government-issue munitions such as M4/16 and M240/249 machine guns. Less conventional armaments such as the multibarrel stacked-round Metal Storm weapon (Fig. 6) may also be adapted. NROWS platforms can be housed in a variety of configurations, including roof or wall mounts, inside protective ballistic shrouds, or in a "pop-up" unit suitable for installation at or directly below ground level. With the latter method, the weapon system can remain hidden until needed, making it less vulnerable to enemy surveillance and preemptive attack.

### 3.2 Robotic Response System

The mobile detection assessment response system (MDARS) provides a robotic capability to conduct semiautonomous random patrols and surveillance activities, including barrier-assessment and theft-detection functions. The current platform features diesel-powered four-wheel hydrostatic drive, global positioning system (GPS) navigation, and ladar-based obstacle avoidance. Soon to enter production by general dynamics robotics systems, the MDARS robot is equipped with an intrusion detection system (IDS) that can acquire and track multiple human targets out to 300 m. The IDS sensor suite includes Doppler radar and both regular vision and forward looking infrared (FLIR) cameras, which also provide a digital video feed to the C2 console.

The addition of a less-lethal weapon module, long envisioned as a preplanned product improvement under the MDARS Modernization Program, was completed in 2007 for

**FIGURE 7** Two air-powered FN303 less-lethal weapons are mounted on TRC precision aiming platforms attached to either side of the MDARS superstructure.

evaluation at the Joint Experiment. This add-on capability allows the remote system to audibly challenge intruders and attempt to delay or repel those showing hostile intent. The current weapon is a semiautomatic air-powered FN Herstal FN303 that is highly effective to 50 m, with a maximum range of 100 m. There are several different types of fin-stabilized 18-mm rounds available for a variety of missions, including impact, impact plus marking (i.e. indelible or washable paint and inert powder), or impact plus irritant, such as pepper spray.

Two FN303 weapons are mounted on TRC precision aiming platforms (Fig. 7), which in turn are attached to either side of the MDARS superstructure that supports the IDS module. This configuration allows both payloads to be trained on an intruder directly to the front or rear, or for individual tracking of separate targets. Each TRC system uses a single-board controller to receive incoming commands, position the pan-and-tilt axes, control bore-sighted cameras, and monitor arming and firing of the attached weapon. The controller accepts XML remote-procedure calls (RPCs) from the C2 software pertaining to weapon movement, arming, and firing.

When the robot enters sentry mode, the onboard software moves the weapons from their stowed to ready position and begins looking for intruder data packets from the IDS module. These packets contain a list of detected targets, each with an identifier, range and bearing from the robot, status flags, and a confidence percentage indicating the probability that the target is human. Each potential intruder is analyzed by the onboard software to determine the optimal target to prosecute. The remote operator can influence this process if desired by individually designating the console-displayed intruder tracks as either primary or friendly. The system attempts to point both weapons at a primary-flagged intruder if possible, or the nearest intruder otherwise, and will not track a target designated as friendly.

Since the intruder data packet contains a "snapshot" representation of where potential intruders were last seen, the predicted locations are estimated by calculating the speed and heading of each target, based on up to four previous range and bearing values. In

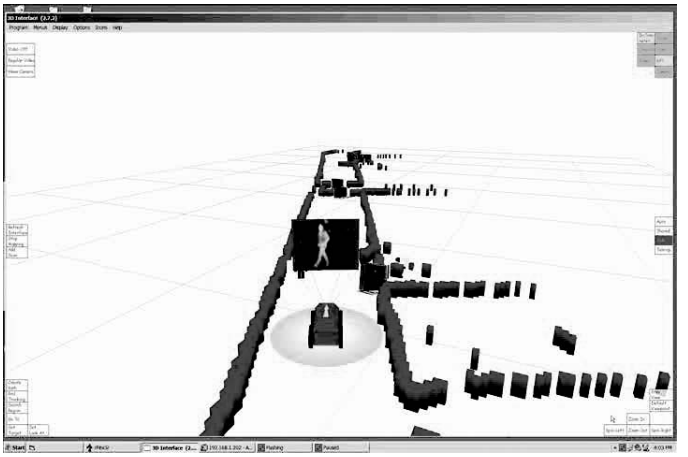


**FIGURE 8** Originally developed by Curtis Nielsen at Brigham Young University: this 3-D display provides enhanced situational awareness to the operator, such as laser-detected surroundings, robot location, robot pose, camera orientation, and video imagery.

this fashion, the projected fire-control solutions are computed in advance, and the system is locked on and ready to shoot as soon as the operator gives the signal to engage. The weapon-payload response can be optionally configured to initially fire warning shots at the ground in front of the intruder, followed by a second volley directed at chest level if he or she continues to advance.

## 4 FUTURE PLANS

While efforts to enhance the automation of detection, acquisition, tracking functions for UGV weapon payloads continue, achieving performance compared to the sophisticated fire-control systems already employed on military aircraft and tanks will be challenging. The most prevalent UGVs on today's battlefield are man-portable, where size, weight, and power constraints impose significant hurdles to adapting the complex armament that much larger vehicles are able to accommodate. These same man-portable systems are also more prone to tampering and sabotage, being easy to tip over, disable, or even capture, and so near-term incorporation of less-lethal defensive measures is of considerable interest.

Longer term efforts are investigating augmented-virtuality displays for improved situational awareness, allowing operators to more quickly assess the tactical situation (Fig. 8). Under the Warfighter's Associate concept, the control paradigm has progressively shifted from low-level joystick to high-level mouse input, and even speech recognition is finally showing real-world potential. Laboratory demonstrations of proximal human–robot interaction have shown that desired robot actions can be reliably inferred from the perceived state and behavior of its human counterpart. This innovative approach may one day allow an intelligent robot to acquire and prosecute a confirmed threat, based on where its human partner is observed to be aiming and firing.

## REFERENCES


1. Policy for Non-Lethal Weapons (1996). *Official Website for DoD Issuances*, available online at: http://www.dtic.mil/whs/directives/.
2. Department of Defense Nonlethal Weapons and Equipment Review: A Research Guide for Civil Law Enforcement and Corrections (2004). *Special Report*. National Institute of Justice, http://www.ncjrs.gov/pdffiles1/nij/205293.pdf.
3. Hightower, J. D., and Smith, D. C. (1983). Teleoperator technology development. *Proceedings of the 12th Meeting of the United States-Japan Cooperative Program in Natural Resources*. San Francisco, CA.
4. Aviles, W. A., Hughes, T. W., Everett, H. R., Umeda, A. Y., Martin, S. W., Koyamatsu, A. H., Solorzano, M. R., Laird, R. T., and McArthur, S. P. (1990). Issues in mobile robotics: the unmanned ground vehicle program teleoperated vehicle. *Proceedings SPIE Mobile Robots V,* Boston, MA, pp. 587–597.
5. Everett, H. R., and Gage, D. W. (1996). *A Third Generation Security Robot*, Vol. 2903, SPIE Mobile Robot and Automated Vehicle Control Systems, Boston, MA, pp. 20–21, 118–126.
6. Everett, H. R., Pacis, E. B., Kogut, G., Farrington, N., and Khurana, S. (2004). Towards a Warfighter's Associate: eliminating the operator control unit. *SPIE Proceedings 5609: Mobile Robots XVII*, Philadelphia, PA.
7. Kogut, G., Drymon, L., Everett, H. R., Pacis, E. B., Nguyen, H., Stratton, B., Goree, J., and Feldman, B. (2005). Target detection, acquisition, and prosecution from an unmanned ground vehicle. In *SPIE Proceedings 5804*, G. R. Gerhart, C. M. Shoemaker, and D. W. Gage Eds. Unmanned Ground Vehicle Technology VII, Orlando, FL, pp. 560–568.
8. Elliott, E. D., and Eagleson, R. (1997). Web-based teleoperated systems using EAI. *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, Orlando, FL. Vol. 1, pp. 749–754.
9. Held, R., Efstathiou, A., and Greene, M. (1966). Adaption to displaced and delayed visual feedback from the hand. *J. Exp. Psychol.* **72**, 887–891.
10. Day, P. N. (1999). An investigation into the effects of delays in visual feedback on real-time system users. In M. A., Sasse, and C. Johnson Eds. *Human-Computer Interaction —INTERACT '99*. IOS Press, Oxford, pp. 674–675.
11. Drury, J. L., Scholtz, J., and Yanco, H. A. (2003). Awareness in human-robot interactions. *Proceedings of the IEEE Conference on Systems, Man, and Cybernetics*. Washington, DC.
12. Martin, S. W. and Hutchinson, R. C. 1989. Low-cost design alternatives for head-mounted displays. *Proceedings, SPIE 1083*. Three Dimensional Visualization and Display Technologies, Los Angeles, CA.
13. Laird, R. T., and Everett, H. R. 1990. Reflexive teleoperated control. Proceedings, association for unmanned vehicle systems, *17th Annual Technical Symposium and Exhibition (AUVS '90)*, Dayton, OH, pp. 280–292.


## FURTHER READING


Unmanned Ground Vehicles http://www.spawar.navy.mil/robots/, 2007.

Non-lethal Bibliography http://www.au.af.mil/au/aul/bibs/soft/nonlethal.htm, 2007.

Ankin, A. C. "Governing Lethal Behavior", Technical Report GIT-GVU-07-11, available online at http://www.gatech.edu/ai/robot-lab/online-publications/formalizationv35.pdf, 2008.

# DEFENDING AGAINST DIRECTED ENERGY WEAPONS: RF WEAPONS AND LASERS

MICHAEL J. FRANKEL
*EMP Commission, Washington, D.C.*
EDWARD T. TOTON
*Toton, Incorporated, Reston, Virginia*

## 1 INTRODUCTION

Like many inventors of a new technology, the first caveman to heave a rock in anger at his fellow troglodyte must have quickly realized he was on to something. The concentration and direction of expended energy on a target where it will have the most impact, while minimizing the expenditure of wasted energy elsewhere where it will not, is the essence of directed energy weapons (DEWs). So, heaved rocks and other forms of kinetic weapons such as bullets are directed energy threats. High explosives, which may in more usual circumstances squander much of their kinetic energy in a spherically symmetric expansion into mostly empty space, may also be configured as DEWs through shape charge configurations or other specialized charge designs. But, the more common perception of DEWs today deals with devices that radiate electromagnetic energy in the form of high or low energy "light"—lasers and radio frequency (RF) weapons—and both charged and neutral particle beams.

A great deal of research dollars have been expended—and continue to be expended—by the US government in pursuit of the development of DEWs. The first suggested use of such devices in a military context dates back to the 1950s when charged particle beams were studied as a proposed defense against atomic weapons [1].[1] In the 1970s, there was particular interest in charged particle beam weapons in which directed beams of electrons might be used to protect ships from incoming missiles by engaging and thermally exploding energetic materials in incoming antiship missiles [2].[2] These efforts involved huge accelerators to produce the particles, elaborate steering mechanisms, and a host of technical challenges to propagate a beam, which had to overcome the natural tendency of similarly charged particles to run away from each other's vicinity. In the 1980s, the Strategic Defense Initiative Organization (SDIO) provided the sponsorship and funding to demonstrate a range of DEW: X-ray lasers (powered by nuclear explosions) and other nuclear-pumped directed energy schemes, continuous wave and pulsed chemical lasers, tunable free-electron lasers, neutral particle

[1]Compact accelerators capable of firing high energy electrons at incoming nuclear warheads were proposed by Nobel Laureate Robert Wilson in a now almost forgotten episode that presaged the inauguration of the "Star Wars" program in the 1980s by almost 30 years.
[2]cf. Navy's Chair Heritage program.

beams, high powered microwave weapons, and of course rocks [3].[3] Additionally, the technical feasibility of even more exotic directed energy schemes, such as $\gamma$-ray lasers, was examined, at least analytically. Resources have also been devoted to development efforts that may protect US systems against the threat of hostile use of DEWs by adversaries. These efforts range from the development of directed energy attack sensors to the development of hardened systems that can withstand an assault by DEW threat systems. Presently, the Department of Defense continues to explore the potential of DEWs for a variety of both tactical and strategic defense missions. However, much of this information has been classified and, in many ways, is not directly relevant to the threat to the civilian infrastructure described below.

## 2 DIRECTED ENERGY WEAPONS AND HOMELAND SECURITY

The focus of this article is homeland security and what can be done to protect ourselves from directed energy threats. Much of the directed energy gadgetry developed in pursuit of robust weapons systems, the gigantic accelerators and huge pulse power and energy storage systems, and technologically sophisticated and complex tracking and targeting systems would not seem to represent the most likely, easily transportable and concealable, threats available to either terrorists or rogue regimes intent on creating local, homeland, disruption. What remains then to consider are two directed energy threats to homeland security: lasers and radio frequency (RF) weapons.

### 2.1 Lasers

Lasers (*light amplification by stimulated emission of radiation*) are devices that produce highly concentrated beams of light, either continuously or in a pulsed mode operation. The mechanism of lasing involves the creation of a so-called electronic population inversion in a lasing medium in which excited atoms all transition to the same lower energy state, each atom giving up the same bit of energy in the form of a light wave. The coherent concentration of these individual but identical bits of light energy gives rise to the intensely energetic monochromatic beam that emerges from a laser. Lasing has been achieved in solid, liquid, and gaseous media and at a wide spectrum of frequencies ranging from the infrared through the visible, ultraviolet, and even $\times$ rays.

### 2.2 Radio Frequency (RF) Weapons

RF weapons deliver energy to a target in the form of electromagnetic radiation. The essential elements of such an electromagnetic weapon are a power source, a physical device to convert the power into electromagnetic radiation, and an antenna to broadcast the radiation in the desired direction. Traditionally, RF weapons are classified into two classes: narrow band, often described as high power microwave (HPM) weapons and wideband, usually described as ultra-wideband (UWB) weapons. HPM weapons are characterized by a narrow frequency band and generally operate in the gigahertz range. Depending upon the design details and type of power source, they may operate either

[3]The modern incarnation of designer rocks involve a number of complex interceptor systems including such as a theater high altitude area defense (THAAD) system, which is designed as a "hit to kill" intercept.

continuously or in pulsed mode. They will also generally require an expensive and highly specialized type of vacuum tube to convert the energy from a power source into guided microwave frequency waves. On the other hand, UWB RF sources will discharge their electromagnetic energy in a brief pulse containing a wide spectrum of energies ranging from tens of megahertz to tens of gigahertz. Instead of a technologically complex tube, they may use an intense spark gap as a radiation source. Depending on the design, these may also be repetitively pulsed. UWB weapons tend to be high power, but low energy, threats, which facilitates their design in small packages, unlike many HPM threats. Other nomenclature usage—such as transient electromagnetic discharge (TED) devices in place of UWB—may be found in the literature.

## 3 CONSEQUENCES OF EMPLOYMENT: WHAT DIRECTED ENERGY WEAPONS CAN DO

### 3.1 Lasers

In a terrorist employment, the chief concern is that lasers might be used as antipersonnel weapons to temporarily blind, or even permanently damage, the eyesight of individuals at critical operational moments. In particular, concern over the potential vulnerability of airline pilots to illumination by a mobile ground-based laser during takeoff and landing of commercial airliners has been a cause of considerable disquiet. At one end of the range of potential effects of aiming such focused laser energy on a pilot is the possible infliction of permanent eye damage, since intense light energy is focused by the eye's lens on the retina. The rods and cones situated there, the physiological task of which is to distinguish and transduce the different colors of ordinary light, can be destroyed at a sufficiently intense illumination. At lower intensities a pilot may experience temporary blindness from the intense glare or be "dazzled" by an intense sparkle as laser light scatters off the cockpit glass (Figure 1). The magnitude of this threat is enhanced by the ease of acquisition of such laser weapon threats. It is not only the relatively compact and high power systems that are readily available through many industrial catalogues and at educational institutions can represent an active threat, but the ubiquitous laser pointers favored by large numbers of faculty at almost any institution of higher learning in the United States and available at almost any store that sells educational supplies can also

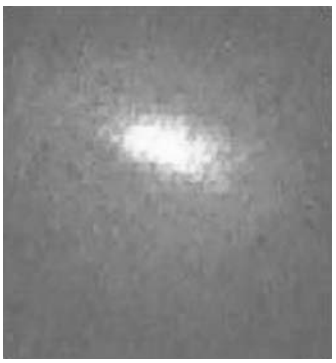


**FIGURE 1** Laser-induced cockpit glare. A pilot's eye view.

represent an active threat. Most troubling is the identification of more than 400 incidents since 1990 by the Federal Aviation Administration wherein aircraft cockpits have been illuminated by lasers leading to pilot distraction during critical phases of flight [4, 5]. While no aircraft losses resulted from these incidents, the National Transportation Safety Board has documented cases of pilot eye damage and incapacitation during critical phases of flight [6]. In the words of a recent report by the Congressional Research Service:

> A recent rash of incidents involving lasers aimed at aircraft cockpits has raised concerns over the potential threat to aviation safety and security. While none of these incidents has been linked to terrorism, security officials have expressed concern that terrorists may seek to acquire and use higher powered lasers to, among other things, incapacitate pilots. There is also growing concern among aviation safety experts that the ubiquity and low cost of handheld laser devices could increase the number of incidents where pilots are distracted or temporarily incapacitated during critical phases of flight [7].

Unlike energy emanating from more usual sources, which tends to spread itself out and dissipate its intensity with distance from the source, the highly collimated and energetic laser beam tends to propagate long distances with relatively little spread. Thus, its almost undiminished effects may be felt at very long distances from its origin in the absence of absorption by the atmosphere. On a clear day with low water vapor in the air, laser beams may propagate for very long distances. NASA has documented one incident of interference with pilot vision by a green laser at a distance of 90 miles from the source [8].

### 3.2 RF Weapons

It is often asserted that RF weapons affect only electronic devices, and do not directly affect people. This is not entirely true since microwave systems have also been developed for nonlethal antipersonnel applications.[4] But our concern over terrorist employment leads us to focus on the threat to electronic systems. RF systems, both of the HPM and UWB variety, work by coupling unwanted electrical energy contained in the strong electromagnetic field projected by the RF weapon to runs of wire and circuit elements in vulnerable electronic equipment. The effects of such RF weapon illumination on equipment will generally vary with the intensity of the illumination. At relatively low intensities, computer chips may experience "upset" and "latch-up" conditions, in which the internal electronic states in chips would have been affected by the imposed currents and voltages and a manual restart, or reboot, may be necessary. At higher intensities, the electronics may be degraded to the point they cannot be restarted and would have to be repaired or replaced. At still higher intensities, manifestations of physical damage, such as arcing or melting of circuit elements, may be observed (Figure 2).

RF technologists often speak of "front door" and "back door" vulnerability of equipment. Front door refers to the coupling of the RF energy from a beam directly into the vulnerable circuit element—such as memory chips and capacitors—through an intended signal path, usually via an antenna that collects the radiated energy and conducts it in the form of an impressed electric current to the vulnerable element. Back door refers to

[4] As anyone who owns a microwave oven is aware, RF energies can also heat things up. The Pentagon's nonlethal weapons development effort has demonstrated a "people stopper" that can be used for crowd control, which works by inflicting an intensely painful burning sensation when specially designed microwave devices are focused on human skin. Other organizations have also explored antipersonnel use of RF.

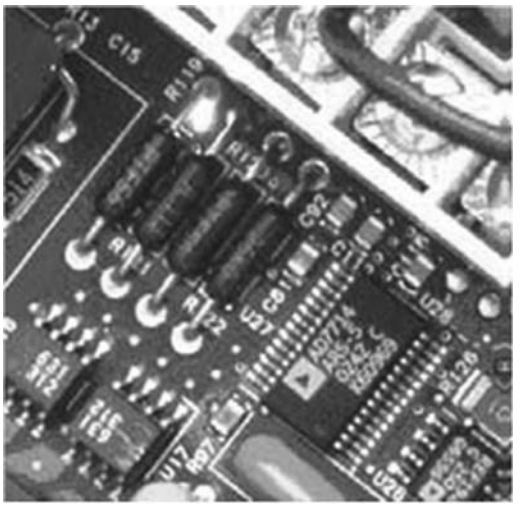



**FIGURE 2** Flashover observed in integrated circuit board during current injection testing (courtesy W. Radasky, Metatech Corp.)

the coupling of radiant energy through unintended paths, such as joints or cracks, and from there to circuit elements by coupling to metallic elements that act as expedient antennae. Most HPM and UWB threats attack systems through the "back door" as their frequency content is in the gigahertz regime and, at those frequencies and corresponding wavelengths, the physical size of typical commercial equipment is on the order of the threat wavelength.

The advance of electronics technology has also conspired to increase the potential vulnerability of our electronic systems. "Old" electronic systems that utilized vacuum tubes and relatively large-scale metallic elements were much more robust and resistant to interference by stray electromagnetic energy than modern digital electronic systems. The latter are characterized by submicron scale circuit features and "smart" capabilities enabled by a plethora of low-voltage computer chips whose continued functioning may not withstand stray circuit voltages. The shift from analog to digital processing inside modern electronics and the shift to processing frequencies above 1 GHz also greatly increases the probability of upset.

Of particular concern is modern supervisory control and data systems (SCADAs), which are increasingly deployed within every nook and cranny of our modern electronic-based critical infrastructures. Their function is to automatically monitor and remotely control the operation of geographically far flung systems such as the electric power grid, the pumps on our oil and gas pipelines, and our national telecommunications infrastructure. These ubiquitous control units confer great economic benefit and enormous operational agility, but are essentially unhardened computers—electronically quite similar to the personal computers found on every desk—which have been demonstrated to be highly sensitive to RF radiation. In the 1980s, catastrophic failure of a SCADA system controlling flow in a natural gas pipeline located 1 mile from the naval depot of Den Helder in the Netherlands caused a large gas explosion in a 36 in. diameter pipeline. This failure was caused by electromagnetic interference traced to an L-band naval radar coupling into the wires of the SCADA system. Radio frequency

**FIGURE 3** Consequences of SCADA system failure. Smoke from gas pipeline explosion, Bellingham, Washington.

energy caused the SCADA system to open and close at the radar scan frequency, a relay that was, in turn, controlling the position of a large gas flow-control valve. The resulting changes in valve position created pressure waves that traveled down the pipeline and eventually caused the pipeline to fail. A similar gas pipeline explosion in Bellingham Washington was also traced to the failure of SCADA control (Figure 3). In another incident ultimately traced to the operation of a Navy AN/SPS-49 radar system 25 miles off the coast of San Diego, the radar-induced failure of a SCADA system controlling the opening and closing of water and gas flow valves led to the subsequent letter of complaint by the San Diego County Water Authority to the Federal Communications Commission, warning of a potential "catastrophic failure" of the aqueduct system. The potential consequences of a failure of this 825 million gallon per day flow rate system ranged from "spilling vents at thousands of gallons per minute to aqueduct rupture with ensuing disruption of service, severe flooding, and related damage to private and public property."

The critical infrastructures on which the functioning of modern society is dependent are susceptible to disruption, degradation, or destruction by RF weapons fired at a distance to the line-of-sight exposed electronic components. The electric power grid depends on unhardened SCADA monitoring systems to detect and respond to problems. The SCADAs along with the critically important autonomous relays that protect the very long lead replacement time circuit elements such as the very high voltage transformers (which are no longer manufactured domestically and typically require more than a year's delay to fill an order) are increasingly of digital electronic design and susceptible to RF weapon damage. In the case of the autonomous relays, over the last 20 years, solid-state digital systems have increasingly replaced the older electromechanical designs, which has significantly increased their vulnerability to the threat of an RF weapon environment. A worrisome scenario envisions a series of simultaneous attacks on geographically separated elements of the electric grid by such electromagnetic weapons, which may produce a cascading failure of large sections of the grid. The data and operational control centers that enable the accounting and daily flow of trillions of dollars through our financial and banking systems are enabled by computers and other electronic elements that are

intrinsically susceptible to RF weapon environments. Similarly, transportation control centers, as well as switches that control railroad track function, contain digital electronic systems susceptible to RF energies. Thus, a terrorist in possession of such a means would find himself in a very target rich environment.

## 4 THE ATTRACTION OF DEW FOR TERRORISTS

From the perspective of terrorist employment, directed energy weaponry offers a number of attractive features. First, they are easily available. Compact high power laser and RF emitter systems can be purchased almost anywhere in the country for legitimate industrial or educational uses. They may be obtained at moderate cost and without the risks of discovery associated with the purchase, manufacture, or need for concealment from the attention of security and law enforcement authorities, that attends acquisition, transport, and employment of conventional high explosive systems. Secondly, high power lasers and high power RF systems are easily transportable. They are compact enough to be easily carried and concealed by a small truck or van. Yet smaller systems, still powerful enough to inflict damage are man-portable. Although probably not a terrorist weapon of choice, we have already noted how even a laser pointer can produce effects that may endanger the safety of airline travel. An RF weapon in a suitcase is available for purchase today (Figure 4). Thirdly, compact DEWs are easy to conceal and use covertly from a stand-off distance. A terrorist employment could drive an RF weapon system mounted in the back on enclosed van, park at a significant distance from a line-of-sight target, and take down an electronic target in complete silence, escaping immediate notice and facilitating an easy retreat and opportunity for additional attacks on other facilities. It might even take considerable time before it is realized that a deliberate attack was perpetrated. Fourthly, while an explosive may be fired and used only once, a directed

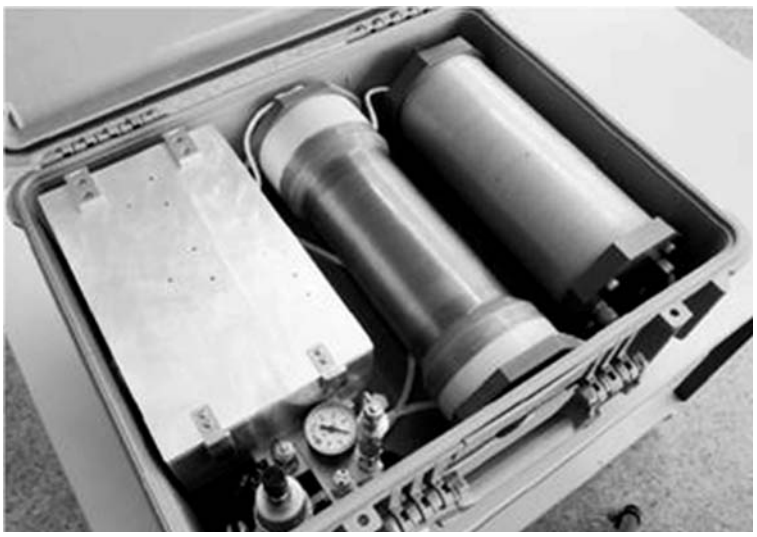


**FIGURE 4** RF weapon in a suitcase. Available for purchase from Diehl Stiftung and Co. KG, Germany.

energy system may have a "deep magazine." Unless powered by a special one-shot output device such as a compressed flux explosive generator, a directed energy device can be fired again and again, as long as the power system contains energy. Many RF weapon environments are high power and low energy environments, which reduces the need for a large energy source.

## 5 THE RISK OF TERRORIST EMPLOYMENT

Risk is formally accounted as the multiplicative concatenation of the (conditional) probabilities of threat, times vulnerability, and times consequence. We have discussed some of the potential consequences of terrorist employment of such weapons in the previous section. The vulnerability of modern digital electronics to electromagnetic disruption is also well established, not only by the accidental demonstrations such as the SCADA failures previously referenced (along with countless other instances) but also by scientific testing programs, which have established the susceptibility levels and thresholds for electromagnetic shock for commercial electronic devices [9]. Testimony at a Congressional hearing indicated that electronic equipment may be degraded or damaged when impressed field levels are on the order of kilovolts to tens of kilovolts per meter [9]. Similarly, the vulnerability of human eyesight to high power lasers has been amply demonstrated over many years. The threat is also clearly real. If we consider it simply from a capabilities-based perspective, it is clear that the technology knowledge is not just widely disseminated but acquisition of the physical devices themselves is about as easy as filling an order from an internet catalogue. A recent government-sponsored effort explored the ease with which a home-brew RF weapon might be assembled from parts available for purchase from a local radio shack [10].[5] Congressional reports have also speculated about the possibility of terrorist interest in exploiting the capabilities of such devices [11].[6] That is, the existence of threat, vulnerability, and consequence is well established, and the risk is undeniable. Quantitative assessment of such factors relative to other risks and risk prioritization remains a task for the Department of Homeland Security.

## 6 MANAGING THE RISK: RECOMMENDATIONS

Characterizing risk in terms of threat, vulnerability, and consequence is the essence of risk analysis. What to do about it is the essence of risk management [12, 13]. There are a number of actions that may be taken to reduce our vulnerability to DEW employment, and reduce the consequences as well. The following recommendations are offered:

- Perform a site vulnerability assessment by knowledgeable RF professionals.
- Reduce line-of-sight vulnerabilities to directed energy interference. Data centers or operational centers should not be sited within glass walled buildings with clear views of nearby roads. If you can see the road, the road can see you and may

[5]The hearings were devoted to a different sort of electromagnetic pulse phenomenon, that due to a nuclear source which a different frequency spectrum than that associated with RF weapons, but the radiation field intensities for expected damage are not dissimilar.

[6]Subsequent government-sponsored tests at Aberdeen proved inconclusive.

point something back. Similarly, unimpeded views into open upper floor and open windows should not be offered to potential observers in other buildings, even if the other building is at a kilometer distance.

- Consider the routing of cables and other conducting metal runs that enter a facility. These may become conduits into internal equipment for unwanted electrical energies imposed by RF weapons on exposed runs of cable. Where possible, these should be buried or otherwise hidden from view.
- Compile and maintain lists of critical equipment whose loss would not only shut down operations or endanger safety but might also be difficult to quickly replace. Consider maintaining an inventory of spares for critical components.
- For "high value" targets, deploy attack warning sensors to improve situational awareness that an attack has actually occurred or is underway.
- Consider the cost–benefit and utility of selective hardening of some critical components. For high value operations such as computer data centers, consider placing the computers within an interior, RF shielded, room.
- Continue current government investment in protective materials development efforts for both laser and RF threats. Such materials might include easily applicable "spray on" hardening for RF protection or optically reactive materials for laser protective applications. For private industry, begin such investment.
- For critical facilities, enforce access control and maintain "keep out" distances. Do not allow uninspected bag, briefcases, or shipments into critical facilities.

Risk may not be eliminated, but prudent preparations and some advance planning may serve to reduce it to tolerable levels.

## REFERENCES


1. Schweber, S. S. (2007). Defending against nuclear weapons, a 1950s proposal. *Phys. Today* 36–41.
2. Snow, D. M. (1980). Lasers, charged-particle beams, and the strategic future. *Polit. Sci. Q.* **95**(2), 277–294.
3. Missile Defense Agency http://www.mda.mil/mdaLink/pdf/thaad.pdf.
4. Nakagawara, V. B., Dillard, A. E., McLin, L. N., and Connor, C. W. (2004). *The Effects of Laser Illumination on Operational and Visual Performance of Pilots During Final Approach*, Department of Transportation, DOT/FAA/AM-04/9, June.
5. *U.S. Secretary of Transportation Norman Y. Mineta Announces New Laser Warning and Reporting System for Pilots, Measures to Safeguard Pilots and Passengers, Support Timely Enforcement*, Department of Transportation Press Release DOT 08-05.
6. National Transportation Safety Board *Safety Recommendation Letter–Safety Recommendations A-97-13 through -15*. Washington, DC.
7. Elias, B. (2005). *Lasers Aimed at Aircraft Cockpits: Background and Possible Options to Address the Threat to Aviation Safety and Security*, CRS Report for Congress, January 26, 2005, http://fas.org/sgp/crs/RS22033.pdf.
8. National Aeronautics and Space Administration, Aviation Safety Reporting System (NASA/ASRS). Report Numbers 285090 and 290037. Moffett Field, CA.
9. Radasky W. A. (2004). Special issue on High Power Electromagnetics (HPEM) and Intentional Electromagnetic Interference (IEMI). *IEEE Trans. Electromagn. Compat*. **46**(3).

10. Jakubiak, S. (1999). *Statement before the House Military Research and Development Subcommittee, hearing on EMP Threats to the U.S. Military and Civilian Infrastructure*, October 7, 1999.
11. Shriner, D. (1998). *The Design and Fabrication of a Damage Inflicting RF Weapon by 'Back Yard' Methods*, Testimony before the Joint Economic Committee, United States Congress, February 25, 1998.
12. Wilson, C. (2004). *High Altitude Electromagnetic Pulse (HEMP) and High Power Microwave (HPM) Devices: Threat Assessments*, CRS Report for Congress, August 20, 2004, http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-6028:1.
13. Scouras, J., Cummings, M. C., McGarvey, D. C., Newport, R. A., Vinch, P. M., Weitekamp, M. R., Colletti, B. W., Parnell, G. S., Dillon-Merrill, R. L., Liebe, R. M., Smith, G. R., Ayyub, B. M., and Kaminskiy, M. P. (2005). *Homeland Security Risk Assessment. Volume I. An Illustrative Framework*, RP04-024-01a. Homeland Security Institute, Arlington, VA, November 11, 2005.

## FURTHER READING

Beason, D. (2005). *The E-bomb: How America's New Directed Energy Weapons Will Change the Way Future Wars Will Be Fought*, Da Capo Press.

McCarthy, W. J. (2000). *Directed Energy and Fleet Defense: Implications for Naval Warfare*, Occasional Paper No. 10, Center for Strategy and Technology, Air University, Maxwell AFB, https://research.maxwell.af.mil/papers/ay2000/csat/csat10.pdf.

# THE SENSOR WEB: ADVANCED TECHNOLOGY FOR SITUATIONAL AWARENESS

KEVIN A. DELIN

*SensorWare Systems, Inc., Pasadena, California*

EDWARD SMALL

*Sacramento Metropolitan Fire District, Sacramento, California*
*and FEMA Urban Search and Rescue Team, CA Task Force 7, Sacramento, California*

## 1 INTRODUCTION

The need for situational awareness in the dynamic environment of emergency and rescue operations is well understood. Data must be continually collected, analyzed, assimilated,

and disseminated to both local operational personnel and remote commanders. The basic principles of "Facts, Probabilities, Own Situation, Decision, and Plan of Operation" for fire and rescue strategies are just as relevant today as they were when originally described in 1953 [1]. Simply stated, situational awareness informs decision making and decreases reaction time to changing conditions, even allowing for anticipation of events in certain instances.

Failure to effectively collect, synthesize, and distribute facts to personnel involved at all levels of a field operation will result in service delays, or worse, death. Emergency services personnel cannot begin operations without having the ability to monitor for hazards and account for personnel. Because emergency and rescue operations are labor intensive, however, continuous and effective monitoring for hazardous conditions often becomes less of a priority, or disappears entirely. It is therefore of critical importance to find a technological means to generate situational awareness for those personnel working in the hazardous area, both as a means to speed the course of the operation and to protect the personnel from danger.

Here, one such new piece of equipment, the Sensor Web, is examined. This technology can aid and substitute for human efforts in understanding the changing, and often chaotic, conditions during emergency service operations. First, the Sensor Web technology will be briefly described. Then, a series of representative field applications, including actual operations, will be given, which illustrate the unique capabilities of the Sensor Web as applied to emergency services. Finally, future directions of the technology are considered.

## 2 SENSOR WEB TECHNOLOGY

The Sensor Web is an embedded, intelligent infrastructure for sensors. Physically, it consists of spatially distributed sensor/actuator platforms (called "pods") that wirelessly communicate with one another (Fig. 1). Originally developed at National Aeronautics and Space Administration (NASA) for planetary exploration of unknown environments, the Sensor Web is also well suited for providing situational awareness in the chaotic and unpredictable environments associated with emergency and rescue operations. Despite its sophistication, such a system would cost no more than traditional, less capable wireless solutions and could actually reduce total operational costs by providing continual, automated in-field analysis thereby freeing up rescue personnel for other, more demanding, tasks.

### 2.1 Sensor Web Protocols

The wireless communication between pods should be thought of as an information bus, in the same way that buses connect the individual components (hard drive, optical drive, memory, logic units, etc.) of a computer. Consequently, while the individual pods are certainly networked with each other, the Sensor Web is not, in and of itself, a network but rather a spatially distributed macroinstrument [2]. The distinction is crucial: a network consists of components that *route information* along communication paths to specific destination points, while a macroinstrument consists of components that *share information* with each and every other piece at all times without any intervening routing. The Sensor Web's applicability to situational awareness, in fact, derives from having

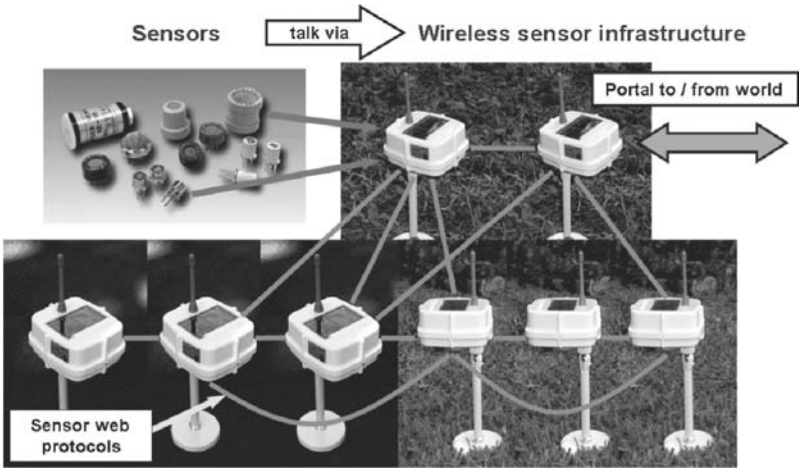



**FIGURE 1** Schematic representation of a Sensor Web. Sensors are connected to the pods (white boxes). The pods communicate wirelessly to form an amorphous network where all pods are equivalent and any pod can be a portal to the outside world.

its sensor measurements taken, distributed, and interpreted *collectively* over this unique, massively redundant, communication architecture.

It can be stated in another way, that every pod pushes its data out onto the Sensor Web in an omni-directional manner. There is never a purposeful routing of data toward a specific pod or a special portal or gateway. In this way, every pod is made aware of conditions throughout the entire Sensor Web during each measurement cycle. In fact, while the computation hardware in a pod can be quite sophisticated, it is the sharing of information among the pods that gives the Sensor Web its macrointelligence. This is similar to how perception is created in the brain from a complex, interacting set of neurons that share electrochemical signals [3] rather than from individual intelligence at each neuron.

The Sensor Web communication architecture of data sharing is distinct from both hub-and-spoke and mesh network types. In hub-and-spoke networks, individual spoke nodes can be synchronized to the hub but the information must always be routed through the hub to get to other points. Mesh networks are typically based on asynchronous Internet-like (TCP/IP) protocols and require information routing as well. In marked contrast to these two network types, the Sensor Web communication architecture, by design, is synchronous (all measurements across the system are taken at the same time) and requires no routing.

The Sensor Web communication protocols are simple and robust. Each measurement cycle begins with the pods taking in sensor data. After a measurement is taken, each individual pod in the system broadcasts its information (data it has taken or received from others) in an omni-directional manner to all pods in communication range. Each pod then processes and analyzes the information it has received and the cycle repeats. In this way, the information is hopped pod-to-pod and spread throughout the entire Sensor Web. The entire system becomes a coordinated whole by possessing this internal, continuous data stream, drawing knowledge from it, and reacting to that knowledge.


(a) (b)

**FIGURE 2** Sensor Web pods. (a) A standard pod is in the background and shows both the 900-MHz antenna and a solar panel to harvest additional energy for the pod's rechargeable batteries. In the foreground is a special display pod where a flat panel display has replaced the solar panel and reveals the conditions at other pods. This allows mobile personnel to monitor the Sensor Web without having to access a computer. Labels have been attached to the pods to clearly mark their software-assigned identification. (b) A responder deploys a Sensor Web pod. The pods can be mounted using a variety of hardware including stands, magnetic bases, and spikes.

## 2.2 Sensor Web Pods

A key feature of the Sensor Web is that its component parts, the sensor platforms or pods, are all alike (Fig. 2). In general, they only differ by the sensors attached to them. A single pod, known as the mother, holds the single, system-wide clock that will synchronize all pods. The mother, however, holds no special hardware; indeed any pod may be designated as the mother simply by labeling it as such. Unlike hub-and-spoke and mesh networks, the Sensor Web is a truly amorphous network with no central point and no specially designated portal or gateways.

Each Sensor Web pod consists of five basic modules:

1. *The radio.* Although any radio frequency can be chosen, the 900 MHz license-free Industrial, Science and Medical (ISM) band has been used in manufactured Sensor Web systems to date. This frequency requires no licensing of end-users and does not compete with the more common frequencies found at emergency sites (minimizing jamming). In addition, radios operating at this frequency do not require line-of-sight communication (even going through concrete walls) and have an upper range of about 200 m (compliant with government power regulations). Because each pod will essentially function as a repeater and retransmit data it receives from other pods, the effective radio range is extended far beyond the limits imposed by the specifications and regulations associated with a single radio.

2. *The microprocessor.* This component contains the system's protocols, communicates with the attached sensors, and carries out data analysis as needed.
3. *The power system.* The combination of solar panels, rechargeable batteries and micropower electronic design have kept Sensor Web pods operating in the field for years without requiring maintenance.
4. *The pod packaging.* The package is lightweight, durable, inexpensive, and sealed against such elements as rain, standing water, water sprays, dust storms, and caustic chemicals. In addition, it enables an easy and rapid mounting.
5. *The sensor suite.* This module is completely determined by the specific application. It is the ability to accommodate a wide range of sensor types that makes the Sensor Web so versatile. For the types of operations discussed here, typical sensors include those for monitoring gases and environmental conditions such as air temperature and humidity.

### 2.3 Sensor Web Properties

As just described, the Sensor Web is a distributed macroinstrument based on its unique protocols that allow for data sharing via nonrouted, synchronous inter-pod communication. These characteristics create valuable Sensor Web properties when the technology is applied to emergency and rescue operations (Fig. 3).

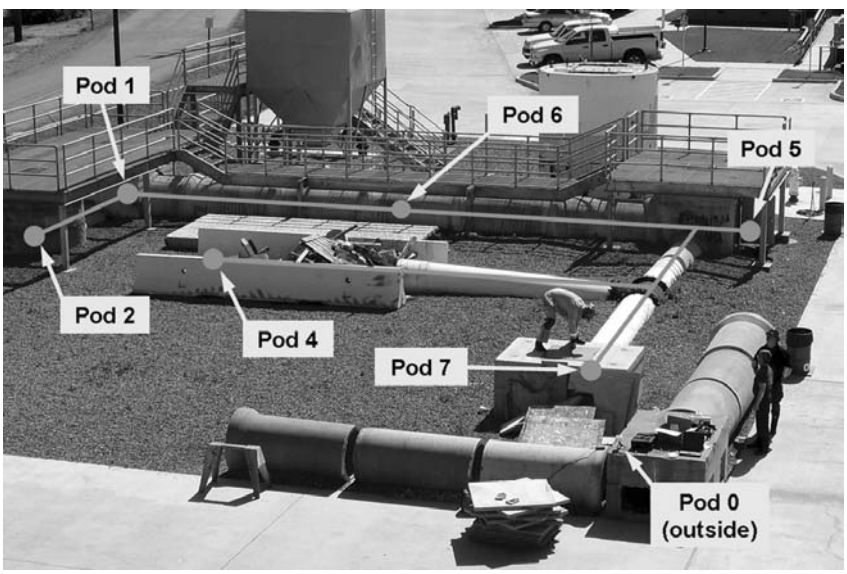



**FIGURE 3** A confined space training facility for Urban Search and Rescue. The Sensor Web system was deployed inside the structure as indicated schematically by the dots. The size of the structure is indicated by the size of the firefighter on top of the structure near pod 7. Lines connecting dots indicate physical paths, not pod connectivity. When deployed, the pods were able to wirelessly communicate through the concrete barriers; for example, pod 4 was in direct communication with pods 1, 2, and 6. When a chain saw was intentionally left running between pods 5 and 6, personnel were able to observe the migration of carbon monoxide through the structure with one front toward pods 6, 1, and 2 and a secondary front toward pod 7. All pods in the system went into alarm together when the gas first reached threshold levels at pod 6.

1. The redundant, nonrouted data sharing allows for any pod to be a portal to the outside world. Since every piece of the Sensor Web contains all the same information, anyone with access to a single pod will be provided with the same situational awareness picture. This means that the first responder at the rescue scene looking at the flat panel display of a pod, the incident commander directing operations who has plugged his laptop computer into another pod, and remote government personnel examining the information of a third pod being sent out over the Internet, will all simultaneously have a common, unified picture of operations.
2. A single, system-wide clock provides for an immediate synchronous snapshot that can be intuitively understood by field personnel. Because the Sensor Web is synchronous, all the measurements are taken at the same time and, in essence, become a pixel in the overall picture taken by the Sensor Web. This picture is an immediate integration and valuable for in-field personnel to understand plume motion, for example, without the need for time-consuming posthoc analysis. Moreover, when combined with the massively redundant, nonrouted communication paths, this snapshot is known to all pods in the Sensor Web which allows for *anticipatory* warnings and alarms. In this way, field personnel are alerted to dangerous conditions anywhere in the work zone immediately by the Sensor Web rather than by a remote incident commander.
3. Synchronous system behavior reduces latency between data taking and data reporting. Each pod has the same situational awareness picture at the end of every measurement cycle. Because each pod can act as a portal into the system, this implies that all end-users are kept up-to-date on every measurement cycle.
4. The massively redundant, nonrouted communication paths provide for a highly robust structure with no central point of system failure. Since all pods are potential portals, the loss of any particular pod does not affect the entire operation. Since any pod can be designated as the single, system-wide clock, the worse case scenario of a damaged mother pod is rapidly recoverable simply by assigning (via a software label) the designation of "mother" to another pod. This worse case failure can even be corrected automatically without human intervention if, after a predetermined amount of time without receiving signal from the mother, the pod with the current lowest serial number in the Sensor Web promotes itself to mother.
5. The redundant, nonrouted, data sharing allows for recoverable single point sensor failure. Because every pod contains a microprocessor and knows all sensor measurements across the system at each measurement cycle, each pod can locally analyze global conditions across the entire Senor Web. It is therefore possible for the system to immediately evaluate a seemingly anomalous measurement against the background of neighboring measurements to determine, on a statistical basis, false positives or to distinguish between a merely worsening trend versus a true critical situation requiring evacuation. It is also possible for the system to "suggest", within the same measurement cycle, a missing sensor measurement by combining spatial interpolation of neighboring measurements with recent local measurement trends.
6. The massively redundant, nonrouted communication paths allow the system to be easily and rapidly deployed. No special skill is required to set up a Sensor Web as all the pods are essentially the same (in contrast to other networking schemes which requires special hardware gateways or router tables). As a result, once the mother

pod is switched on to provide a clock for the system, the pods may be dispersed as dictated by the needs of the situation. Data taking is immediate and the pods may even be reshuffled on the fly and, as long as they stay within communication range, maintain the overall Sensor Web macroinstrument. This is particularly valuable if pods are assigned to specific rescue squads that are moving independently through a building. Because emergency service operations do not allow the time to leisurely recall complex equipment function, the simplicity and speed of deployment may be among the Sensor Web's most compelling and important features.

## 3 SENSOR WEBS APPLIED TO FIELD OPERATIONS

To date, there have been over 30 Sensor Web field deployments with systems spanning distances up to 6 miles and running continuously for over 3 years. The systems have been tested extensively in numerous, challenging environments from the remote ice slopes of Antarctica to the searing heat of the central New Mexico desert to the corrosive salt air of the Florida coast [4–6]. Real time, streaming output of some of these systems may be viewed over the Internet using a variety of user interface displays [6]. Here, the Sensor Web capabilities as applied specifically to emergency and rescue operations will be examined. As will be shown, the Sensor Web's properties and physical robustness allow it to efficiently bring key environmental parameters together in a continuous operational picture and disseminate this picture to in-field and remote personnel.

A critical issue for any type of deployment is determining a pod's location. For extended, outdoor operations, this is most easily accomplished by using an external Global Positioning System (GPS) unit during deployment, noting pod placement coordinates, and putting these coordinates into the pod's memory as it is deployed. Pods can then share their individual coordinates with each other just as they do with sensor data. If pod power usage, size, and cost are not an issue, it is also possible to place a GPS unit inside each pod. Sometimes, however, GPS coordinates may not be a practical option because (i) pods may be shielded from strong GPS signals (as when placed inside a building), (ii) building geometry provides a more transparent understanding of pod placement (e.g. "pod at the west end of the first floor corridor"), or (iii) typical GPS resolution may not be accurate enough (as in the case of placing a pod against a wall and determining which room it is in). In such cases, simple hand mapping by in-field personnel has been found to be effective and easily performed, even under rapid deployment circumstances. In addition, these hand-mapped "coordinates" typically provide rescue personnel with a clearer, intuitive picture of how the Sensor Web is deployed in the area. Pods can still autonomously perform spatial data analysis in these cases because a relative pod placement map can be formed by each pod through a shared knowledge of every individual pod's nearest neighbors.

### 3.1 Atmospheric Monitoring

The predominant cause of death in a confined space incident is from a hazardous atmosphere. Typically, in a confined space or structural collapse operation, one highly competent person is dedicated to the position of "environmental officer". This person continuously monitors the atmosphere by way of a gas sensor with remote sampling capability, or by periodically requesting a reading from the entrant who is carrying a gas

sensor, or both. This person also directs the forced ventilation efforts to enhance victim survivability and to maintain as tenable, and explosion-free, an atmosphere as possible.

There are several difficulties associated with the present technique. First, because all of the gases monitored have different vapor densities, they tend to stratify at different levels in the space, or may become trapped in dead spaces and fail to diffuse into the atmosphere. For this reason, atmospheric sampling must occur at 4-ft intervals, both vertically and horizontally. This significantly slows the progress of field personnel motion as they move into or even exit a confined space operation. Second, while the use of a sampling pump and tubing is a common method of obtaining remote gas samples within the confined space, there is the issue of the time it takes for the atmospheric sample to be drawn through the sample tubing. Since this may take up to 3 sec/ft of tubing and 50-ft sections of tubing are not uncommon, gas monitoring can require 1.5–2.5 min of delay per sample. Third, with the portable devices typically used by rescue personnel, evacuation of the space is often at the discretion of those working. Experience has shown that most in-field personnel consider an alarm to be an annoyance, and remain focused on completing their task; the atmosphere is only a "little hazardous". Finally, documentation of the atmospheric monitoring for most types of confined space operation is required by state/federal law, yet maintaining this documentation during the operation takes away from the actual emergency or rescue services.

Sensor Webs have been built and successfully used for monitoring confined space atmospheres. Here, the pods are equipped with the four gas sensors necessary for this application (e.g. oxygen, carbon monoxide, hydrogen sulfide, and explosive limits). The pods also contain sensors for air temperature and humidity. The measurement cycle for this Sensor Web is programmed for 30 sec. These systems have been used for several years now in confined space operations and collapsed structure training exercises. It has been found that the rescue personnel readily adapt to the new technology and have no difficulty infusing the technology into standard procedures (Fig. 4).

Benefits of using the Sensor Web for atmospheric monitoring are as follows:

1. Providing a permanent sensing infrastructure that frees the rescue personnel from having to take measurements. As a squad penetrates the confined space or collapsed structure, it deploys pods along the ingress path, effectively growing the Sensor Web. Once in place, the Sensor Web allows personnel to move freely into and out of the operations area. This is especially important during lengthy operations where squads will be replaced periodically. Moreover, since all pods would alarm when any pod detects a hazard, other responders working in other portions of the building will be aware if there is a gas leak that could affect them as well. As a result, responders will quickly know when to exit and how to modify egress paths by detecting remote atmospheric changes due to gas leaks.
2. Reducing the latency of obtaining measurements compared to drawing gas through a tube. Measurements are now available to the environmental officer at the sampling frequency (here, 30 sec.) throughout the field of operation.
3. Providing the environmental officer and incident commanders with a full picture of atmospheric conditions without diverting the rescuer's attention from other crucial tasks (Fig. 5). During an actual collapsed structure training operation, the Sensor Web revealed trends of oxygen displacement from the expired carbon dioxide of rescuers in confined areas, as well as increases in temperature and humidity from rescuers and equipment. This allowed the incident commander to move ventilation


**FIGURE 4** Sensor Web used for atmospheric monitoring. (a) A 10-pod Sensor Web system, including laptop and several varieties of pod mounting hardware fit compactly in a case, ready for rapid field deployment. (b) A pod being lowered into a confined space to determine atmospheric conditions. The pod will be left in this space for the duration of the operation allowing personnel to freely move into and out of the area.

fans from other parts of the operation into the affected confined areas to allow rescuers to proceed without stopping. While the Sensor Web system provides warning of imminent hazardous conditions, just like the single station gas detectors, the greater value may be in its ability to display trends in environmental conditions and disseminate that information to commanders with authority to act.

4. Providing an accurate and immediate record of conditions recorded every 30 sec by the Sensor Web and output to a laptop connected to the mother pod.

### 3.2 Structural Integrity Monitoring

The dangers present in and around structures compromised by natural or man-made disasters are rarely static. Building conditions can continue to deteriorate by the actions of earthquake aftershocks, wind, rain, and snow loading, and the intentional or unintentional actions of rescue workers.

The 4-gas Sensor Web pods described above also have an accelerometer built into them. The accelerometer functions as a tiltmeter to determine a change of state in the pod's orientation. The pod, attached to shoring or a building wall, can monitor changes while they are occurring and warn of impending failure. Such pods therefore perform double-duty, monitoring both atmosphere and structural integrity with the attendant reporting benefits for both parameters (Fig. 6).

Shoring stress tests revealed that the Sensor Web provided warning 60 s (two measurement cycles) before shoring failure. Such an advanced warning, distributed throughout

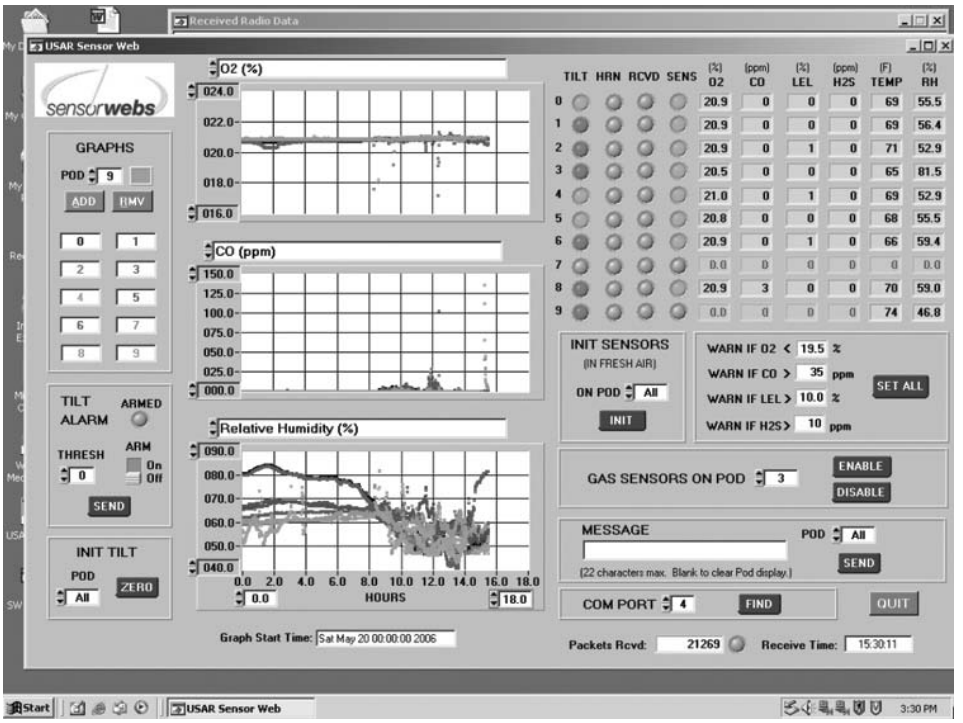



**FIGURE 5** A screen-capture of the user interface for the Sensor Web. Time-based trending data are immediately available as are current readings from the system. The interface also serves as a command portal into the system. Note the spike in CO concentration at hour 15. This was a result of an acetylene torch being ignited inside the collapsed structure.

the entire space of operations, would greatly reduce the risk of personnel being caught in a further collapse.

### 3.3 Decontamination Monitoring

During biological decontamination operations, a chemical agent is introduced at the proper temperature and humidity to destroy the intended pathogen. Such operations are typically very complex logistically and labor intensive. The target structure to be decontaminated is first sealed with tarps that must hold the caustic decontaminant gas over many hours. Typical operation will have the caustic gas pumped into and out of the structure continually with small fans placed throughout the structure to ensure even distribution of the gas. The entire building's atmosphere needs to be monitored during the decontamination procedure to ensure that proper conditions exist (decontaminant concentration, temperature, and humidity) to kill the pathogen.

Presently, wet chemistry techniques are used to monitor the operation. Long plastic tubing is distributed throughout the structure from a central hub. Atmospheric samples are pumped out of the hub at regular intervals and examined chemically to maintain appropriate conditions in the building.

There are several disadvantages with this technique. First, the distribution of the plastic tubes can take nearly a full day, even in a modest-sized home. Second, sampling


**FIGURE 6** Pods are attached to shoring.

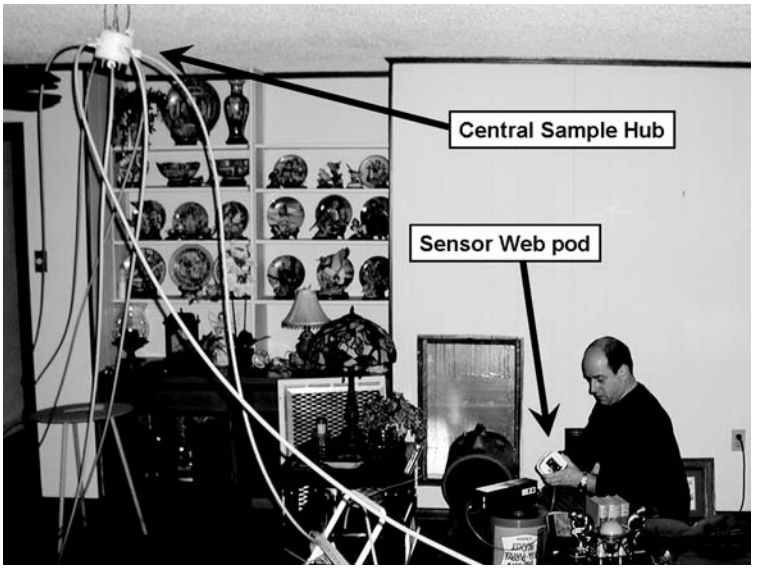
in this manner means that the chemical analysis will only yield the average conditions of the building due to gas mixing in the central hub. As a result, there still might be pockets in the structure where an appropriate concentration of decontaminant is not obtained, allowing for the pathogen to live. Lastly, water can collect in the plastic tubing due to the high humidity conditions typically needed during operations. This water can effectively absorb the gas ($ClO_2$ in the case of anthrax decontamination), which will create spurious results during chemical analysis. The tubes can also fill with ice during winter-time decontaminations and therefore make sample retrieval impossible and force operators to abort the entire operation.

A Sensor Web with $ClO_2$ sensors attached to each pod has been successfully used to alleviate these problems (Fig. 7). Inclusion of the technology into the operations was easy and personnel were able to learn the system in literally under 15 min. At least a dozen actual decontaminations have been performed using this system. In addition to the tremendous labor reduction in eliminating the tube system for gas sample retrieval, the Sensor Web allows operators to follow the $ClO_2$ gas plume throughout the structures in real time. On more than one occasion, this enabled operators to immediately find leaks in the building's tarps as well as building pockets where $ClO_2$ gas concentrations were lower than expected.

## 4 FUTURE DIRECTIONS

The Sensor Web is a general information infrastructure for sensors. It collects, analyzes, and reacts to whatever conditions are important to the end user, and can be coupled with existing methods of obtaining the necessary data. Any low-bandwidth sensor can be attached to the Sensor Web and enhance the situational awareness properties of the system. Initial experiments using a Sensor Web to track in-field personnel during operations

(a)




(b)

**FIGURE 7** Sensor Web used for decontamination operations. (a) Environmental Protection Agency (EPA) decontamination team member deploying a Sensor Web pod. The black box attached to the pod is the $ClO_2$ sensor. (b) A Sensor Web is deployed in a decontamination area that also uses the traditional sampling method to monitor $ClO_2$ concentration. Note the traditional method requires plastic tubing that runs through the entire house and connects to a central hub where atmosphere samples will be pumped out for chemical analysis.

show promise. Such a capability would benefit locating fire fighters lost in buildings as well as provide an accurate count of personnel going into and out of a rescue operation area.

Other applications for the Sensor Web immediately present themselves, especially involving infrastructure protection. The properties of the Sensor Web make it ideal for sentinel security systems where a disturbance at one pod will be known by all. Moreover, the massively redundant connectivity of the macroinstrument makes the Sensor Web amenable to over-the-horizon monitoring of rail and highways.

Finally, the reactive capabilities of the Sensor Web to dynamic environments are only now being explored. Future systems may, for example, control ventilation during rescue operations based on changing atmospheric conditions and consequently free up additional labor that can be better applied to the actual rescue tasks at hand. Clearly, the situational awareness capability inherent in the Sensor Web can only increase with advances in the underlying technology and with no additional cost compared to that of more traditional, less capable wireless solutions.

## REFERENCES

1. Layman, Lloyd. (1953). *Fire Fighting Tactics*, National Fire Protection Association, Quincy, MA.
2. Delin, K. A. (2002). The Sensor Web: A macro-instrument for coordinated sensing. *Sensors* **2**, 270–285.
3. Koch, C., and Laurent, G. (1999). Complexity and the Nervous System. *Science* **284**, 96–98.
4. Delin, K. A. (2005). Sensor webs in the wild, *Wireless Sensor Networks: A Systems Perspective*, N. Bulusu, and S. Jha, Eds. Artech House, Norwood, MA, pp. 259–272.
5. Delin, K. A., Jackson, S. P., Johnson, D. W., Burleigh, S. C., Woodrow, R. R., McAuley, J. M., Dohm, J. M., Ip, F., Ferré, T. P. A., Rucker, D. F., and Baker, V. R. (2005). Environmental studies with the sensor web: principles and practice. *Sensors* **5**, 103–117.
6. See links at www.sensorwaresystems.com.

# Critical Information Infrastructure Protection

*Country Surveys*
*International Organization and Forums*

# CRITICAL INFORMATION INFRASTRUCTURE PROTECTION, OVERVIEW

MYRIAM DUNN CAVELTY
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 INTRODUCTION

For a number of years, policymakers at the highest levels have been expressing their concern that insecure information systems threaten economic growth and national security. As a result of these concerns, a complex and overlapping web of national, regional, and multilateral initiatives has emerged. Despite the sometimes substantial differences between these governmental protection policies, they offer a wealth of empirical material from which a variety of lessons can be distilled for the benefit of the international community.

## 2 BACKGROUND

The importance of protecting infrastructures has greatly increased in the global security political debate of late, due in particular to the traumatic terrorist attacks in New York and Washington (2001), Madrid (2004), and London (2005). In all of these cases, the perpetrators exploited elements of the civilian infrastructure for the purpose of indiscriminate murder. In the case of the 11 September 2001 attacks in the US, they used the transport infrastructure by turning airplanes into weapons. In Europe, trains, underground railways, and train stations as well as computers were targeted. This approach not only demonstrated the brutal nature of the "new terrorism", but also reinforced the view that traditional concepts of domestic security were no longer commensurate to contemporary requirements and needed to be adapted.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

Long before these attacks, the protection of strategically important installations in the domestic economic and social sphere had already been an important part of national defense concepts [1]. The term "Critical Infrastructure Protection" (CIP), however, refers to a broader concept with a distinctly new flavor. First of all, it is no longer restricted to concrete defense against immediate dangers or criminal prosecution after a crime has been committed, but increasingly refers to preventive security measures as well. Furthermore, contemporary modern societies have become significantly more vulnerable, and the spectrum of possible causes of disruptions and crises has become broader and more diffuse. This is why CIP has become a crystallization point for current security policy debates [2].

## 3 FROM THREATS TO RISKS

The genesis and establishment of the concept of CIP is the result of two interlinked and at times mutually reinforcing factors: The expansion of the threat spectrum after the Cold War, especially in terms of malicious actors and their capabilities on the one hand, and a new kind of vulnerability due to modern society's dependency on inherently insecure information systems on the other.

During the Cold War, threats were mainly perceived as arising from the aggressive intentions of states to achieve domination over other states. Among other things, the end of the Cold War also heralded the end of unambiguous threat perceptions: Following the disintegration of the Soviet Union, a variety of "new" threats were moved onto the security policy agendas of most countries [3]. The main distinguishing quality of these "new" challenges is the element of uncertainty that surrounds them: uncertainty concerning the identity and goals of potential adversaries, the time frame within which threats are likely to arise, the contingencies that might be imposed on the state by others, the capabilities against which one must prepare, and uncertainty about the type of challenge one had to prepare for [4]. Clearly, the notion of "threat" as something imminent, direct, and certain no longer accurately describes these challenges. Rather, they can be characterized as "risks", which are by definition indirect, unintended, uncertain, and situated in the future, since they only materialize when they occur in reality [5].

As a result of these diffuse risks and due to difficulties in locating and identifying enemies, part of the focus of security policies has shifted away from actors, capabilities, and motivations towards general vulnerabilities of entire societies. The catchphrase in this debate is "asymmetry", and the US military has been a driving force behind the shaping of this threat perception in the early 1990s [6]. The US as the only remaining superpower was seen as being predestined to become the target of asymmetric warfare. Specifically, those adversaries who were likely to fail against the American war machine might instead plan to bring the US to its knees by striking against vital points at home that are fundamental not to the military alone, but to the essential functioning of industrialized societies as a whole [7]. These points are generally defined as critical infrastructures (CI). They are deemed critical because their incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a nation.[1]

[1]The definition of what to include in a definition of critical infrastructure varies slightly from country to country. This Handbook shows in detail how each country defines the critical infrastructure and what sectors are included.

Fear of asymmetrical measures against such "soft targets" was aggravated by the second factor: the so-called information revolution. Most of the CI relies on a spectrum of software-based control systems for smooth, reliable, and continuous operation. In many cases, information and communication technologies (ICT) have become all-embracing, connecting other infrastructure systems and making them interrelated and interdependent. These technologies are in general regarded as inherently insecure: Security has never been a system design driver, and pressure to reduce time-to-market is intense, so that a further explosion of computer and network vulnerabilities is to be expected, leading to the emergence of infrastructures with in-built instability, critical points of failure, and extensive interdependencies [8]. At the same time, the spread of ICT was (and is) seen to make it much easier to attack asymmetrically, as big, specialized weapons systems or an army are no longer required. Borders, already porous in many ways in the real world, are nonexistent in cyberspace.

## 4 EVOLUTION OF THE CRITICAL (INFORMATION) INFRASTRUCTURE PROTECTION (CIIP) ISSUE

Commensurate with this threat perception, the US was the first nation to address the new vulnerability of the vital infrastructures in a broad and concerted effort. New risks in designated sectors[2] like information and communications, banking and finance, energy, physical distribution, and vital human services were identified by the Presidential Commission on Critical Infrastructure Protection (PCCIP) [9].[2] The PCCIP concluded in 1997 that the US was so dependent on these infrastructures that the government had to view them through the lens of a "national security focus", since serious consequences for the entire nation were to be expected if these elements were unavailable for any significant amount of time.

According to this approach, critical infrastructures should be understood to include material and IT assets, networks, services, and installations that, if disrupted or destroyed, would have a serious impact on the health, security, or economic well-being of citizens and the efficient functioning of a country's government. Such infrastructures could be damaged by structural threats as well as by intentional, actor-based attacks. The first risk category would, for example, include natural catastrophes, human-induced catastrophes (e.g., dam failure, nuclear reactor accident), personnel shortages through strikes or epidemics, organizational shortcomings due to technical or personal failures, human error, technical outages, and dependencies and supply shortages. In the second category, the spectrum of possible attackers is extensive, ranging from bored teenagers, disaffected or dissatisfied employees, organized crime, fanatics and terrorist cells, to hostile states.

There is an equally broad range of attack options, including hacker attacks as well as the physical destruction of civilian or military installations. The main focus of early CIP efforts was, however, directed towards the as-yet largely unknown risks emanating from cyberspace: The global information infrastructure appeared to facilitate anonymous attacks from anywhere in the world, while at the same time serving as a source for hacker tools for everyone. Based on this threat perception, a CIP policy crystallized under US President Bill Clinton that was largely directed towards information security. In many ways, other countries followed this lead with a similar focus on the information aspect.

[2]A sector is defined as "A group of industries or infrastructures which perform a similar function within a society", see: [9].

However, since the terrorist attacks of 11 September 2001, there has been a noticeable return of the classical threat concept to the CIP debate. Especially from the US point of view, efforts have been made since then to tackle a series of structural threats within the framework of an increasingly actor-oriented counter-terrorism strategy. In the US, CIP became a key component of Homeland Security and is currently discussed predominantly with a view to developing strategies against terrorism. In this context, the physical aspects of CIP have gained more attention, while the importance of information aspects has diminished slightly in comparison. In the meantime, this CIP focus on counterterrorism has also become a hallmark of recent debates in the EU, which has recently begun to develop a CIP policy that consists mainly of coordinating the measures adopted by member states. The same is true for other parts of the world.

## 5 DISTINCTION BETWEEN CIP AND CIIP

More than ten years after the beginning of the CIP debate, there still is little clarity with regard to a clear and stringent distinction between the two key terms "CIP" and "CIIP". In official publications, the term CIP is frequently used even if the document is only referring to the information aspects of the issue.

The reason for this is that the two cannot and should not be discussed as completely separate concepts. In our view, CIP is more than CIIP, but CIIP is an essential part of CIP. Focusing exclusively on cyber-threats while ignoring important traditional physical threats is just as dangerous as the neglect of the virtual dimension—what is needed is a sensible handling of both interrelated concepts. Nonetheless, there is at least one characteristic for distinguishing between the two: While CIP comprises all critical sectors of a nation's infrastructure, CIIP is only a subset of a comprehensive protection effort, as it focuses on measures to secure the critical *information* infrastructure. The definition of exactly what should be subsumed under CI, and what should come under the heading of CII, is another question: Generally, the CII is that part of the global or national information infrastructure that is essentially necessary for the continuity of a country's critical infrastructure services. The CII, to a large degree, consists of, but is not fully congruent with, the information and telecommunications sector, and includes components such as telecommunications, computers/software, the internet, satellites, fiber-optics, etc. The term is also used for the totality of interconnected computers and networks and their critical information flows.

Due to their role in interlinking various other infrastructures and also providing new ways in which they can be targeted, information infrastructures do play a very specific role in the debate, as we have already mentioned. They are regarded as the backbone of critical infrastructures, given that the uninterrupted exchange of data is essential to the operation of infrastructures in general and the services that they provide. Centralized SCADA (Supervisory, Control, and Data Acquisition) systems are widely employed to monitor and control infrastructures remotely. But SCADA-based systems are not secure: once-cloistered systems and networks are increasingly using off-the-shelf products and IP-based networking equipment, and require interconnection via the internet, which opens the door to attackers from the outside in addition to those on the inside.

As the information revolution is an ongoing and dynamic process that is fundamentally changing the fabric of security and society, continuing efforts to understand these changes are necessary. This requires research into information-age security issues, the

identification of new vulnerabilities, and new ways for countering threats efficiently and effectively. One such effort is the International CIIP Handbook, which aims to make a contribution towards this ambitious goal. The entire publication is available on the internet (http://www.crn.ethz.ch).

The CIIP Handbook focuses on national governmental efforts to protect critical (information) infrastructure as well as those of international organizations. The overall purpose of the International CIIP Handbook is to provide an overview of CII protection practices in a broad range of countries.

## 6 CRITICAL SECTORS

Specific countries identify critical sectors in their territory and provide definitions of CII and CIIP. Some countries, such as Australia, Canada, Germany, the Netherlands, New Zealand, the UK, or the US, provide clear definitions of what constitutes CIP, while other countries—for example Brazil, Korea, or Russia—, offer no definition. Everywhere, CIIP is understood more or less explicitly as a subset of CIP, including protection, detection, response, and recovery activities at both the physical and the virtual levels. However, a clear distinction between CIP and CIIP is lacking in most countries, and one finds both terms being used interchangeably. As was pointed out in the introduction, this reflects the continuing difficulties that arise from having to distinguish between physical and virtual aspects of critical infrastructures.

In designating critical sectors, all countries have followed the example of the Presidential Commission on Critical Infrastructure Protection (PCCIP), which was the first official publication to correlate critical infrastructures with specific business sectors or industries [10]. The choice of the "sector" as a unit of analysis is a pragmatic approach that roughly follows the boundaries of existing business/industry sectors. This approach reflects the fact that the majority of infrastructures is owned and operated by private actors. In addition, the decision on which infrastructures and sectors to include in the list of critical assets requires input from private-sector experts, besides experts and officials at various levels of government. More often than not, expert groups address the issue, either in larger or smaller groups [11]. A component or a whole infrastructure is usually defined as "critical" due to its strategic position within the whole system of infrastructures, and especially due to the interdependency between the component or the infrastructure and other infrastructures. However, as we show below, there is also a more symbolic understanding of criticality that influences the designation of critical assets.

It is broadly acknowledged, however, that the focus on sectors is too artificial to represent adequately the realities of complex infrastructure systems. For a more meaningful analysis, it is therefore deemed necessary to evolve beyond the conventional "sector"-based focus and to look at the services, the physical and electronic (information) flows, their role and function for society, and especially the core values that are delivered by the infrastructures. Therefore, experts groups often focus on four steps in the identification of what is critical: 1) critical sectors, 2) sub-sectors for each sector on the basis of organizational criteria, 3) core functions of the sub-sectors, and 4) resources necessary for the functioning of the sub-sectors [12].

Table 1 shows which country defines which sectors as critical. One must be careful, however, to avoid misleading comparisons: While for instance Australia, Canada, the Netherlands, the UK, and the US are very precise in identifying critical sectors and

**TABLE 1 Critical Sectors in Different Countries**

| Country Sector | AUS | A | BR | CAN | EST | F | FIN | GER | HUN | IND | IT | JAP | KOR | MAL | NL | NO | NZ | POL | RU | SE | SING | SPA | SWIT | UK | USA | TOTAL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Banking and Finance | √ | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | **24** |
| Central Government/Government Services | | √ | | √ | √ | √ | | √ | √ | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | √ | √ | √ | √ | **20** |
| Chemical and Nuclear Industry | | | | √ | | | | | | √ | | | | √ | √ | | | √ | | | | √ | √ | | √ | **8** |
| Emergency/Rescue Services | √ | | √ | √ | √ | √ | | | √ | √ | √ | | √ | √ | | √ | √ | √ | √ | | | | √ | √ | √ | **17** |
| Energy/Electricity | √ | √ | | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | √ | √ | √ | √ | | | √ | √ | √ | √ | √ | **21** |
| Food/Agriculture | √ | | | √ | √ | √ | √ | √ | √ | | √ | √ | | | √ | √ | | | | | √ | √ | √ | √ | √ | **16** |
| Health Services | √ | | √ | √ | √ | √ | √ | | √ | | √ | | | √ | √ | √ | | | | | √ | √ | √ | √ | √ | **16** |
| Information Services/Media | √ | √ | | | | √ | √ | | √ | | √ | | √ | | √ | √ | | | √ | √ | √ | | √ | | √ | **14** |
| Military Defense/ Army/Defense Facilities | | | | | | √ | | | √ | √ | | | √ | √ | | √ | | | √ | | | | | √ | √ | **9** |
| National Icons and Monuments | √ | | | | | | | | | | | | | | | | | | | | | | | | √ | **2** |
| Sewerage/Waste Management | √ | | | | | | | | | | √ | | | √ | √ | √ | | √ | | | | | √ | √ | √ | **9** |
| Telecommunications | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | √ | √ | √ | √ | √ | √ | √ | √ | | √ | √ | **22** |
| Transportation (land, sea, air)/Logistics/ Distribution | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | √ | | √ | √ | √ | √ | √ | √ | **24** |
| Water Infrastructure | | | | | √ | | | | | | | | | | √ | | | | | | | | | | √ | **3** |
| Water (Supply) | √ | | √ | | √ | √ | √ | √ | √ | | √ | √ | | √ | √ | √ | | | | √ | √ | √ | √ | √ | √ | **18** |

sub-sectors as well as products and services that these sectors provide, other countries, such as Austria, Brazil, Poland, Russia, have no official list of critical sectors.

Variations between countries can be explained by differences in conceptualizations of what is critical, but also by country-specific peculiarities and traditions. Sociopolitical factors as well as geographical and historical preconditions determine whether or not a sector is deemed to be critical.

The most frequently mentioned critical sectors in all countries are listed below. These are the core sectors of modern societies, and possibly the areas where a large-scale interruption would be most devastating:

- Banking and Finance,
- Central Government/Government Services,
- (Tele-) Communication/Information and Communication Technologies (ICT),
- Emergency/Rescue Services,
- Energy/Electricity,
- Health Services,
- Food,
- Transportation/Logistics/Distribution, and
- Water (Supply).

A comparison across time shows that the concept of criticality has undergone change, and that the criteria for determining which infrastructures qualify as critical have expanded over time; the PCCIP, for example, defined eight sectors as critical for the US, while today, critical infrastructures in the US already include 18 sectors.

We can thus distinguish between two differing, but interrelated perceptions of criticality [13]:

- *Criticality as systemic concept.* This approach assumes that an infrastructure or an infrastructure component is critical due to its structural position in the whole system of infrastructures, especially when it constitutes an important link between other infrastructures or sectors, and thus reinforces interdependencies.
- *Criticality as a symbolic concept.* This approach assumes that an infrastructure or an infrastructure component is inherently critical because of its role or function in society; the issue of interdependencies is secondary—the inherent symbolic meaning of certain infrastructures is enough to make them interesting targets.[3]

The symbolic understanding of criticality allows the integration of non-interdependent infrastructures as well as objects that are not man-made into the concept of critical infrastructures, including significant personalities or natural and historical sites with a strong symbolic character. Additionally, the symbolic approach allows essential assets to be defined more easily than the systemic one, because in a sociopolitical context, the defining element is not interdependency as such, but the role, relevance, and symbolic value of specific infrastructures [15].

The emphasis on the interconnectedness of various sectors, in connection with this symbolic understanding, creates a specific set of problems for decision-makers: Basically,

[3]For an example (critical assessment without interdependencies), see: [14].

everything is networked, and even a discrete event of little apparent significance could potentially set off unpredictable cascading effects throughout a large number of sectors. When the concept of criticality, and accordingly the scope of what is to be secured, is expanded from interconnected physical networks like the electrical grid and road networks to include everything with emotional significance, ranging from schools to national monuments, almost everything becomes potentially critical. In this situation, decision-makers must be careful not to follow the natural impulse to increase security ad absurdum and aim to protect everything that could possibly be at risk, because total protection will never be possible, and the effects on society will likely be negative. Prioritization must be based on careful risk assessment that comprises calculations of the likelihood of a given threat source displaying a particular potential vulnerability, and the resulting impact of that adverse event [16].

At the same time, one must be aware of the fact that current methodologies for analyzing CII—and first and foremost among them risk analysis—are insufficient in a number of ways: One of the major shortcomings is that the majority of them do not pass the "interdependency test". In other words, they fail to address, let alone understand, the issue of interdependencies and possible cascading effects. Besides, the available methods are either too sector-specific or too focused on single infrastructures and do not take into account the strategic, security-related, and economic importance of CII.[4] Moreover, there are both theoretical and practical difficulties involved in estimating the probabilities and consequences of high-impact, low-probability events—and this is the scenario we are dealing with in the context of CI(I)P. It also appears that there is no way of apolitically cataloguing objects, vulnerabilities, and threats on a strategic policy level, such as the economy at large, in a meaningful way.

Clearly, therefore, long-term research into CIP and CIIP matters is needed. A holistic and strategic threat and risk assessment at the physical, virtual, and psychological levels is the basis for a comprehensive protection and survival strategy, and will thus require a comprehensive and truly interdisciplinary research and development agenda that encompasses fields ranging from engineering and complexity sciences to policy research, political science, and sociology.

## 7 PAST AND PRESENT INITIATIVES AND POLICY

Many of the national CIIP efforts, including, specific committees, commissions, task forces, and working groups as well as key official reports and fundamental studies, and important national programs, were triggered or at least accelerated by the *Presidential Commission on Critical Infrastructure Protection* (PCCIP) set up by US President Bill Clinton in 1996, and to some extent by the preparations for anticipated problems on the threshold of the year 2000 (Y2K problem). This led to the establishment of (interdepartmental) committees, task forces, and working groups. Their mandate often included scenario work, the evaluation of a variety of measures, or assessments of early-warning systems. These efforts resulted in policy statements—such as recommendations for the establishment of independent organizations dealing with information society issues—and reports laying down basic CIIP policies.

[4]This issue is addressed in additional detail in by Myriam Dunn, who argues that shortcomings include the lack of data to support objective probability estimates, persistent value questions, and conflicting interests within complex decision-making processes [17].

In the aftermath of 11 September 2001 ("9/11"), several countries launched further initiatives to strengthen and allocate additional resources to their CIP/CIIP efforts. Prior to 9/11, for many people, critical infrastructure protection was synonymous with cyber-security. The attacks of 9/11, however, highlighted the fact that terrorists could cause enormous damage by attacking critical infrastructures directly and physically, and thus demonstrated the need to re-examine physical protection, especially in the US [18]. The perception that the cyber-dimension had been unduly prioritized before 9/11 subsequently led to a shift in focus from the virtual to the physical domain, and from CIIP to CIP. Subsequently, CIP became a key component of *Homeland Security* and is currently discussed predominantly with a view to developing strategies against Muslim terrorism. The physical aspects of CIP have been moved to the forefront, while the importance of information aspects has diminished. This CIP focus on counterterrorism has also become a hallmark of debates in the EU, which has recently begun to develop a CIP policy that consists mainly of coordinating the measures adopted by member states.

CIIP policies are at various stages of implementation—some are already being enforced, while others are just a set of suggestions—and come in various shapes and forms, ranging from a regulatory policy focus concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to the inclusion of cyber-security into more general counter-terrorism efforts. Most countries consider CIIP to be a national-security issue of some sort. In parallel, however, they often pursue a business continuity strategy under the "information society" label. The law enforcement/crime prevention perspective is also found in all countries. Furthermore, data protection issues are a major topic for civil rights groups. While all of the perspectives can be found in all countries, the emphasis given to one or more of the perspectives varies to a considerable degree.[5]

All countries examined have recognized the importance of public-private partnerships (PPP). Governments actively promote information-sharing with the private sector, since large parts of critical infrastructures are owned and operated by the business sector. Different types of such partnerships are emerging, including government-led partnerships, business-led partnerships, and joint public-private initiatives. In Switzerland, Korea, the UK, and the US, strong links have already been established between the private business community and various government organizations. One of the future challenges in many countries will be to achieve a balance between security requirements and business efficiency imperatives. Satisfying shareholders by maximizing company profits has often led to minimal security measures. This is because like many political leaders, business leaders tend to view cyber-attacks on infrastructures as a tolerable risk.

Despite the general consensus on the positive aspects of PPPs, their implementation remains difficult. It has been shown that it is relatively easy for the government and private actors in a PPP to agree on the existence of a problem and on the need for a remedy. It is, however, much harder to agree on actual measures to be taken, on the actors responsible for implementing them, on the party that will assume legal responsibility for such measures, and on the party that will bear the costs for implementing them [20].

[5]This issue is also addressed by Isabelle Abele-Wigert, who shows how practical and academic dialog is hampered by vastly differing terminology and viewpoints of what constitutes the problem [19].

## 8 ORGANIZATIONAL OVERVIEW

Only in a few countries central governmental organizations have been created to deal specifically with CIIP. For example, the US, France, Switzerland, Singapore, and Korea have all made provisions in this regard. Mostly, responsibility lies with multiple authorities and organizations in different governmental departments. Very often, responsibility for CIIP protection is given to well-established organizations or agencies that appear suitable for the task. Depending on their key assignment, these agencies bring their own perspective to bear on the problem and shape policy accordingly.

In countries such as France and New Zealand, CIIP efforts are mainly led by the defense establishment, whereas in other countries, such as the UK or Switzerland, approaches to CIIP are jointly led by the business community and public agencies. Furthermore, in Australia as well as in the US and New Zealand, CIIP is integrated into the overall counterterrorism efforts, where the intelligence community plays an important role. In India, Korea, Japan, Singapore, and Estonia, the fostering of the information society and economic growth through safe information infrastructures is at the forefront.

The establishment of these organizational units and their location within the government structures are influenced by various factors such as civil defense tradition, the allocation of resources, historical experience, and the general threat perception of key actors in the policy domain. Depending on their influence or on the resources at hand, various key players shape the issue in accordance with their view of the problem. Different groups, whether they be private, public, or a mixture of both, do not usually agree on the exact nature of the problem or on what assets need to be protected with which measures. There are at least four (overlapping) typologies for how CIIP issues are viewed: an IT-security perspective, an economic perspective, a law enforcement perspective, and a national-security perspective. While all typologies can be found in all countries, the emphasis given to one or more of them varies to a considerable degree. Ultimately, the dominance of one or several typologies has implications for the shape of the protection policies and, subsequently, for determining appropriate protection efforts, goals, strategies, and instruments for solving problems.

In the end, the distribution of resources and the technical and social means for countering the risk are important for the outcome. We can observe that the different actors involved—ranging from government agencies and the technology community to insurance companies—have divergent interests and compete with one another by means of scenarios describing how they believe the threat will manifest itself in the future [21]. Furthermore, the selection of policies seems to depend largely upon two factors: One is the varying degree to which resources are available to the different groups. The other factor is the impact of cultural and legal norms, because they restrict the number of potential strategies available for selection [22]. In general, we can identify two influential discourses: On the one hand, law enforcement agencies emphasize their view of the risk as "computer crime", while on the other hand, the private sector running the infrastructures perceives the risk mainly as a local, technical problem or in terms of economic costs [23]. Because the technology generating the risk makes it very difficult to fight potential attackers in advance, protective measures focus on preventive strategies and on trying to minimize the impact of an attack when it occurs. Here, the infrastructure providers are in a strong position, because they alone are in the position to install technical safeguards for IT security at the level of individual infrastructures.

Norms are also important in selecting the strategies. Most importantly, the general aversion of the new economy to government regulation as well as legal restrictions limits

the choice of strategies [24]. Besides these cultural differences with regard to strategy, the nature of cyber-attacks naturally positions law enforcement at the forefront: It is often impossible to determine at the outset whether an intrusion is an act of vandalism, computer crime, terrorism, foreign intelligence activity, or some form of strategic attack. The only way to determine the source, nature, and scope of the incident is to investigate. The authority to investigate such matters and to obtain the necessary court orders or subpoenas clearly resides with law enforcement. As a consequence of the nature of cyber-threats, the cyber-crime/law enforcement paradigm is emerging as the strongest viewpoint in most countries.

## 9 EARLY WARNING AND PUBLIC OUTREACH

The earlier a potential risk is identified, the greater the chance to act in a timely, resource-efficient, and strategically adequate manner. Therefore, timely warning of attacks is an indispensable component of ensuring that a breakdown of important infrastructure, or even only of certain components of ICT, will be limited to an incident that is short, rare, controllable, geographically isolated, or with as little consequences as possible for the national economy and security.

Early-warning systems are designed for the following purposes: understanding and mapping the hazard; monitoring and forecasting impending events; processing and disseminating understandable warnings to political authorities and the population; and undertaking appropriate and timely actions in response to the warnings. In CIIP, early warning is focused mainly on IT security incidents. The general trend in CIIP early warning points towards establishing central contact points for the security of information systems and networks. Among the existing early-warning organizations are various forms of *Computer Emergency Response Teams* (CERTs), e.g., special CERTs for government departments, CERTs for small and medium-sized businesses, CERTs for specific sectors, and others. CERT functions include handling of computer security incidents and vulnerabilities or reducing the probability of successful attacks by publishing security alerts.[6] Internationally, CERTs primarily exchange information at the Forum of Incident Response and Security Teams (FIRST).

In some countries, permanent analysis and intelligence centers have been developed in order to make tactical or strategic information available to the decision-makers within the public and private sectors more efficiently. Tasks of early-warning system structures include analysis and monitoring of the situation as well as the assessment of technological developments. Examples can be found in Canada (Integrated Threat Assessment Center) [26]. and in Switzerland (Reporting and Analysis Center for Information Assurance, MELANI) [27].

Often, these entities manage outreach, cyber-security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders. Generally, many private enterprises, public entities, and home users lack the resources to manage cyber-security risks adequately. Many entrepreneurs and home users are unaware of the extent to which their individual cyber-security preparedness affects overall security, and internet users must be made aware of the importance of sound cyber-security practices and require more user-friendly tools to

[6]The issue is further addressed by Thomas Holderegger, who examines early-warning players in the CIIP sector and specifies their tasks and responsibilities, with a specific focus on the role of the nation state [25].

implement them. Public outreach efforts therefore entail cataloguing existing best practices, developing strategies to market those practices to specific audiences, creating incentive plans to ensure acceptance of those practices, contributing to the development of a national advertising campaign, and developing a strategy to communicate the importance of cyber-security and their role in enhancing it to public and private CEOs across the country.

## 10 LEGAL ISSUES

Although many countries have been concerned with the protection and security of information (infrastructures) and related legislation for some years, they have begun to review and adapt their cyber-security legislation after 9/11. Because national laws are developed autonomously, some countries have preferred to amend their penal or criminal code, whereas others have passed specific laws on cyber-crime.

The following is an overview of important common issues currently discussed in the context of legislation procedures:

- Data protection and security in electronic communications (including data transmission, safe data storage, etc.);
- IT security and information security requirements;
- Fraudulent use of computer and computer systems, damage to or forgery of data, and similar offences;
- Protection of personal data and privacy;
- Identification and digital signatures;
- Responsibilities in e-commerce and e-business;
- International harmonization of cyber-crime law;
- Minimum standards of information security for (e-)governments, service providers, and operators, including the implementation of security standards such as BS7799, the code of practice for information security management ISO/IEC 17799, the Common Criteria for Information Technology Security Evaluation ISO/IEC 15408, and others;
- Public key infrastructure and its regulation.

Across all boundaries, there are two main factors that influence and sometimes even hinder efficient law enforcement—one with a national, the other with an international dimension:

- *Lack of know-how or of functioning legal institutions.* Even if a country has strict laws and prohibits many practices, the enforcement of such laws is often difficult. Frequently, the necessary means to prosecute misdemeanors effectively are lacking due to resource problems, inexistent or emerging cyber-crime units, or a lack of supportive legislation, such as the storing of rendition data [28].
- *Lack or disparity of legal codes.* While most crimes, such as theft, burglary, and the like are punishable offenses in almost every country of the world, some rather grave disparities still remain in the area of cyber-crime [29].

## 11 INTERNATIONAL ISSUES

From the discussion of legal issues, it becomes obvious that like other security issues, the vulnerability of modern societies—caused by dependency on a spectrum of highly interdependent information systems—has global origins and implications. To begin with, the information infrastructure transcends territorial boundaries, so that information assets that are vital to the national security and the essential functioning of the economy of one state may reside outside of its sphere of influence on the territory of other nation-states. Additionally, "cyberspace"—a huge, tangled, diverse, and universal blanket of electronic interchange—is present wherever there are telephone wires, cables, computers, or electromagnetic waves, a fact that severely curtails the ability of individual states to regulate or control it alone. Any adequate protection policy that extends to strategically important information infrastructures will thus ultimately require transnational solutions.

There are four possible categories of initiatives that may be launched by multilateral actors: deterrence, prevention, detection, and reaction.

- *Deterrence.* or the focus on the use of multilateral cyber-crime legislation: Multilateral initiatives to deter the malicious use of cyberspace include initiatives a) to harmonize cyber-crime legislation and to promote tougher criminal penalties (e.g. the Council of Europe Convention on Cybercrime) [30], and b) to improve e-commerce legislation (e.g., the efforts of the United Nations Commission on International Trade Law (UNCITRAL) for electronic commerce) [31].
- *Prevention.* or the design and use of more secure systems and better security management, and the promotion of more security mechanisms: Multilateral initiatives to prevent the malicious use of cyberspace center around a) promoting the design and use of more secure information systems (e.g., the Common Criteria Project) [32]; b) improving information security management in both public and private sectors (e.g., the ISO and OECD standards and guidelines initiatives) [33]; c) legal and technological initiatives, such as the promotion of security mechanisms (e.g., electronic signature legislation in Europe).
- *Detection.* or cooperative policing mechanisms and early warning of attacks: Multilateral initiatives to detect the malicious use of cyberspace include a) the creation of enhanced cooperative policing mechanisms (e.g., the G-8 national points of contact for cyber-crime); and b) early warning through information exchange with the aim of providing early warning of cyber-attacks by exchanging information between the public and private sectors (e.g., US Information Sharing & Analysis Centers, the European Early Warning & Information System, and the European Network and Information Security Agency (ENISA)).
- *Reaction.* or the design of stronger information infrastructures, crisis management programs, and policing and justice efforts: Multilateral initiatives to react to the malicious use of cyberspace include a) efforts to design robust and survivable information infrastructures; b) the development of crisis management systems; and c) improvement in the coordination of policing and criminal justice efforts.

The most important legislative instrument in this area is the Council of Europe Cybercrime Convention (CoC). This convention is the first international treaty on crimes committed via the internet and other computer networks. Its main objective is to pursue a common law enforcement policy aimed at the protection of society against cyber-crime,

especially by adopting appropriate legislation and fostering international cooperation [34]. An additional protocol to the CoC outlaws racist and xenophobic acts committed through computer systems.

While other politically powerful entities such as the G8 also try to foster collaboration and a more efficient exchange of information when it comes to cyber-crime and terrorism, the CoC goes one step further. It lays out a framework for future collaboration between the prosecution services of the signature states. It achieves this mainly by harmonizing the penal codes of the CoC signatory states. As a result, crimes such as hacking, data theft, and distribution of pedophile and xenophobic material, etc., will be regarded as illegal actions per se, thus resolving the problem of legal disparities between nations that was mentioned above. This also allows the authorities to speed up the process of international prosecution. Since certain activities are defined as illegal by all CoC member states, the sometimes long and painful task of cross-checking supposed criminal charges committed in a foreign country becomes obsolete if the offence is already included in the national penal code. Consequently, reaction times will be shortened and the parties to the CoC will establish a round-the-clock network within their countries to handle aid requests that demand swift intervention [35]. While the implementation of the CoC will most likely be a slow and sometimes thorny process, the idea of finding a common denominator and harmonizing the response to at least some of the most crucial problems is certainly a step in the right direction.

## REFERENCES


1. Luiijf, E. A. M., Burger H. H., and Klaver M. H. A. (2008). Critical infrastructure protection in The Netherlands: a quick-scan. In *EICAR Conference Best Paper Proceedings 2003*, U. E. Gattiker, P. Pedersen, and K. Petersen, Eds. http://cipp.gmu.edu/archive/2_Netherlands CIdefpaper_2003.pdf [last accessed in June 2008].
2. Dunn, C., and Kristensen, S. K. (2008). *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security*, Routledge, London.
3. Buzan, B., Wæver, O., and de Wilde, J. (1998). *Security: A New Framework for Analysis*, Lynne Rienner, Boulder.
4. Goldman, E. O. (2001). New threats, new identities and new ways of war: the sources of change in national security doctrine. *J. Strateg. Stud.* **24**, 12–42.
5. (a) Bailes, A. J. K. (2007). Introduction: a world of risk. In *SIPRI Yearbook 2007: Armaments, Disarmament and International Security*, pp. 1–20; (b) Beck, U. (1999). *World Risk Society*, Polity Press, Cambridge.
6. Rattray, G. (2001). *Strategic Warfare in Cyberspace*, MIT Press, Cambridge.
7. Berkowitz, B. D. (1997). Warfare in the information age. In *In Athena's Camp: Preparing for Conflict in the Information Age*, A. John, and R. David, Eds. RAND, Santa Monica, pp. 175–190.
8. Rathmell, A. (2001). Controlling computer network operations. *Infor. Secur. Int. J.* **7**, 121–144.
9. President's Commission on Critical Infrastructure Protection (PCCIP) (2008). *Critical Foundations: Protecting America's Infrastructures*, Washington, October 1997: Appendix B, Glossary, B-3. http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf [last accessed in June 2008]. Publication quoted in the following as PCCIP.
10. President's Commission on Critical Infrastructure Protection (PCCIP) (2008). *Critical Foundations: Protecting America's Infrastructures*, Washington, October 1997. http://www.ihs.gov/misc/links_gateway/download.cfm?doc_id=327&app_dir_id=4&doc_file=PCCIP_Report.pdf [last accessed in June 2008]. Publication quoted in the following as PCCIP.

11. Dunn, M. (2004). Part II: analysis of methods and models for CII assessment. In *The International Critical Information Infrastructure Protection (CIIP) Handbook 2004*, M. Dunn, and W. Isabelle, Eds. Center for Security Studies, Zurich, pp. 219–297.
12. Dunn, M. (2004). Part II: analysis of methods and models for CII assessment. In *The International Critical Information Infrastructure Protection (CIIP) Handbook 2004*, M. Dunn, and W. Isabelle, Eds. Center for Security Studies, Zurich, p. 227f.
13. Metzger, J. (2004). The concept of critical infrastructure protection (CIP). In *Business and Security: Public-Private Sector Relationships in a New Security Environment*, A. J. K. Bailes, and F. Isabelle, Eds. Oxford University Press, Oxford, pp. 197–209.
14. United States General Accounting Office (GAO) (2008). Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations; House Committee on Government Reform. *Homeland Security: Key Elements of a Risk Management*, Statement of Raymond J. Decker, Director Defense Capabilities and Management. 12 October 2001, p. 6. http://www.gao.gov/new.items/d02150t.pdf [last accessed in June 2008].
15. Metzger, J., op. cit.
16. Stoneburner, G., Goguen, A., and Feringa, A. (2002). Risk management guide for information technology systems. In *Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-30. US Government Printing Office, Washington, p. 8. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf [last accessed in June 2008].
17. Dunn, M. (2006). Understanding critical information infrastructures: an elusive quest. In *International CIIP Handbook 2006. Analyzing Issues, Challenges, and Prospects*, M. Dunn, and V. Mauer, Eds. Center for Security Studies, Zurich, Vol. II, pp. 27–53.
18. Moteff, J. (2005). Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences. CRS Report for Congress. February 4, p. 3.
19. Wigert, I. (2006). Challenges governments face in the field of critical information infrastructure protection (CIIP): stakeholders and perspectives. In *International CIIP Handbook 2006, Analyzing Issues, Challenges, and Prospects*, M. Dunn, and V. Mauer, Eds. Center for Security Studies, Zurich, Vol. II, pp. 55–68.
20. Andersson, J. J., and Malm, A. (2006). Public-private partnerships and the challenge of critical infrastructure protection. In *International CIIP Handbook 2006, Analyzing Issues, Challenges, and Prospects*, M. Dunn, and V. Mauer, Eds. Center for Security Studes, Zurich, Vol. II, pp. 139–167.
21. (a) Bendrath, R. (2003). The American cyber-angst and the real world—any link? In *Bombs and Bandwidth: The Emerging Relationship Between IT and Security*, R. Latham, Ed. The New Press, New York, pp. 49–73; (b) Bendrath, R. (2001). The cyberwar debate: perception and politics in US critical infrastructure protection. In *The Internet and the Changing Face of International Relations and Security*, Information & Security: An International Journal. A. Wenger, Ed. Vol. 7, pp. 80–103.
22. Dunn, M. (2004). Cyber-threats and countermeasures: towards an analytical framework for explaining threat politics in the information age. *Conference paper, SGIR Fifth Pan-European IR Conference*. The Hague, 10 September 2004.
23. Bendrath, R. The cyberwar debate, op. cit., p. 97.
24. Bendrath, R. The cyberwar debate, op. cit., p. 98.
25. Holderegger, T. (2006). The aspect of early warning in critical information infrastructure protection (CIIP). In *International CIIP Handbook 2006. Vol. II. Analyzing Issues, Challenges, and Prospects*, M. Dunn, and V. Mauer, Eds. Center for Security Studies, Zurich, pp. 111–135.
26. http://www.itac-ciem.gc.ca/index-eng.asp, 2008.
27. http://www.melani.admin.ch/, 2008.

28. Goodman, S. E., Hassebroek, P. B., King, D., and Azment, A. (2002). International coordination to increase the security of critical network infrastructures. Document CNI/04. *Paper presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures*. Seoul, 20–22 May 2002.
29. Gelbstein, E., and Kamal, A. (2002). *Information Insecurity. A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security*, United Nations ICT Task Force and United Nations Institute for Training and Research, New York, November 2002. http://www.un.int/unitar/patit/dev/old%20site/curriculum/Information_Insecurity_Second_Edition_PDF.pdf.
30. Council of Europe (2008). *Convention on Cybercrime*, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm [last accessed in June 2008].
31. http://www.uncitral.org/english/workinggroups/wg_ec/index.htm, 2008.
32. http://www.commoncriteriaportal.org [last accessed in June 2008].
33. (a) The International Organization for Standardization ISO (2000). *Developed a code of practice for information security management (ISO/IEC 17799:2000)*. http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html; (b) The Organisation for Economic Cooperation and Development (OECD) (2008). *Promotes a "Culture of Security" for Information Systems and Networks*, http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html [last accessed in June 2008].
34. *Convention on Cybercrime*, op. cit.
35. Taylor, G. (2008). *The Council of Europe Cybercrime Convention. A Civil Liberties Perspective*, http://www.crime-research.org/library/CoE_Cybercrime.html [last accessed in June 2008].

# AUSTRALIA

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Australia takes an all-hazards approach to the protection of critical infrastructures, whether information-based or not. The definition of critical infrastructure (CI) accepted

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

by Australia is "those physical facilities, supply chains, information technologies and communication networks that, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the social or economic well-being of the nation or affect Australia's ability to conduct national defense and ensure national security" [1]. The national information infrastructure (NII) is a subset of the critical infrastructure. As in many countries, the majority of the elements of the critical infrastructure are owned or operated as commercial enterprises.

In Australia, the CIP program is led by the Attorney-General's Department (AGD), primarily through the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN). The TISN brings together the nine sectors considered to be critical to Australia. These are [2]:

- Communications (Telecommunications (Phone, Fax, Internet, Cable, Satellites) and Electronic Mass Communications),
- Energy (Gas, Petroleum Fuels, Refineries, Pipelines, Electricity Generation and Transmission),
- Banking and Finance (Banking, Finance, and Trading Exchanges),
- Food Supply (Bulk Production, Storage, and Distribution),
- Emergency Services,
- Health (Hospitals, Public Health, and Research and Development Laboratories),
- Mass Gatherings (Icons (e.g., Sydney Opera House) and places of mass gatherings)
- Transport (Air Traffic Control, Road, Sea, Rail, and Inter-modal (Cargo Distribution Centers)),
- Utilities (Water, Waste Water, and Waste Management).

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

National Counter-Terrorism Plan (2003, revised 2005)
E-Security National Policy Statement (2007)

### 2.1 Guiding Principles of Australia's CIP Policy

Critical Infrastructure Protection (CIP) requires the active participation of the owners and operators of infrastructure, regulators, professional bodies, and industry associations, in cooperation with all levels of government, and the public. To ensure this cooperation and coordination, all of these participants should commit to the following set of common, fundamental principles of CIP [3]. These principles are to be read as a whole, as each sets the context for the one following.

- CIP is centered on the need to minimize risks to public health, safety, and confidence, to ensure Australia's economic security and maintain the country's international competitiveness, and to ensure the continuity of government and its services;
- The objectives of CIP are to identify critical infrastructure, analyze vulnerability and interdependence, and protect Australia from, and prepare for, all hazards;

- Because all critical infrastructures cannot be protected from all threats, appropriate risk management techniques should be used to determine their relative severity and duration, the level of protective security, and to set priorities for the allocation of resources and the application of the best mitigation strategies for business continuity;
- The responsibility for managing risk within physical facilities, supply chains, information technologies, and communication networks primarily rests with the owners and operators;
- CIP needs to be undertaken with an all-hazards approach, with full consideration of interdependencies between businesses, sectors, jurisdictions, and government agencies;
- CIP requires a consistent cooperative partnership between the owners and operators of critical infrastructure and governments;
- The sharing of information relating to threats and vulnerabilities will assist governments, and owners and operators of critical infrastructure, in managing risk better;
- Care should be taken, when referring to national security threats to critical infrastructure, including terrorism, to avoid causing undue concern in the Australian domestic community and to potential tourists and investors overseas;
- Stronger research and analysis capabilities can ensure that risk mitigation strategies are tailored to meet Australia's unique critical infrastructure circumstances.

### 2.2 CIP and Counter-Terrorism Policy

The National Counter-Terrorism Committee (NCTC) has primary responsibility for the oversight of the protection of critical infrastructures from terrorism. In general, however, CIP is a shared responsibility of the corporate sector and the Australian federal, state, and territory governments. In the field of CIIP, the Attorney-General's Department coordinates arrangements [4].

The Australian government takes actions in the following fields:

- Identifying Australia's critical infrastructure and determining broad areas of risk;
- Assisting businesses in mitigating their risk through business-government partnerships, e.g., the Trusted Information Sharing Network (TISN) and Infrastructure Assurance Advisory Groups (IAAGs), and through state and territory governments;
- Promoting domestic and international best practices in CIP.

### 2.3 e-Security

Resulting from a review of the e-Security environment, the former government released an e-Security national policy statement in 2007. The former government followed this up with funding of AUS$74 million over four years for e-Security initiatives [5]. The catalyst for this action was the increasing interconnectedness of the electronic environment and the need to address e-Security threats to different segments on the Australian economy holistically [6]. In consequence, the agenda appoints a new interdepartmental committee with responsibility across the entire range of government, the E-Security Policy and Coordination (ESPaC), to coordinate e-Security policy throughout the different areas.

In order to assign the roles and responsibilities of relevant Australian government agencies clearly, three priorities are defined by the agenda:

- Reducing the e-Security risk to Australian government information and communication systems;
- Reducing the e-Security risk to Australia's national critical infrastructure;
- Enhancing the protection of home users and SMEs from electronic attacks and frauds.

These new priorities and the focus on the interconnectivity of the different areas have had a considerable impact on the administrative arrangements in the field of e-Security (see chapter Organizational Overview). A second departure from the 2001 agenda is the emphasis on initiatives to address sophisticated and targeted attacks that are difficult to detect and fight by conventional measures. Thirdly, it has been decided to review the new agenda every two years instead of every four years, given the rapid evolvement of new e-Security threats [7].

One of the major initiatives was a significant expansion of the Australian Government Computer Emergency Readiness Team [8] (GovCERT.au) within the AGD.

## 3 ORGANIZATIONAL OVERVIEW

In Australia, the CIP program is led by the Attorney-General's Department (AGD), in close collaboration with the owners and operators of critical infrastructures. CIP efforts are primarily coordinated through the Trusted Information Sharing Network for critical infrastructure protection (TISN) [3], which provides the framework for public-private collaboration in the field of CIP and CIIP (see the chapter on Organizational Overview).

The AGD collaborates also closely with other public agencies. In 2007, as a result of the budgetary announcement by the former government and the revised E-Security National Agenda, the role and responsibilities of several public agencies increased. The most important administrative change concerned the establishment of a whole of government E-Security Policy and Coordination Committee (ESPaC) in line with the push towards a holistic approach to addressing the security of the electronic environment. While the newly created ESPaC is a standing interdepartmental committee with responsibility for e-Security policy, all agencies involved in CIIP collaborate closely. For instance, the Defence Signals Directorate (DSD), the Australian Security Intelligence Organisation (ASIO), and the Australian Federal Police (AFP) are engaged in formal Joint Operating Arrangements supporting threat and vulnerability assessment and the analysis of, and the response to, critical incidents affecting the integrity of Australia's information infrastructure.

### 3.1 Public Agencies

***3.1.1 Attorney-General's Department (AGD).*** Attorney-General's Department (AGD), provides expert support to the Government in the maintenance and improvement of Australia's system of law and justice and its national security and emergency management systems. The mission of the Attorney-General's Department is achieving a just and secure society [9].

Within the department, the Security and Critical Infrastructure Division (SCID) is responsible for the administration and development of legislation and the provision of

legal and policy advice with respect to counter-terrorism, national security, telecommunications interception and critical infrastructure protection. The Division coordinates Australian Government activities in critical infrastructure protection, building on the work to protect Australia's National Information Infrastructure that began in 1999, and provides policy and legal policy advice on these issues. The division performs a leadership role in the development of a business-government partnership for critical infrastructure protection with Australian industry [10].

***3.1.2 E-Security Policy and Coordination (ESPaC) Committee.*** The E-Security Policy and Coordination (ESPaC) Committee was established in 2007 and replaced two former committees—the Electronic Security Coordination Group (ESCG), run by the Department of Broadband, Communications and the Digital Economy, and the Information Infrastructure Protection Group, run by the AGD. The incorporation of these agencies into the new ESPaC committee "ensures effective e-security coordination across the three areas of critical infrastructure, home and SMEs, and government" [3].

The tasks of the ESPaC Committee correspond to those of its predecessors (the Electronic Security Coordination Group and the Information Infrastructure Protection Group): awareness raising, promoting e-Security skills, advancing research and development, and coordinating the government policies related to e-Security.

The ESPaC Committee is chaired by the AGD and is comprised of representatives from the following government agencies: the Australian Communications and Media Authority; the Australian Government Information Management Office; the Australian Federal Police; the Australian Security Intelligence Organization; the Department of Broadband, Communications and the Digital Economy; the Defence Signal Directorate; the Department of Defence; the Department of the Prime Minister and Cabinet; and the Office of National Assessments.

The Information Infrastructure Protection Group (IIPG) was an interdepartmental committee of the Australian government responsible for providing policy coordination and/or technical response in relation to threats to the National Information Infrastructure (NII). It was replaced by the ESPaC [11].

***3.1.3 Department of Broadband, Communications and the Digital Economy (DBCDE).*** The Department of Broadband, Communications and the Digital Economy (DBCDE), formerly the Department of Communications, Information Technology and the Arts, (DCITA) participates in the Australian government's CIP activities through the Trusted Information Sharing Network (TISN). It chairs and provides secretariat support to the IT Security Expert Advisory Group (ITSEAG). The ITSEAG provides advice to the TISN on current and emerging security issues affecting owners and operators of critical infrastructure, including:

- Voice over Internet Protocol (VoIP) enterprise systems,
- Supervisory Control and Data Acquisition (SCADA) systems,
- Wireless services.

DBCDE also provides the secretariat for the Communications Sector Infrastructure Assurance Advisory Group (CSIAAG) of the TISN, which has developed an all-hazards risk management framework for the national critical communications infrastructure [12].

***3.1.4 Australian Government Computer Emergency Readiness Team (GovCERT.au).*** GovCERT.au was established in 2005 within the Attorney-General's Department to enhance Australia's preparedness with regard to attacks on information security. GovCERT.au is responsible for:

- Liaising with the Computer Emergency Response Teams of foreign governments;
- Coordinating inquiries from foreign governments about cyber-security issues that affect Australia's critical infrastructure and business sector;
- Coordinating the Australian government's policy on how to prepare for, respond to, and recover from computer emergencies affecting the national information infrastructure;
- Managing the Australian government's Computer Network Vulnerability Assessment Program [13], which provides cash grants to critical infrastructure owners and operators to undertake security assessments of their IT systems and networks, including physical and personnel security aspects relating to those networks.

GovCERT.au is the Australian government's point of contact for foreign governments on Computer Emergency Response issues affecting the national information infrastructure.

GovCERT.au receives information about IT security issues from foreign governments that needs to be passed on to Australian critical infrastructure owners and operators. GovCERT.au does not handle day-to-day computer incidents [14].

***3.1.5 Australian Government Information Management Office (AGIMO).*** The Australian Government Information Management Office (AGIMO), part of the Department of Finance and Administration, provides strategic advice, activities, and representation relating to the application of ICT to government administration, information, and services.

AGIMO's functions and responsibilities include:

- Promoting improved government services through technical interoperability and the integration of business processes across Australian government services and with state/territory and local authorities;
- Developing and enhancing government e-procurement processes;
- Promoting comprehensive telecommunications arrangements for the entire government;
- Identifying and promoting the development of the ICT infrastructure necessary to implement emerging strategies for the entire government;
- Developing an e-Government Authentication Framework to assist people in verifying electronic communications.

In cooperation with other government bodies, AGIMO manages international contacts and represents Australia in world forums on ICT-related issues. AGIMO also manages the .gov.au domain in consultation with state and territory governments [15].

***3.1.6 Defence Signals Directorate (DSD).*** The Defence Signals Directorate (DSD) is Australia's national authority on information security and signals intelligence. DSD plays an integral role in the protection of Australia's official communications and information systems. It does so by providing expert assistance to Australian agencies in relation

to cryptography, network security, and the development of guidelines and policies on information security.

The activities of the DSD's Information Security Group (INFOSEC) include information and incident collection, analysis and warning services, setting awareness and certification standards, and defensive measures, including protective security measures, response arrangements, and contingency planning. In addition to its support for Australian government departments and authorities, INFOSEC also plays an important role working with industry towards the development of new cryptographic products [16].

***3.1.7 Australian Security Intelligence Organisation (ASIO).*** The Australian Security Intelligence Organisation (ASIO) is Australia's national security service. Its functions are set out in the Australian Security Intelligence Organisation Act 1979 (the ASIO Act). ASIO's main role is to gather information and produce intelligence that will enable it to warn the government about activities or situations that might endanger Australia's national security. The ASIO Act defines security as the protection of Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defense system, and acts of foreign interference. Some of these terms are further defined in the ASIO Act [17].

***3.1.8 The Australian Federal Police (AFP).*** The introduction of the Cybercrime Act (2001) prompted the Australian Federal Police (AFP) to join forces with state and territory police to create a national organization to address the threat of cyber-crime. The distinction between cyber-crime and cyber-terrorism is blurred because many of the tools and techniques are common to both activities. Consequently, the creation of the Australian High Tech Crime Centre (AHTCC) was a major and important CIIP measure. The AHTCC provides a national coordinated approach to dealing with instances of high-tech crime affecting the Australian jurisdiction, including the investigation of electronic attacks against the National Information Infrastructure [18].

## 3.2 Public-Private Partnerships

***3.2.1 The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN).*** Because the vast majority of the critical infrastructure is owned or operated on a commercial basis, public-private collaboration is a key component of CIIP. The Attorney-General's Department writes: "As with most businesses, those who own or run critical infrastructure know the best way to protect it, how to manage an incident and how to get things up and running again. While the Government believes that regulations are not the best way to protect all types of critical infrastructure in some areas regulations are needed for special reasons. For example, in the transport industry regulations are needed so Australia can meet international obligations" [19]. The Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) is the most important initiative to encourage the cooperation between the private and the public actors.

Building on the recommendations of the first Consultative Industry Forum (CIF) [20], the former government announced the formation of the Business-Government Task Force on Critical Infrastructure. The task force recommended replacing the CIF with a "learning network" to share information about critical infrastructure protection. In 2002, the government announced the creation of a Trusted Information-Sharing Network for Critical Infrastructure Protection (TISN) [21].

The TISN is organized according to Australia's critical infrastructure sectors. Each of the sector groups, the so-called Infrastructure Assurance Advisory Groups (IAAGs), is chaired by a representative of the critical infrastructure from that sector [3]. Membership is restricted to owners and operators of CI and government. Logistical support for the group is provided by government agencies that deal with the sector on a day to day basis, e.g., the Health Department with the Health group. The Attorney-General's Department provides support to Emergency Services, Banking, and Mass Gatherings. Each sector group is represented by their chair at the Critical Infrastructure Advisory Council (CIAC). The CIAC reports to the attorney-general. It is a way for critical infrastructure owners and operators to communicate with the Australian government at a high level. It also feeds into Australia's counter-terrorism arrangements.

Two permanent Expert Advisory Groups have been set up to advise the Critical Infrastructure Advisory Council—one for IT Security and the other for Critical Infrastructure Protection Futures [22].

## 4 EARLY WARNING AND PUBLIC OUTREACH

There are two key organizations that provide comprehensive early-warning services for cyber-attacks in Australia. The Defence Signals Directorate (DSD) has the remit to assist federal and state/territory IT networks, and the Australian Computer Emergency Response Team (AusCERT) provides some similar services to private sector operators of CI. In addition, the Australian government has launched the OnSecure website, run by the DSD.

### 4.1 Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS)

The DSD manages the Information Security Incident Detection Reporting and Analysis Scheme (ISIDRAS). The function of the ISIDRAS is the collection of information on security incidents that affect the security or operability of government computer and communication systems.

The ISIDRAS facilitates high-level analysis of information security incidents with the aim of improving knowledge of both threats and vulnerabilities to Australian government information systems and about how to protect these systems more effectively. ISIDRAS provides regular reporting of incidents. Government agencies that have detected a security breach can report the incident by completing an Australian Government IT Security Incident Reporting Form or via the OnSecure Website (which is a joint initiative between the Defence Signal Directorate and the Australian government Information Management Office to assist government agencies in dealing with information security breaches) [23]. Information derived from these reports is used as a basis for threat assessments and security advice.

### 4.2 Australian Computer Emergency Response Team (AusCERT)

The Australian Computer Emergency Response Team (AusCERT) is an independent non-profit organization located at the University of Queensland. It provides an important information security service to the private sector and to some government agencies on a fee-for-service basis. AusCERT's aims are to reduce the probability of successful attacks,

to reduce the direct costs of security to organizations, and to lower the risk of consequential damage [24]. In May 2003, the Australian government announced the launch of AusCERT's National Information Technology Alert Service (NITAS) [25], which is sponsored by the federal government. NITAS provides a free service to subscribers, most of whom are owners and operators of the NII [26].

## 5 LAW AND LEGISLATION

### 5.1 Electronic Transactions Act 1999

The Electronic Transactions Act of 1999 creates a light-handed regulatory regime for using electronic communications in transactions. It facilitates electronic commerce in Australia by removing existing legal impediments under Commonwealth law that may prevent a person from using electronic communications. The act gives business and the community the option of using electronic communications when dealing with government agencies [27].

### 5.2 Cybercrime Act 2001

The Cybercrime Act of 2001 amended the Criminal Code Act 1995. It also amended the Crimes Act 1914 and the Customs Act 1901 to enhance the applicability of the existing search-and-seizure provisions relating to electronically stored data. It gives federal law enforcement agencies the authority to investigate and prosecute groups who use the internet to plan and launch cyber-attacks (such as hacking, computer virus propagation, or denial-of-service attacks) that could seriously interfere with the functioning of the government, the financial sector, and industry. The offenses and investigation powers were drafted in a manner to make them consistent with the draft of the Council of Europe's Cybercrime Convention.

The act covers:

- Unauthorized modification of data to cause impairment;
- Unauthorized impairment of electronic communication;
- Unauthorized access to, or modification of, restricted data;
- Unauthorized impairment of data stored on a computer disk, etc.;
- Possessing, producing, supplying, or obtaining data with intent to commit a computer offense;
- Causing an unauthorized computer function with intent to commit a serious offense.

The offenses were drafted in a way that recognizes the inter-jurisdictional character and extend to situations where:

- The conduct occurs wholly or partly in Australia;
- The result of the conduct occurs wholly or partly in Australia; or
- The offender was an Australian citizen or Australian company.

### 5.3 Security Legislation Amendment (Terrorism) Act 2002

The Security Legislation Amendment (Terrorism) Act 2002 [28] amended the Criminal Code Act 1995 to:

- Create a new offense of engaging in a terrorist act and a range of related offenses;
- Modernize Australia's treason offense; and
- Create offenses relating to membership in or other specified links with a terrorist organization.

An organization can be listed in regulations if the attorney-general is satisfied that the organization is a terrorist organization and that the organization has been identified in a decision of the United Nations Security Council relating to terrorism. A court may also find that an organization is a terrorist organization [29].

The act also specifically outlawed cyber-terrorism: "The action or threat of action which seriously interferes with, seriously disrupts, or destroys, an electronic system including, but not limited to information, telecommunications and financial systems [ ... ]. The action is done or the threat is made with the intention of: advancing a political, religious or ideological cause; and coercing, or influencing by intimidation, the government of the Commonwealth or a State, Territory or foreign country (or part of)" [30].

### 5.4 Spam Act 2003

Australia's anti-spam legislation was introduced in 2003 in response to concerns about the impact of spam on the effectiveness of electronic communication and the costs imposed on end users. The Spam Act 2003 [31] prohibits the sending of spam, which is defined as a commercial electronic message sent without the consent of the addressee via e-mail, short message service (SMS), multimedia message service (MMS), or instant messaging. The requirements under the Spam Act apply to all commercial electronic messages, including both bulk and individual messages. The Australian Communications and Media Authority (ACMA) has enforcement responsibility for the Spam Act.

In June 2006, the former Department of Communications, Information Technology and the Arts (now Department of Broadband, Communications and the Digital Economy) released a review of the Spam Act [32] which found that the measures in the Act had been successful in curbing spam, but that it remained a significant problem.

## ACKNOWLEDGMENT

We acknowledge the contribution of the expert, Alex Webling of the Attorney-General's Department within the Australian government, who validated the content of this chapter.

## REFERENCES

1. Attorney-General's Department National Security. (2008). Website http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructureProtection.
2. http://www.tisn.gov.au/agd/WWW/TISNhome.nsf/Page/Business-Govt_partnership, 2008.
3. http://www.tisn.gov.au/, 2008.

4. Commonwealth of Australia (2005). *National Counter-Terrorism Plan*, 2nd ed., September. http://www.nationalsecurity.gov.au/agd/WWW/rwpattach.nsf/VAP/(5738DF09EBC4B7EAE52BF217B46ED3DA)~NCTP_Sept_2005.pdf/$file/NCTP_Sept_2005.pdf.
5. http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf, 2008.
6. Australian Government *E-Security National Agenda 2007*, http://www.dbcde.gov.au/__data/assets/pdf_file/71201/ESNA_Public_Policy_Statement.pdf, 2008.
7. Yates A. (2007). *National Security Briefing Notes*, July. http://www.homelandsecurity.org.au/files/2007_e-security_agenda.pdf.
8. http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA) ~GovCERT.au+October+2007.PDF/$file/GovCERT.au+October+2007.PDF, 2008.
9. The Attorney-General's Department *About the Department*, http://www.ag.gov.au/www/agd/agd.nsf/Page/About_the_Department, 2008.
10. http://www.ag.gov.au/www/agd/agd.nsf/Page/Organisational_StructureNational_Security_and_Criminal _JusticeSecurity_and_Critical_Infrastructure, 2008.
11. *E-Security National Agenda*, (2007). op. cit., p. 1.
12. http://www.dbcde.gov.au/communications_for_business/security/critical_infrastructure_security, 2008.
13. http://www.tisn.gov.au/agd/WWW/tisnhome.nsf/Page/CIP_Projects#section2, 2008.
14. http://www.ag.gov.au/govcert, 2008.
15. http://www.agimo.gov.au, 2008.
16. http://www.dsd.gov.au, 2008.
17. http://www.asio.gov.au, 2008.
18. http://www.ahtcc.gov.au, 2008.
19. http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_CriticalInfrastructure Protection, 2008.
20. Attorney-General's Department, Protecting Australia's National Information Infrastructure. (1998). *Report of the Interdepartmental Committee on Protection of the National Information Infrastructure*. Canberra, December 1998.
21. http://www.cript.gov.au, 2008.
22. http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~TISN+diagram+v.2+Dec+07.pdf/$file/TISN+diagram+v.2+Dec+07.pdf, 2008.
23. http://www.onsecure.gov.au, 2008.
24. NII Report, (1998). op. cit. p. 2 http://www.auscert.org.au.
25. http://www.nationalsecurity.gov.au/www/attorneygeneralHome.nsf/0/64534A395BA69AF4CA256D24007BDCA2, 2008.
26. http://www.national.auscert.org.au, 2008.
27. http://www.ag.gov.au/agd/WWW/securitylawHome.nsf/Page/e-commerce_Electronic_Transactions_Act_-_Advice_for_Commonwealth_Departments, 2008.
28. Security Legislation Amendment (Terrorism) Act 2002, No. 65, (2002). *An Act to Enhance the Commonwealth's Ability to Combat Terrorism and Treason, and for Related Purposes*, http://scaleplus.law.gov.au/html/comact/11/6499/pdf/0652002.pdf.
29. http://www.nationalsecurity.gov.au/agd/www/NationalSecurityHome.nsf/Page/RWPA41035442ED47EF7 CA256D6A001215A5, 2008.
30. Security Legislation Amendment (Terrorism) Act (2002). op. cit.
31. http://www.dbcde.gov.au/__data/assets/pdf_file/0015/34431/Main_Features_of_the_spam_act.pdf, 2008.
32. http://www.dbcde.gov.au/__data/assets/pdf_file/0008/40220/Report_on_the_Spam_Act_2003_Review-June_2006.pdf, 2008.

# AUSTRIA

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Contemporary sources of dangers and risks to the state, the society, and the individual may be found in the fields of politics, the economy, the military, society, the environment, culture and religion, and information technology (IT). Information and communication technology has acquired a dimension of its own in security policy because it links all other security aspects, thus becoming a power factor in its own right and leaving room for many options. Austria as a modern society and as a small state is particularly vulnerable in the area of information. This includes both the military and the civilian sectors, and increasingly business and industry as well [1].

Accordingly, Critical Information Infrastructure Protection is of crucial importance for Austria. Responding to a parliamentary inquiry [2], the Austrian federal chancellor defined critical infrastructures as "natural resources; services; information technology facilities; networks; and other assets which, if disrupted or destroyed would have serious impact on the health, safety, or economic well-being of the citizens or the effective functioning of the Government" [3]. This definition conforms to the definition elaborated by the EU (see chapter on the EU in this book).

The same inquiry also raised the question of whether there was a list of critical infrastructures in Austria [3]. In its answer, the Ministry of Internal Affairs clarified that there is a list of civilian objects worthy of protection, but they are not explicitly denoted as critical infrastructure. However, it can be assumed that Critical Infrastructure Protection in Austria manly refers mainly to these objects. The list of civilian objects worthy of protection includes about 180 items, which are categorized in the following classes:

- Institutions of the legislative, executive, and judiciary powers,
- Infrastructure facilities of energy supply companies,
- Information and communication Technologies,
- Infrastructure facilities that ensure the provision of vital goods,
- Transport and traffic infrastructures.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

Following the Security and Defense Doctrine of 2001, which can be considered to be the guideline for Austria's security and defense policy, security in all its dimensions is the basic prerequisite for the existence and functioning of a democracy as well as for the economic welfare of the community and its citizens. Therefore, security must be conceived and implemented within a comprehensive security policy.

There have been several organizational and procedural efforts since the 1990s to manage CIP/CIIP in Austria. The issue of CIIP has been addressed by the government, especially by the Ministry of Internal Affairs; the Ministry of Defense; the Ministry of Traffic, Innovation, and Technology; and the Federal Chancellery, which has taken the leadership and is the central point in different projects.

On the European level, Austria takes part in all relevant EU activities regarding the protection of critical infrastructures, such as the European Program for the Protection of Critical Infrastructure (EPCIP) and the Critical Infrastructure Warning Information Network (EUCIWIN). Austria, like most other EU member states, shares the opinion that the protection of critical infrastructures has to follow the principle of subsidiarity, which means that the protection of the critical infrastructure is primarily the task of the member states. Activities of the EU are seen as complementary measures.

### 2.1 Security and Defense Doctrine 2001

According to the principle of comprehensive security, the Security and Defense Doctrine [4] recommends the development of the existing Comprehensive National Defense Program into a system of Comprehensive Security Provision by focusing on the new risks and threats and by amending legal provisions [5]. One can therefore deduce that this will also include all measures referring to CIIP.[1] This doctrine clearly stresses that for small states, full and unimpaired access to the information they require is a basis for their freedom of action in security matters [5].

The implementation of Austria's security policy within the framework of the Comprehensive Security Provision relies on systematic co-operation among various policy areas on the basis of appropriate sub-strategies.

### 2.2 IT Strategy and the "Platform Digital Austria"

The IT strategy of the government was formulated in July 2001, based on a decision of the Council of Ministers of 6 June 2001 referring to the New Structuring of the IT Strategy of the Government. The strategy consisted of the following three service types: Administration and Public Relations, Techniques and Standards, and Project Management and International Affairs. A special body, the ICT Board, was established to guarantee

[1]The concept of "Comprehensive National Defense" as developed from 1961 onwards was embedded in the Constitution in 1975. Under Article 9a of the Austrian Constitution, the role of Comprehensive National Defense is to "maintain [Austria's] independence from external influence as well as the inviolability and unity of its territory, especially to maintain and defend permanent neutrality". Together with the constitutional amendment, the Austrian parliament unanimously adopted a resolution in 1975 "on the fundamental formulation of Comprehensive National Defense in Austria" (defense doctrine). These were the foundations of the national defense plan, which was adopted by the Austrian government in 1983 and identified the "protection of the country's population and fundamental values from all threats" as a basic goal of Austrian security policy.

strategic co-ordination of ICT within the framework of the public government. This board was composed of the chief information officers of all the Federal Ministries and was located at the Federal Chancellery. It was responsible for coordinating the IT activities with each ministry, the local authorities, and the municipalities.

In 2005, the strategy was restructured. The basic elements of the 2001 strategy were retained, and the existing organizations were consolidated. However, in order to ensure sustainability, the ICT Board and the E-Cooperation board (the body responsible for coordination of e-government) were summarized in one unit, the ICT-Strategy Unit of the federal government [6]. This group forms the central unit of the new "Platform Digital Austria", where all IT and e-government efforts are coordinated. The ICT-Strategy Unit is responsible for public relations; the ICT budget, controlling, and sourcing; law, organization, and international activities; program and project management; and technical infrastructure.

### 2.3 Citizen Card and e-government

The Austrian Citizen Card Concept does not define a single citizen card for electronic identification, but only specifies the minimum technical requirements in a neutral way. Because of the open, technologically neutral approach, a variety of entities can issue citizen cards. These include both public bodies (including federal ministries and universities) and private bodies (certification authorities, banks) and can even involve other technologies such as mobile phone signatures [7]. In order to make use of the possibilities offered by electronic identification, citizens need to register their card as citizen card, download software, and buy a reader for the chip. After this registration process, they can use their card for e-identification and for electronic signatures. Different governmental services can be accessed by using the citizen card, and the e-government activities will be extended continuously [8].

### 2.4 Zentrales Ausweichsystem (ZAS)

After a fire at the Austrian Central Bank at the end of the 1970s, the government decided to establish an alternative replacement system for the data stock of the government. This system is located in the so-called Einsatzzentrale Basisraum (EZB) in St. Johann/Salzburg. Due to its coordinative function in the procurement of IT technologies, the Federal Chancellery has been responsible for the development of the EZB.[2]

The Zentrale Ausweichsystem (ZAS) has been a central part of the governmental crisis prevention system since the 1980s and has been fully operational on a day-to-day basis ever since. Some fundamental and very important systems (like the law information system/RIS) are run by this system. In addition, the ZAS serves as an archive for important backup data, such as the data from the public record office and from the Schengen Information System.[3]

### 2.5 Austrian Information Security Handbook

By order of the Federal Chancellery, the Center for Secure Information Technology Austria (A-sit, see below) publishes the Austrian Information Security Handbook (known

[2]The ZAS is located on an installation of the Austrian military; therefore, not much is publicly known about the institution itself.
[3]Cf. [9].

until 2005 as the IT-Security Handbook). This handbook gives an overview of IT security in general and informs readers in a broad and comprehensive way about fundamental aspects and measures in the field of IT. The handbook was updated in 2003, 2004, and 2007 based on the idea that security is a continuous process. It consists of two parts: "IT Security Management", which offers concrete instructions in this field; and "IT Security Measures", which describes standard security measures for IT systems requiring a medium security level [10].

### 2.6 Official Austrian Data Security Website

The Official Austrian Data Security Website [11], which is coordinated by the Federal Chancellery, serves as an information desk for citizens in important matters such as data security, the Schengen Information System, Europol, etc. It also informs the public about the work of the Commission on Data Protection, whose reports are available on the website. It also serves as a complaint board for citizens who want to report violations of their data privacy.

## 3 ORGANIZATIONAL OVERVIEW

At the public level, no single central authority is responsible for CII/CIIP, which is considered to be a cross-agency task. However, the Federal Chancellery fulfills a coordinating task. CIIP is mainly addressed by the Ministry of Internal Affairs, the Ministry of Defense, and the Ministry of Traffic, Innovation, and Technology. In addition, the Center for Secure Information Technology Austria (A-SIT) and the Stopline.at—Initiative, both organized as public-private partnerships perform important tasks in the field of CIIP.

### 3.1 Public Agencies

***3.1.1 Ministry of Internal Affairs (BMI).*** Several divisions of the Ministry of Internal Affairs (BMI) deal with CIIP, especially with aspects of data security and cyber-crime. For example, the head office for the public safety at the Federal Crime Police Office operates a reporting center for child pornography [12].

Another important agency belonging to the BMI is the Federal Agency for State Protection and Counter-Terrorism (BVT), which is responsible for the coordination of personal security and the security of installations. In addition, it evaluates and develops the ability to provide protection on a permanent basis with regard to possible new threat scenarios.

The BMI also serves as the point of contact for European Processes concerning Critical Infrastructure Protection.

***3.1.2 Ministry of Defense.*** In the framework of the Ministry of Defense, Department II (also known as the "control department") is responsible for all aspects of information warfare. It fulfills its duties in close cooperation with the Leadership Support Command[4] and the two military intelligence services.[5] One of these, the Abwehramt, which

[4]The Austrian armed forces and the Ministry of Defense are currently undergoing reform, so that a change in responsibilities is possible.

[5]"Heeresnachrichtenamt" and "Heeresabwehramt".

is responsible for the protection of the armed forces, also has a special department called Electronic Defense.[6]

The Austrian Federal Constitution and the Defense Law determine the cooperation between the army and civil authorities in crisis situations if the latter are not able to guarantee the maintenance of public order and inner security themselves. Part of this is the protection of civilian installations against interference by unauthorized third parties, including the protection of critical information infrastructures.

The final report of the Politico-Military Commission [14], which was released in autumn 2004, recommends that the Austrian armed forces be given an important role in the protection of the vital, civilian ICT, as well as the capacity to provide redundant systems in case of catastrophes or threats [15].

These protective measures have been tested in several exercises held in close co-operation with the civilian institutions. The largest maneuver of this kind in Austria took place in the federal states of Carinthia and Styria from 13–16 April 2004. The Schutz 2004 maneuver was planned and executed as a security assistance mission under the leadership of the civil authorities.

***3.1.3 Ministry for Traffic, Innovation, and Technology (BMVIT).*** The Ministry for Traffic, Innovation, and Technology (BMVIT) is responsible for the safety of the public critical infrastructure. It operates a coordinating center for private owners and operators of critical infrastructure, and a center for security research. One of its recent activities has been to order an ICT master plan that would analyze the strengths and weaknesses and the state of the art of Austria's critical infrastructure. Another part of this mandate consisted in presenting options for measures, targets, missions, and visions [16]. The BMVIT also coordinates the Austrian Security Research Program, in which critical infrastructure protection will play an essential part [17].

***3.1.4 Commission on Data Protection (DSK).*** The Commission on Data Protection (DSK) serves as independent control authority that deals with data processing in the public and private sectors.[7] The DSK is located at the Federal Chancellery. All citizens have the right to appeal to this commission if their rights in the field of data security are violated. The commission verifies these claims and takes measures to remedy confirmed violations. The Council on Data Protection has exclusive consultative agendas and periodically publishes the Report on Data Security.

### 3.2 Public-Private Partnerships

***3.2.1 Center for Secure Information Technology Austria (A-SIT).*** The Center for Secure Information Technology Austria (A-SIT) was founded in May 1999 as an association supported by the Austrian National Bank, the Ministry of Finance, and the University of Technology in Graz. Its tasks include general monitoring issues of IT security[8] and the evaluation of encryption procedures [19], as well as supporting the introduction of the Citizen Card, supporting public institutions, and developing a security policy for all

[6]The chief of this department, Colonel Walter J. Unger, published several articles concerning IT security and cyberterrorism. See e.g.: [13].
[7]For more information, see [18].
[8]A-SIT offers tools and demonstration examples on its homepage: http://demo.a-sit.at.

important electronic payment systems for the Austrian National Bank. It is also a member of the Computer Incident Response Coordination Austria (CIRCA).

***3.2.2 Stopline.at.*** Stopline.at is an online center that can be addressed by all internet users—also anonymously if they wish—who come across child pornography or right-wing extremist content on the internet. The relevant laws describing the respective crimes are §207a StGB (Austrian penal code) regarding child pornography, and the Austrian National Socialist prohibition law and the law against displaying National Socialist regalia as well as symbols of right-wing radicalism, respectively.

Stopline.at was founded as a private initiative by the Austrian internet service providers and has become reporting office that is authorized and accepted by the public authorities. Stopline.at cooperates closely with the Federal Ministry of the Interior (Federal Office of Criminal Investigation and Federal Office for the Protection of the Constitution and Counter-Terrorism).

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 Computer Incident Response Coordination Austria (CIRCA)

The Computer Incident Response Coordination Austria (CIRCA) is Austria's main organization in the field of IT early-warning systems. It is a public-private partnership whose main actors are the Federal Chancellery, the Federation of the Austrian Internet Service Providers (ISPA), and A-SIT. Other members are representatives of the social partners (economic interest groups), the federal states, and of other critical infrastructure providers. It is a web of trust between Internet Service Providers (ISPs), IP network operators from the public and private sectors, and enterprises in the field of IT security. The electronic communication network of the private sector is run by ISPA, whereas the Federal Chancellery has the lead in the public sector.

The aim of this Austrian security net is to provide an early-warning system against worms, viruses, distributed denial-of-service attacks, and other threats that endanger IP networks and their users. Therefore, CIRCA issues alerts and risk assessments and provides information about precautionary measures. Its strategy is both proactive and reactive, and involves a continuous exchange of information and news between the Federal Chancellery and CIRCA [20].

### 4.2 Computer Emergency Response Team (CERT.at)

In March 2008, the Austrian domain registry nic.at launched the Austrian Computer Emergency Response Team (CERT.at) [21]. The purpose of the CERT is to coordinate security efforts and incident response for IT security problems on a national level in Austria. The level of support given by CERT.at varies depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and CERT.at's resources at the time. Special attention is given to issues affecting critical infrastructure. In addition, the CERT also releases educational material for SMEs and the general public.

The CERT.at cooperates with local and international CERTs as well as with other information security teams. It therefore shares information about incidents and security breaches with its partners. Nevertheless, it strictly protects the privacy of its customers.

## 5 LAW AND LEGISLATION

There is a broad variety of legal acts and laws dealing with CII/CIIP in a very broad sense. Most of them refer to the processing, collection, transfer, and protection of (personal) data through or by public agencies (e.g. the police and security agencies).

The general responsibilities of governmental authorities are laid out in the Bundesministeriengesetz (Federal Ministry Law), which defines the agendas of each ministry.

The following can be regarded as the central and most relevant legislative acts:

### 5.1 Information Security Law and Information Security Order

With the Information Security Law[9] and the Information Security Order,[10] Austria guarantees the secure use of classified information within the jurisdiction of the federal government according to international law. They regulate the access, transmission, identification, electronic processing, registration, and preservation of classified information. In accordance with international law, information regarding security arrangements within the EU or with other states qualifies as classified information. The Information Security Law specifies four types of classified information:

- *Limited.* if the unauthorized transmission of information would be contrary to the interests mentioned in Article 20, paragraph 3 of the Federal Constitution;
- *Confidential.* If the information has to be kept secret according to additional federal laws and if maintaining secrecy is in the public interest;
- *Restricted.* If the information is confidential and its publication would harm the interests mentioned in Article 20, paragraph 3 of the Federal Constitution;
- *Top Secret.* If the information is secret and its publication could seriously damage the interests mentioned in Article 20, paragraph 3 of the Federal Constitution.

Consequently, every type of classification corresponds to a certain security infrastructure (building, organizational structures, and personnel).

The Data Security Law therefore only grants access to Confidential, Restricted, and Top Secret information to individuals who have completed an advanced security examination according to paragraphs 55 to 55b of the Security Police Act. In the civilian sphere, this security examination is conducted by the Federal Office for Constitutional Protection and Counter-Terrorism.

### 5.2 Data Security Law 2000

The Data Security Law (DSG)[11] contains extensive regulations on the processing of personal data. With this law, Austria adopted the EU guideline for data security of the year 1995. The DSG 2000 stresses the importance of data-security measures and measures to enhance confidentiality for personal data. As a rule, the user of personal data is responsible for ensuring that the information is used in a correct manner, that no unauthorized persons have access to data, that the data is not destroyed, and that its secure storage is guaranteed. The DSG lists the following as civil rights:

[9]BGBl I Nr. 23/2002.
[10]BGBl II Nr. 548/2003.
[11]BGBl 165/99; see the explanations given by the Ministry of Internal Affairs. http://www.bmi.gv.at.

- The fundamental right to a secure processing of personal data,
- the right of information,
- the right to have incorrect or wrong data corrected,
- and the right to have data deleted.

Another important part of the DSG's activities is the duty to report. This means that with certain exceptions (e.g., for reasons of national security), all applications for personal data must be reported. Additionally, the Data Security Website contains all necessary information, forms, and addresses for rapid reporting.

### 5.3 Security Police Law

The Security Police Law (SPG)[12] defines the duties and authority of the civilian security services. Several articles and/or sections refer to the collection, transfer, storage, and deletion of personal data,[13] as well as measures to prevent the unauthorized use of data. It also provides special rights for individuals whose privacy has been violated by the security services.[14]

Together with this law, the office of a "legal protection agent"[15] was established as a controlling institution. The main duty of the legal protection agent is to protect the rights of citizens by ensuring that investigations of threats as well as observation and surveillance stay within legal rules.

### 5.4 Military Competence Law

In analogy to the Security Police Law, the Military Competence Law (MBG)[16] regulates the tasks and duties of the Austrian armed forces, including the two military intelligence services.[17] The MBG regulates the collection, transfer, and deletion of personal data. Paragraph 55 regulates the rights of citizens in cases where data security measures have been disregarded. The MBG also provides for the establishment of the institution of a "legal protection agent" who monitors the legality of measures undertaken by the intelligence services.[18]

### 5.5 Telecommunication Law

The Telecommunication Law[19] (TKG) includes extensive and detailed regulations referring to data security in general, and specific regulations regarding communication exchange. Furthermore, these regulations stipulate confidentiality of telecommunication.[20] The law also states that the suppliers of communication lines are responsible for securing all data. Paragraph 89 obliges the suppliers of communication lines to place all technical means necessary for the surveillance of telecommunication at the disposal of the security agencies.

[12] BGBl 566/91 idF BGBl 85/2000.
[13] Cf. especially section 4 of the law, "Verwenden personenbezogener Daten im Rahmen der Sicherheitspolizei".
[14] Cf. especially section 6 of the law, "Besonderer Rechtsschutz".
[15] "Rechtsschutzbeauftragter" (ombudsman in charge of protecting the rights of citizens).
[16] BGBl 86/ 2000.
[17] Second Section of the Law on Intelligence Services.
[18] Paragraph 57 of the law.
[19] Telekommunikationsgesetz, BGBl 100/ 1997 idF BGBl 134/ 2002.
[20] Fernmeldegeheimnis, Datenschutz. Chapter 12, paragraphs 87–101.

### 5.6 Penal Code (StGB)

Several articles of the Austrian Penal Code (StGB) refer to CII/CIIP. Some new regulations were introduced to the Penal Code in 2002 [22]:

*Paragraph 118a.* Unlawfully accessing a computer system: This crime is punishable with a prison sentence up to six months or a fine. The law applies not only to illegal access, but also to unauthorized registration on a computer system or to those who offer these possibilities to another person, make them public, or use them to gain benefit. The law also applies to cases where users who are authorized to use part of the system have accessed other parts that are off-limits to them. But an essential element is that a violation of security measures has to have occurred. Thus, if no security measures are in place, unauthorized access is not a crime. It is worth mentioning that the perpetrator will only be prosecuted with authorization from the injured party.

*Paragraph 119.* Infraction of the confidentiality of telecommunications: This crime is defined in a similar way to violations of the privacy of correspondence. The punishments and the requirement for the prosecution are the same as in paragraph 118a.

*Paragraph 119a.* Improper interception of data: This constitutes a crime that is punished and prosecuted. It is essential that the intercepted data not be intended for the intercepting person. It does not matter whether the perpetrators intend to use the data for themselves, to make it public, or to offer it to another party. The law makes no distinction between the methods applied.

*Paragraph 126b.* Disruption of the operability of computer systems: The elements of the crime of "Disruption of the operability of computer systems" are directly connected with paragraph 126a. The law outlaws the disruption of systems by introducing or sending data. The authorization of the injured party is not needed for prosecution, because this law applies to the diffusion of viruses, worms, etc.

*Paragraph 126c.* Abuse of computer programs or access data: This article is a very complex one. It prohibits the abuse of computer programs or access data, such as passwords. It is generally intended to cover Trojans and spy programs, as well as accessing and distributing passwords and access codes for various purposes. However, the maximum punishment is not higher than in the other articles.

### 5.7 Penal Procedure (StPO)

The Penal Procedure (StPO) regulates the special investigation methods for combating organized crime. These methods are provisions for optical and acoustic surveillance by civilian security institutions. The law also regulates the installation of a legal protection agent who monitors the legality of the special investigation methods. According to the StPO, the Minister of Justice is obliged to report annually on the use of special investigation methods to the Council for Data Protection (DSR),[21] the Commission on Data Protection (DSK), and the Austrian parliament.[22]

[21]The Council for Data Protection (Datenschutzrat, DSK) is a consultative body, which advises the government in questions concerning data protection. http://e-campus.uibk.ac.at/planet-et-fix/M6/3_Datenschutzrecht/3_Institutionen/K633_20datenschutzrat.htm.

[22]Cf. Bundesministerium für Justiz. "Gesamtbericht über den Einsatz besonderer Ermittlungsmethoden im Jahr 2001" (Vienna 2002).

In 2004, Austria introduced the European arrest warrant into its Penal Procedure System. It is an EU regulation that simplifies the extradition of persons for trial or for the enforcement of sentences. It comprises a catalog of 32 crimes where no close examination is required for extradition. A major problem is that these 32 offenses are not defined properly. One of these crimes is "cyber-crime", which has given rise to a lot of controversy, because each of the 25 member states may define it in a different way. In the Austrian penal code, for example, there is no such offence as "cyber-crime".

### 5.8 Electronic Signature Law (SigG)

Since 1999, the Electronic Signature Law (SigG)[23] has regulated the admission of electronic signatures in the Austrian legal system. The controlling board is the Austrian Telecom Control Commission, which gives the suppliers the necessary certificates. It also informs its constituency about security measures related to electronic signatures [23]. Since 24 September 2002, it has been fully operational with the Public-Key-Infrastructure (PKI).

## ACKNOWLEDGMENT

We acknowledge the contribution of the expert, Otto Hellwig of Technische Universität Graz, who validated the content of this chapter.

## REFERENCES

1. Resolution by the Austrian parliament (2001). *Security and Defense Doctrine: Analysis*, —Draft expert report of 23 January. http://www.austria.gv.at/2004/4/18/doktrin_e.pdf.
2. http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXII/J/J_04641/imfname_067709.pdf, 2008.
3. http://www.parlament.gv.at/pls/portal/docs/page/PG/DE/XXII/AB/AB_04595/imfname_069768.pdf, 2008.
4. http://www.bundeskanzleramt.at/2004/4/18/doktrin_e.pdf, 2008.
5. Federal Chancellery Austria. (2001). *Security and Defense Doctrine*, http://www.bundeskanzleramt.at/2004/4/18/doktrin_e.pdf.
6. Digital Austria *Administration on the Net: An ABC Guide for E-Government in Austria*, p. 28. http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=19394, 2008.
7. http://www.buergerkarte.at, 2008.
8. http://www.help.gv.at/sigliste/sig_bund.jsp?cmsid=281, 2008.
9. Der Standard (2007). *Österreichs Hochsicherheits-Datenspeicher wird 25 Jahre alt*, (15 September 2007).
10. The complete handbook is available at http://www.a-sit.at/pdfs/OE-SIHA_I_II_V2-3_2007-05-23.pdf, 2008.
11. http://www.dsk.gv.at/indexe.htm.
12. http://www.bmi.gv.at/kriminalpolizei, 2008.

[23] Signaturgesetz BGBl 1999/ 190.

13. (a) Unger, W. J., and Vetschera, H. (2005). Cyber War und Cyber Terrorismus als neue Formen des Krieges. *Österreichische Militärische Zeitschrift* **43**2, 203–211; (b) Unger, W. J. (2004). Angriff aus dem Cyberspace I-III. In *Truppendienst*, No. 2, pp. 143–147, 271–275, 382–386; No. 3; No. 4.
14. Bundesheerreformkommission http://www.bmlv.gv.at/facts/bh_2010/archiv/pdf/endbericht_bhrk.pdf.
15. Bundesheerreformkommission (2004). *Endbericht 2004*, p. 49f, 2008.
16. http://www.bmvit.gv.at, 2008.
17. http://www.kiras.at/wDeutsch/index.php and http://www.bmvit.gv.at/innovation/sicherheitsforschung/index.html, 2008.
18. http://www.dsk.gv.at/indexe.htm, 2008.
19. http://www.a-sit.at/asit/asit.htm, 2008.
20. http://www.circa.at, 2008.
21. http://www.cert.at/english/missionstatement/content.html, 2008.
22. http://www.cybercrimelaw.net/countries/austria.html, 2008.
23. http://www.signatur.rtr.at.

# BRAZIL

Manuel Suter and Elgin Brunner
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Broadly defined, the Brazilian critical infrastructures include the areas of oil, electric energy, and telecommunications [1]. More specifically, the SecGov 2006 conference [2] held in Brasilia in November 2006 and sponsored by the Institutional Security Cabinet (Gabinete de Segurança Institucional—GSI) had the goal of discussing topics and questions on Critical Infrastructure Security in Brazil, Information and Communication Security and Terrorism. Eight discussion panels took place on the following topics:

- Public Safety,

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- Energy,
- Finance,
- Transport Systems,
- Water Supply,
- Public Health,
- Telecommunications,
- Terrorism.

Although the Brazilian government has not formally defined what the critical infrastructures are, at least the first seven topics are unofficially considered to represent critical sectors[1].

As regards critical *information* infrastructure, the focus lies on telecommunications and the internet. Based on the understanding that critical infrastructure protection on a nationwide level has consequences that can impact a nation socially, politically, and economically, a new approach was developed and proposed specifically by the federal telecommunications regulatory body, Anatel (see the chapter on Organizational Overview), to be applied to the telecommunications infrastructure, in order to understand the related risks and to develop a suitable program based on four main points: contextualization, a protection strategy, a set of methodologies, and software tools to support them. These methodologies include the development of tools for identifying critical (information and communication) infrastructures and the potential threat landscape, for scenario creation, and for diagnosing [3]. Moreover, information security is no longer understood as an exclusive problem of the sectors related to IT, or even of a particular organization, industry, or government; it is understood instead as consisting of regional and global strategies that facilitate an organized response to the threats and vulnerabilities associated with technology use [4].

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

As mentioned above, Brazilian policies for information infrastructure protection focus on two particular aspects: the internet and telecommunications. Both of these, it is argued, play an important role in social (and digital) inclusion and are essential for national cohesion. The policies adopted in order to create trust in critical network infrastructures [5] show that the two sectors cannot be separated, since the interests of telecom and internet providers in operating secure networks are clearly inter-related, and the latter depend almost entirely on the former for backbone infrastructure and access networks. The Brazilian government has initiated several initiatives in association with internet diffusion, network protection, and communications security.

### 2.1 Brazilian Internet Steering Committee (CGI)

The initiatives of internet governance are mainly conducted under the auspices of the Brazilian Internet Steering Committee (Comitê Gestor da Internet no Brasil—CGI). This committee is a multi-stakeholder organization composed of members of government

[1]Information provided by an expert.

agencies, backbone operators, representatives of the internet service provider industry, users, and the academic community, and was jointly created in 1995 by the Ministry of Communications and the Ministry of Science and Technology.[2] The committee's main tasks are:

- To propose policies and procedures related to the regulation of internet activities;
- To recommend standards for technical and operational procedures for the internet in Brazil;
- To establish strategic directives related to the use and development of the internet in Brazil;
- To promote studies and technical standards for the network and security of services in the country;
- To coordinate the allocation of internet addresses and the registration of domain names;
- To collect, organize, and disseminate information on internet services, including indicators and statistics.

The committee maintains three working groups—on network engineering, on computer security, and on the training of human resources—in order to provide technical, administrative, and operational input for the committee's decisions and recommendations. Moreover, several projects in areas of fundamental importance for the operation and development of the internet in Brazil are coordinated. In order to execute its activities, the non-profit civil organization Brazilian Network Information Center NIC.br was created.

The Brazilian Internet Steering Committee has lately issued the second edition of its Survey on the Use of Information and Communication Technologies in Brazil—ICT Enterprises and ICT Households, reflecting the concern and the commitment of the committee in monitoring and sharing information about the evolution of the internet, which is considered an essential tool for social and economic development, as well as for the democratic participation of citizens and countries in the information society [6].

Of particular importance are also some of the recently initiated combined actions to improve internet security, such as instruction for users. Several initiatives are undertaken by the Computer Emergency Response Team Brazil (CERT.br), which is maintained by the Internet Steering Committee. The Internet Security Best Practices [7] document has been published since 2000 in order to help increase users' security awareness. While this document was written specifically for internet end users and has been constantly updated to reflect the evolving nature of attack and protection technologies, another document has been developed by CERT.br that is aimed specifically at companies: the Best Practices for Internet Network Administrators [8]. This document is addressed to security professionals and network professionals who do not have a dedicated security team at their disposal [9].

[2]The Brazilian Internet Steering Committee was created by interministerial ordinance no. 147 of 31 May 1995 and altered by presidential decree no. 4829 of 3 September 2003. Since July of 2004, the representatives of the civil society are chosen democratically to participate directly in the deliberations and to debate priorities for the internet, along with the government.

### 2.2 Brazilian electronic government program (e-gov)

The Brazilian government sees itself as having an important role to play both as a promoter and as a user of information and communication technologies. Therefore, the government has made the adoption of advanced information communication technologies for its administrative processes and delivery of services to its citizens a high priority. In 2000, it launched an electronic government initiative under the auspices of the Information Society Program of the Ministry of Science and Technology with three overall aims relating to the goal of digital inclusion: to universalize services, to make the government accessible to everyone, and to advance the infrastructure. A presidential decree established the Executive Committee of Electronic Government on 18 October 2000. Three years later, the presidency of Brazil published another important decree creating eight technical committees of e-government, with tasks including the implementation of free software, the advancement of digital inclusion, the integration of systems, legal systems and software licenses, the administration of websites and online services, network infrastructure, government to govern (G2G), and knowledge and strategic information management [10]. The Brazilian e-government model aims at integrating the different government organs in order to guarantee multiple channels of access for the citizens, institutions, local executives, and civil servants through manifold devices such as the traditional office counter and telephone, but also internet and digital TV [11]. In concrete terms, the driving principles of Brazil's electronic government are defined as follows [12].

- The priority of electronic government is to promote citizenship;
- Digital inclusion is inseparable from electronic government;
- Free software is a strategic appeal to implement electronic government;
- Knowledge management is a strategic instrument for the articulation and administration of the public policies of electronic government;
- Electronic government needs to rationalize the use of resources;
- Electronic government needs to relate to the integrated outline of policies, systems, templates, and norms;
- The activities of electronic government must be integrated with other levels of government.

## 3 ORGANIZATIONAL OVERVIEW

Major public efforts in Brazil concerning CIIP include the Information Security Steering Committee, the national policies for ICT under the auspices of both the Ministry of Science and Technology and the Ministry of Communication, and the Brazilian Network Information Center. Brazil has a complex and very sophisticated infrastructure of institutions involved in developing information security policy. Information security issues lie within the jurisdiction of the Institutional Security Cabinet (Gabinete de Segurança Institucional—GSI), which is an essential organ of the Presidency of the Brazilian Republic and assigned with the competence to coordinate the activities respective to information security [13]. The GSI's activities are defined by decree no. 5083 of 17 May 2004 [14]. It does not handle security issues directly, but works through other related organizations. Under its auspices, the Information Security Committee was formed.

As public-private partnerships, Anatel (the federal telecommunications regulatory body), Serpro (the federal data processing service), and CERT.br (the Computer Emergency Response Team Brazil) strive to further and deepen the cooperation between the public and the private sectors.

## 3.1 Public Agencies

***3.1.1 Information Security Steering Committee (CGSI).*** The Brazilian Information Security Steering Committee (Comitê Gestor da Segurança Informação - CGSI) was created by decree no. 3505 on 13 June 2000 [15]. It is composed by representatives from every ministry [16]. The participants discuss information security issues and define the future policy directions of the Brazilian federal administration in working groups. This committee oversees the federal government's commitment under decree no. 3505, which stipulates that there must be an information security policy for every department of the Brazilian federal government [17]. Information security is defined by the committee as including the protection of the information systems from denial of service to authorized users, and against intrusion or unauthorized modification of data and information. It is seen as broadly including the security of human resources, of documents and material, of areas and installations of communication and computing, as well as being designed to prevent, detect, deter, and document eventual threats and their development [18].

***3.1.2 National Policies for ICT.*** The Ministry of Science and Technology maintains a program dedicated to information and communications technologies (ICT). This program formulates a national policy and addresses issues such as software, microelectronics, network services, legal questions, and digital inclusion [19]. The focus lies on the technological and developmental aspects of the information and communication technologies.

Likewise, the Ministry of Communications maintains programs addressing digital inclusion, radio-diffusion, postal services, and telecommunications. These programs all aim to democratize access to these different means of communication and information and to reduce social and regional inequalities therein [20].

***3.1.3 Brazilian Network Information Center (NIC.br).*** As mentioned above, the Brazilian Internet Steering Committee (CGI) was created by interministerial ordinance no. 147 of 31 May 1995 and altered by presidential decree no. 4829 of 3 September 2003. It is a public agency by nature, but its members include representatives of the private corporate and third sectors, as well as of academia. It is responsible for promoting the technical quality, innovation, and dissemination of internet governance and services, and has created the Brazilian Network Information Center (NIC.br) [21] in order to execute its activities. These activities include services—registro.br, CERT.br, and PTT.br—as well as projects such as antispam.br, statistics and indicators, and the internet security card.

This is to say that, as a set of services, the center coordinates Brazilian domain registration and IP assignments, it sponsors the CERT.br, and aims at providing the necessary infrastructure for the direct interconnection between the diverse networks that operate in the metropolitan regions (Ponto de Troca de Tráfego—PTT). Moreover, the committee's Center of Studies on Information and Communication Technologies (Centro de Estudo sobre as Tecnologias da Informação e da Comunicação—CETIC.br) is responsible for the collection, analysis, and dissemination of data about the use and penetration of the internet in Brazil [22].

The projects maintained by the Internet Steering Committee's executive branch, the Network Information Center, include, as mentioned, an anti-spam website designed to serve as an impartial and technically based source of reference concerning spam. This site represents the effort to inform both the users and network administrators about spam, its implications, and the forms of protection and combat. Furthermore, two other projects work on the statistics and indicators about Brazilian internet development and growth and on a document containing recommendations about how to navigate the internet more securely and about how individuals can protect themselves against so-called 'cyber-threats'.

### 3.2 Public-Private Partnerships

***3.2.1 Anatel.*** Anatel (Agência Nacional de Telecomunicações), the federal telecommunications regulatory body modeled on the Federal Communications Commission of the US, was established with the mission of enabling a new model for Brazilian telecommunications, starting with the privatization of the Telebrás system. After privatization has been achieved between 1995 and 2003, the main role of Anatel became that of regulation, concession, and supervision of the telecommunications services in the country [23]. Among the important issues under discussion are the mechanisms for achieving cooperation between the Brazilian government and the private sector under the auspices of Anatel. Initial steps have been taken to address cyber-security issues facing the Brazilian telecom sector infrastructure through cooperation between private companies and this regulatory body.[3] Moreover, and as mentioned earlier, the methodology proposed and used by Anatel in order to identify critical infrastructure—called $MI^2C$—was used for the purpose of defining the critical parts of the Brazilian telecommunications infrastructure [24].

***3.2.2 SERPRO.*** The SERPRO (Serviço Federal de Processamento de Dados) is a private company owned by the Brazilian government with the mandate of providing networking services for information technologies to government agencies in Brazil. Serpro supports thousands of federal government IT systems and runs a large IP-based government intranet system. There are extensive physical and logical security arrangements in place. Serpro has a security committee of about 35 people who develop government system security policies. The coordinator of the committee is a member of the abovementioned Federal Government's Security Committee (CGSI). Moreover, Serpro cooperates on security issues with the Brazilian Internet Steering Committee and its Computer Emergency Response Team.[4] Serpro maintains different programs grouped under the three labels of governmental, entrepreneurial, and citizenship matters, which are closely linked to the Brazilian e-government program.

***3.2.3 CERT.br partnerships.*** The Computer Emergency Response Team Brazil, maintained by the Internet Steering Committee, has a close partnership with the Software Engineering Institute (SEI) of Carnegie Mellon in matters of education. Within this partnership, the governmental cell is provided with educational courses in computer security creation and management, technical formation of information security, and the fundamentals and details of incident handling. Moreover, due to this cooperation, Brazil is a

[3]Cf. Robert Bruce et al., op. cit.
[4]Cf. Robert Shaw., op. cit.

member to the Carnegie Mellon Software Engineering Institute (SEI) CERT coordination center, which is useful in networking and coordinating information security issues internationally.

Moreover, CERT.br is a member of the global Forum of Incident Response and Security Teams (FIRST) [25], which, by bringing together a variety of Computer Security Incident Response Teams (CSIRTs) from government, commercial, and educational organizations worldwide, aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information-sharing among members.

CERT.br is also a research partner of the Anti-Phishing Working Group (APWG), which is the global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming, and e-mail spoofing of all types [26].

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 CTIR Gov

The Computer Security and Incident Response Team (Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, CTIR Gov) is subordinate to the Institutional Security Office of the Presidency of the Republic (GSI) and deals with incidents on networks belonging to the federal public administration of Brazil. An executive order of 30 June 2003 created a working group responsible for determining the various aspects related to the installation and operation of a Computer Emergency Center. The mission of CTIR Gov is to coordinate responses to computer security incidents, to assure the necessary information exchange, and thereby to offer its constituency services that are both reactive (by responding as soon as notification arrives) and proactive (designed to prevent incidents and to reduce their impact). The reactive services aim to reveal the patterns and tendencies by continuous observation of events in order to serve as input to security recommendations, which are later issued to the constituency. The proactive services, which include information assets analysis and constitutive structures from the various information technology environments in the Federal Public Administration, provide a broad view of available resources, their usefulness, and associated risks [27].

### 4.2 CERT.br

CERT.br [28], formerly known as NBSO/Brazilian CERT, is the Brazilian National Computer Emergency Response Team, maintained by the NIC.br—the executive branch of the Brazilian Internet Steering Committee. CERT.br is a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian internet. Besides doing incident handling activities, CERT.br also works to increase awareness in the community and to help new Computer Security and Incidence Response Teams (CSIRTs) to establish their activities. The range of services of CERT.br includes [29].

- To provide a focal point for reporting computer security incidents that provides coordinated support in response (and indication to others) to such reports;

- To establish collaborative relationships with other entities such as law enforcement, service providers, and telecom companies;
- To support tracing intruder activity;
- To provide training in incident response, specially for CSIRT staff and for institutions starting the creation of a CSIRT.

Additionally, CERT.br maintains a list of all Brazilian CSIRTs [30]. CERT.br also participates in the coordination of the Brazilian Honeypots Alliance and uses the data collected thereby to identify malicious activity originating in the Brazilian internet space, and to notify the administrators of the networks involved in malicious activities identified.

### 4.3 Brazilian Honeypots Alliance

The objective of the Brazilian Honeypots Alliance/Distributed Honeypots Project [31] is to increase the capacity for incident detection, event correlation, and trend analysis in the Brazilian internet space. To achieve these goals, the project is working to:

- Set up a network comprising distributed low-interaction honeypots, covering most of the Brazilian IP address space;
- Build a data analysis system that allows to study the attacks trends and correlations;
- Work with CSIRTs to disseminate the information.

The project is jointly coordinated by the CERT.br and the CenPRA (Centro de Pesquisas Renato Archer), a research institution of the Ministry of Science and Technology [32]. The honeypots network has 25 partner institutions including representatives from academia, the government, industry, and the military, which provide hardware and network blocks and maintain their own honeypots. Statistics about malicious activities observed in the honeypots are generated daily [33]. The collected data is used for intrusion detection purposes.

### 4.4 RNP/CAIS

In order to coordinate separate initiatives and secure the integration of regional networks into a national network, the Ministry of Science and Technology created the National Education and Research Network (Rede Nacional de Ensino e Pesquisa—RNP) in 1989 and assigned to it the task of building a national internet network infrastructure for academic purposes. Ten years later, in 1999, the Ministry of Science and Technology and the Ministry of Education jointly started the inter-ministerial Program for the Implantation and Maintenance of the RNP, with the aim of elevating the academic network to a new position. This RNP2 backbone was officially inaugurated in 2000. Since 2002, the RNP has had an agreement with the government to reach certain goals aimed at fostering the activities of technological research in network development and the operation of advanced network means and services that benefit national education and research [34]. The RNP was the basic platform for the early development of internet technology in Brazil, and because of its historic role, it continues to play an important role in security issues.[5]

[5]Cf. Robert Shaw, op. cit.

The RNP's Security Incidents Attendance Center (Centro de Atendimento a Incidentes de Segurança—CAIS), which was created in 1997, is more specifically concerned with network security within the RNP. The mission of CAIS is to resolve and prevent security incidents on the networks of RNP2, to divulge information and security alerts, and also to participate in international organizations for networking purposes. Hence, CAIS acts in the detection, solution, and prevention of security incidents on the Brazilian academic network, in addition to developing, promoting, and spreading security practices for the networks. Its concrete activities range from the providing of incident response services and the promotion of the creation of new security groups nationwide to the testing and recommendation of security tools and policies [35].

## 5 LAWS AND LEGISLATION

Decree no. 3505 of 13 June 2000 establishes the information security policy to be used throughout the government and across all related partners in a number of different areas, including:

- Classification and treatment of information;
- Research in technologies to support national defense;
- Accreditation and certification of products and services;
- Assurance of interoperability of systems;
- Establishing rules and standards relating to cryptography;
- Systems for the confidentiality, availability, and integrity of information.[6]

This decree was updated on 21 June 2004. The update makes the Secretaria de Comunicação de Governo e Gestão Estratégica da Presidência da República a full member of the Comitê Gestor de Segurança da Informação (CGSI) [36].

### 5.1 Brazilian Penal Code

Two amendments to the Brazilian Penal Code dating from 2000 created two new offenses relative to information security. Articles 313-A and 313-B of law no. 9983 of 14 July 2000, respectively, criminalize

- The "entry, or facilitation on the part of an authorized employee of the entry, of false data, improper alteration or exclusion of correct data with respect to the computer systems or the data bank of the public administration for purposes of achieving an improper advantage for himself or for some other person, or of causing damages", as well as;
- The "modification or alteration of the information system or computer program by an employee, without authorization by or the request of a competent authority".[7]

[6]Cf. Robert Bruce et al., op. cit.
[7]This law is an amendment of decree-law no. 2848 of 7 December 1940 in the Penal Code.

### 5.2 Cybercrime Laws

Brazil's criminal law states that gaining unauthorized access to a computer system or violation of the secrecy of a computer system belonging to either a financial institution or securities dealer is a crime under article 18 of law no. 7492 of 16 June 1986, which defines crimes against the national financial system [37].

Senate bill PLS 00152 [38] of 1991 defines the crimes involving wrongful use of computer (and also contains other provisions). This legislation defines as a crime the violation of data by means or clandestine of hidden access to a computer program or system, as well as the violation of the secrecy of data by gaining access to information contained in the system or physical medium of a third party.

Moreover, Brazil has several laws prohibiting the interception of telephone, data, or telematic communications. These laws ensuring privacy and criminalizing data interception are outlined both in the Brazilian Federal Constitution and in public law.[8]

### 5.3 Brazilian Cybercrime Bill

The Brazilian Congress is currently discussing a more specialized Cybercrime Bill. Under the responsibility of Senator Eduardo Azeredo, this bill is said to be inspired by the Convention on Cybercrime of the Council of Europe [39] and attempts to bring together three draft bills dating from 1996 and 1999. In both the criminal and the military criminal codes, 11 offenses are to be typified [40].

- Dissemination of malicious codes aimed at stealing passwords (phishing);
- Credit card fraud;
- Cell phone cloning;
- Offenses against honor (libel, slander, and defamation, with the stipulation of increased penalties);
- Dissemination of malicious codes aimed at causing harm (viruses, trojans, worms, etc.);
- Unauthorized access to computer network;
- Unauthorized access to information;
- Unauthorized possession, transportation, or provision of such information;
- Unauthorized disclosure of a database;
- Compound larceny with the use of computer systems;
- Disruption of public utility services;
- Attacks against a computer network—DoS, DDos, DNS, etc.

While this bill is still under discussion, in the meantime, cyber-crimes in Brazil are being judged in analogy to the Brazilian Penal code.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Mariana Balboni of the Brazilian Internet Steering Committee, Regina Maria De Felice Souza of Agência Nacional de Telecomunicações, and João Henrique de A. Franco and Sérgio Luis Ribeiro of CPqD Telecom & IT Solutions, who validated the content of this chapter.

[8]For more details, cf. Goodman and Brenner, op. cit.

## REFERENCES


1. Claudio, P. *Internet in Developing Countries: the Case of Brazil*, http://www.research.ibm.com/people/p/pinhanez/publications/netbrasil.htm, 2008.
2. http://www.secgov.com.br.
3. Regina Maria De Felice Souza. (2007). *Critical Telecommunication Infrastructure Project*, InfoCitel Electronic Bulletin No. 33, http://www.citel.oas.org/newsletter/2007/marzo/infraestructura_i.asp.
4. Forum of Incident and Response Teams (FIRST). 2nd COLAIS. (2006). *2nd Latin American Conference for Security Incident Response*. Rio de Janeiro, 6–12 October 2006, http://www.rnp.br/en/events/colaris/.
5. Robert S. (2002). Creating trust in critical network infrastructures: the case of Brazil. *ITU Workshop on Creating Trust in Critical Network Infrastructures*. Seoul, Republic of Korea, 20–22 May 2002.
6. Brazilian Internet Steering Committee, Brazilian Network Information Center. (2007). Preface to the *Survey on the Use of Information and Communication Technologies in Brazil—ICT Households and ICT Enterprises 2006*, 2nd ed., São Paulo, http://www.cetic.br/tic/2006/indicadores-2006.pdf.
7. http://cartilha.cert.br (in Portugese), 2008.
8. http://www.cert.br/docs/seg-adm-redes, 2008.
9. Christine, H., and Steding-Jessen, K. (2006). Information security in Brazil. In *Survey on the Use of Information and Communication Technologies in Brazil 2005—ICT Households and ICT Enterprises*, 1st ed., Brazilian Internet Steering Committee/Mariana Balboni, Ed. http://www.cetic.br/tic/2005/indicadores-2005.pdf.
10. http://www.governoeletronico.gov.br, 2008.
11. http://portal.etsi.org/docbox/Workshop/@METIS_Kick-off/Presentations/E-gov%20interoperability%20in%20Brazil%20ePing.ppt, 2008.
12. http://www.governoeletronico.gov.br, 2008.
13. http://www.presidencia.gov.br/estrutura_presidencia/gsi/sobre, 2008.
14. http://www.presidencia.gov.br/estrutura_presidencia/casa_civil/atos/destaque/estreg_gsi/view?searchterm=5083, 2008.
15. http://www.planalto.gov.br/gsi/cgsi, 2008.
16. The current list of representatives is available here: http://www.planalto.gov.br/gsi/cgsi/, 2008.
17. Bruce, R., Dynes, S., Brechbuhl, H., Brown, B., Goetz, E., Verhoest, P., Luiijf, E., and Helmus, S. 30 June (2005). *International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues*. TNO Report 33680, Tuck School of Business, Dartmouth, Delft.
18. http://www.planalto.gov.br/gsi/cgsi, 2008.
19. http://www.mct.gov.br/index.php/content/view/2143.html, 2008.
20. http://www.mc.gov.br, 2008.
21. http://www.nic.br, 2008.
22. http://www.cetic.br, 2008.
23. http://www.globaliswatch.org/files/pdf/GISW_Brazil.pdf, 2008.
24. $MI^2C$ is described in Bezerra, E. K., Nakamura, E. T., Ribeiro, S. L. (2005). Critical telecommunications infrastructure protection in Brazil. *First IEEE International Workshop on Critical Infrastructure Protection*. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1572288.
25. http://www.first.org, 2008.
26. http://www.antiphishing.org, 2008.
27. http://www.ctir.gov.br, 2008.
28. http://www.cert.br/index-en.html, 2008.

29. http://www.cert.br/mission.html, 2008.
30. This list is accessible at http://www.cert.br/contact-br.html, 2008.
31. http://www.honeypots-alliance.org.br, 2008.
32. http://www.cenpra.gov.br, 2008.
33. http://www.honeypots-alliance.org.br/stats, 2008.
34. http://www.rnp.br/en/rnp/history.html, 2008.
35. For a more detailed list, see http://www.rnp.br/cais/sobre.html, 2008.
36. http://www.planalto.gov.br/casacivil/site/exec/arquivos.cfm?cod=560&tip=doc, 2008.
37. This section is based on: Goodman, M. D. and Brenner, S. W. (2002). The emerging consensus on criminal conduct in cyberspace. *UCLA Journal of Law and Technology*, **6**(1), http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php.
38. http://legis.senado.gov.br/pls/prodasen/prodasen.layout_mate_detalhe.show_materia?p_cod_mat=1463, 2008.
39. See also: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_technical_cooperation/cyber/567-LEG-country%20profile%20Brazil%20_30%20May%2007_pdf, 2008.
40. Senado Federal, Gabinete do Senador Eduardo Azeredo. (2007). Octopus interface conference—cooperation against cybercrime. *Cybercrime legislation in Brazil, Presentation by Senator Eduardo Azeredo*. Strasbourg, 11th June 2007.

# CANADA

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

In Canada, critical infrastructure (CI) consists of the physical and information technology facilities, networks, and assets essential to the health, safety, security, or economic well-being of Canadians, and the effective functioning of government [1]. Canada's federal government (i.e., the government of Canada, and each of the provincial and territorial

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

governments) structures its respective critical infrastructure programs as it deems appropriate. The government of Canada classifies critical infrastructure within the ten sectors listed below:

- Energy and Utilities,
- Communications and Information Technology,
- Finance,
- Health Care,
- Food,
- Water,
- Transportation,
- Safety,
- Government,
- Manufacturing [1].

The government of Canada recognizes that the nation's critical infrastructure could potentially be affected by both physical and cyber threats, whether natural or human-induced. Recognizing the complex nature of the threat environment, the government has adopted an all-hazards approach to protect critical infrastructure.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

Canada began implementing dedicated CIP and CIIP policies in 2001 in response to the new risk environment and the increasing interconnectedness of both physical and cyber-based infrastructures. In 2003, the government of Canada brought together the office responsible for critical infrastructure and emergency preparedness and the various agencies responsible for national security into one department, Public Safety and Emergency Preparedness Canada (PSEPC). This department, which is now called Public Safety Canada, was created to keep Canadians safe from a range of risks, including natural disasters, crime, and terrorism. Its responsibilities include ensuring a coordinated response to threats and developing initiatives and programs aimed at strengthening Canada's critical infrastructure [2].

Given the interdependencies and connectedness between critical infrastructures, the interruption of any one service could have a cascading effect and disrupt other essential services or systems. For example, during the North American Power Outage of 2003, large segments of rural and urban communities were in the dark: traffic and street lights were out; banking and government services were interrupted, and fuel distribution was disrupted. The disruption in one sector—electricity—affected a score of others, interrupting the delivery of important services to Canadians.

In light of this increasing interdependency, Public Safety Canada has taken a leadership role in promoting a national partnership among private and public-sector critical infrastructure stakeholders. This leadership has led to the development of the National Strategy and Action Plan for Critical Infrastructure (National Strategy and Action Plan).

### 2.1 The National Strategy and Action Plan for Critical Infrastructure

To address the need for coordinated action, federal, provincial, and territorial governments have drafted a National Strategy and Action Plan that will enhance the resiliency of Canada's critical infrastructure. Its goal is to build a safer, more secure, and more resilient Canada. To achieve this goal, the National Strategy sets out a model for public-private sector partnership, an information sharing framework, and a risk-based approach to protecting critical infrastructure. The Action Plan identifies near-term deliverables that will be used to establish national priorities, goals, and requirements so that funding and resources are applied in the most effective manner [3].

Achieving meaningful progress under the National Strategy and Action Plan calls for critical infrastructure partners to have:

- Risk-based plans and programs in place addressing and anticipating risks and threats;
- Access to robust information-sharing networks that include relevant intelligence and threat analysis; and
- Plans in place to identify and address dependencies and interdependencies to allow for more timely and effective response and recovery [3].

The public-private partnership described in the National Strategy and Action Plan provides the bedrock for effective critical infrastructure protection. Governments and private-sector partners each bring core competencies that add value to the partnership and enhance Canada's protective posture.

The government can support industry efforts and assist in broad-scale protection through activities such as:

- Providing owners and operators with timely, accurate, and useful information on risks and threats;
- Ensuring that industry is engaged as early as possible in the development of risk management activities and emergency management plans; and
- Working with industry to develop and prioritize key activities for each sector.

The federal government will establish sector networks for each of the ten critical infrastructure sectors, which will provide standing fora for public-private sector partners to engage in information exchange and address critical infrastructure priorities (e.g., identify and address risks, develop plans, and conduct exercises). The federal government will also establish a National Cross-Sector Forum, which will be composed of representatives from each of the ten sector networks. The Forum will identify and address cross-sector interdependencies, and provide advice and recommendations to the minister of public safety [3].

Risk management under the National Strategy and Action Plan builds on the Emergency Management Act [4], which requires federal ministers to identify risks, address these risks through plans and conduct exercises. This risk management approach includes:

- Risk profiles that identify and assess risks;
- Plans to protect the most vulnerable areas of critical infrastructure;
- Exercises to validate plans and protective measures; and

- Risk management tools and guidance.

The National Strategy and Action Plan for Critical Infrastructure represents the first milestone in the road ahead. This document identifies a clear set of goals and objectives and outlines the guiding principles that will underpin our efforts to secure infrastructure vital to our public health and safety, national security, governance, economy, and public confidence. Most importantly, it establishes a foundation for building and fostering a cooperative environment where governments and industry can work together to protect our critical infrastructure and secure the foundations of our country and way of life.

### 2.2 Information-Sharing

Information-sharing is one of the most significant issues in CIP and CIIP. Canada has been working to identify better ways to achieve this goal. Information-sharing can be viewed as a means to manage actions that can help deter, prevent, mitigate, and respond to the impact of a threat, as well as a tool to manage risk.

Government of Canada information-sharing practices related to CIP and CIIP are based on the principles articulated in the Access to Information Act (ATIA) [5], which include the public's right to access information held by the government of Canada along with specific exceptions to that right. For example, when confidential information is provided to the government of Canada by a foreign government, that information is protected by a specific and mandatory exemption in the Access to Information Act (ATIA) and cannot be disclosed.

Building on Canada's current system of safeguards, the Emergency Management Act[1] includes important amendments to the ATIA that protect specific critical infrastructure and emergency management information shared by private-sector owners and operators of Canada's critical infrastructure. This type of information will enable the government of Canada to develop comprehensive emergency management plans and mitigation and preparedness measures, improve warning capabilities, and develop better defenses and responses.

To support the information-sharing requirements in the National Strategy and Action Plan for Critical Infrastructure, Canada has developed two guides called "Information Sharing and Protection under the Emergency Management Act" [6] and "Identifying and Marking Critical Infrastructure Information Shared in Confidence with the Government of Canada" [7], both of which elaborate on the information protection measures in the Emergency Management Act. These guides form a framework that provides a clear structure for the process of establishing information-sharing relationships, and encourage consistent approaches among participants, while ensuring that such processes are workable for and relevant to all key stakeholders. The primary goals of Canada's information-sharing framework are to assess threats and vulnerabilities, improve warning and reporting capabilities, and analyze attacks to develop better defenses and responses.

## 3 ORGANIZATIONAL OVERVIEW

In Canada, the lead department dealing with CIP and CIIP is Public Safety Canada. As mentioned above, the department was created in 2003 out of the integration of the former

[1]See the chapter on Law and Legislation.

Department of the Solicitor General, the National Crime Prevention Centre, and the former Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP).

The premise for Public Safety Canada's CIP and CIIP efforts is accurate and timely threat information. The Integrated Threat Assessment Centre (ITAC) helps to arrange the information collected by various intelligence sources. In addition, the Permanent High-Level Forum on Emergencies was established to ensure cooperation between the federal and local governments.

In Canada, the private sector owns and operates more than 80 per cent of the nation's critical infrastructure. This underscores the need for effective relationships between the government of Canada and the private sector, and between all levels of government and the organizations involved in preventing and responding to the various potential threats.

## 3.1 Public Agencies

***3.1.1 Public Safety Canada.*** Public Safety Canada provides policy advice and support to the minister of public safety on issues related to public safety, including national security and emergency management, policing and law enforcement, interoperability and information-sharing, border management, corrections and conditional release, Aboriginal policing, and crime prevention. The Public Safety Canada portfolio also includes the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), the Correctional Service of Canada, the National Parole Board, the Canada Firearms Centre, the Canada Border Services Agency, and three review bodies [8].

Public Safety Canada continues the mandate given to the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) to combine critical infrastructure protection and emergency management responsibilities in one organization. This approach reflects the new risk environment, where the physical and virtual dimensions of infrastructures are increasingly interconnected. Combining critical infrastructure protection and emergency management resources and policy tools with acquired knowledge and experience in emergency management should ensure a stronger, more integrated and effective national security posture. Critical infrastructure protection and emergency management are not seen as separate endeavors, but as part of the assurance and protection continuum.

Public Safety Canada is the focal point for coordinating, analyzing, and sharing information related to physical and virtual threats to the Canadian critical infrastructure. Once it has received notification, the Government Operations Center, located in Public Safety Canada, assesses the threat to Canada and further distributes the bulletin and assessment to critical infrastructure owners and operators as well as emergency management contacts in Canada.[2]

***3.1.2 Integrated Threat Assessment Centre (ITAC).*** The Integrated Threat Assessment Centre (ITAC) [9] was created to facilitate the integration of intelligence from various sources into comprehensive threat assessments. These are based on intelligence and trend analysis evaluating both the probability and potential consequences of threats. Such assessments are aimed at assisting the government of Canada to coordinate activities in response to specific threats more effectively in order to prevent or mitigate risks to public safety.

Several federal government departments feed into ITAC, including: Public Safety Canada, the CSIS, the Department of National Defence, the Canada Border Services

[2]Information provided by an expert.

Agency, Foreign Affairs Canada, Transport Canada, the RCMP, the Communications Security Establishment, the Privy Council Office, and the Ontario Provincial Police [10]. The focus of the threat assessments is on events and trends related to domestic and international terrorism. Although the assessments are related to national security issues, they are produced at various levels of classification, allowing for a broader distribution. ITAC assessments are currently distributed to the federal government and foreign partners through ITAC; law enforcement agencies receive the assessments through the RCMP.

***3.1.3 Federal Provincial High-Level Forum on Emergencies.*** Major emergencies require extremely close cooperation between the federal government, provinces and territories, municipalities, and first responders. The government of Canada has therefore invited provinces and territories to establish a permanent high-level forum on emergencies in order to allow for regular strategic discussion of emergency management issues among key national players[2].

### 3.2 Public-Private Partnerships

The Canadian private sector, which owns and operates more than 80 per cent of the nation's infrastructure, plays a key role in securing cyberspace. National sector associations such as the Canadian Electricity Association (CEA), the Canadian Bankers Association (CBA), the Canadian Telecommunications Emergency Preparedness Association (CTEPA), and others have been active in promoting enhanced CIP/CIIP efforts. Currently, Canada's CI sectors are working to enhance information-sharing among their members, with government, and between sectors.

It is increasingly recognized that information on threats, vulnerabilities, corrective measures, and best practices should be shared widely across sectors and with governments. Canadian industry and governments at all levels are working together to improve information-sharing and analysis efforts. Industry sectors have identified a variety of challenges, including such issues as timeliness and relevancy of threat information. As industry efforts to increase cooperation and information-sharing mature, so will the national ability to respond to and manage cyber-incidents and attacks.[3]

## 4 EARLY WARNING

### 4.1 Canadian Cyber Incident Response Centre (CCIRC)

Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) [12] provides national and international leadership in cyber-readiness and response. CCIRC is Canada's national focal point for coordinating cyber-security incident response and monitoring the cyber-threat environment 24 hours a day, seven days a week.

CCIRC leverages the IT security capabilities of the federal government to provide the following services to critical infrastructure sectors:

- Incident response, coordination, and support;
- Monitoring and analysis of the cyber-threat environment;
- IT security-related technical advice;

[3]Cf. [11].

- National awareness and education (training, standards, best practices).

When warranted, Public Safety Canada issues cyber-alerts and advisories, as well as other cyber-related information products to respond to potential, imminent, or actual threats, vulnerabilities, or incidents affecting Canada's critical infrastructure. This information is made available to all levels of government, as well as to non-government organizations.

CCIRC will build upon existing international relationships and is designed for improved interoperability with its allied partners.

### 4.2 Government Operations Centre (GOC)

Public Safety Canada is home to the Government Operations Centre (GOC) [13]. The GOC operates 24 hours a day, seven days a week. Its purpose is to provide strategic-level coordination and direction on behalf of the government of Canada in response to an emerging or occurring event affecting the national interest. It also receives and issues information dealing with any emerging or occurring threat to the safety and security of Canadians and Canada's critical infrastructure.

Information received by the GOC is quickly verified, analyzed, and distributed to the appropriate response organizations. This is made possible through Public Safety Canada's close linkages with other government departments and agencies; provincial, territorial, and municipal governments; and the private sector.

Calling upon resources and experts in various fields, the GOC helps to ensure that the right resources are in the right place at the right time. It coordinates the response to calls for help from other government departments and agencies; provincial, territorial, and municipal governments; and the private sector.

## 5 LAW AND LEGISLATION

### 5.1 Canadian Criminal Code Sections

- 342.1 (1): Every one who, fraudulently and without colour of right, (a) obtains, directly or indirectly, any computer service, (b) by means of an electromagnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offense under paragraph (a) or (b) or an offense under section 430 in relation to data or a computer system, or (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offense under paragraph (a), (b) or (c) is guilty of an indictable offense and liable to imprisonment for a term not exceeding ten years, or is guilty of an offense punishable on summary conviction [14].
- 342.2 (1): Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component

thereof, the design of which renders it primarily useful for committing an offense under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offense contrary to that section, (a) is guilty of an indictable offense and liable to imprisonment for a term not exceeding two years; or (b) is guilty of an offense punishable on summary conviction [14].

- 430. (1.1): Every one commits mischief who willfully (a) destroys or alters data; (b) renders data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of data; or (d) obstructs, intercepts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto [15].

### 5.2 Emergency Management Act 2007

The Emergency Management Act (EMA) came into force in August 2007 and replaced its predecessor, the Emergency Preparedness Act 1985, with new and more comprehensive measures that strengthen the federal role in emergency management and critical infrastructure protection.

The purpose of the new Emergency Management Act (EMA) is to strengthen the readiness posture of the government of Canada to prepare for, mitigate the impact of, and respond to all hazards in Canada by emphasizing the need for a common and integrated approach to emergency management activities in the government of Canada. It recognizes that emergency management in an evolving risk environment requires a collective and concerted approach between all jurisdictions, including the private sector and non-governmental organizations. The act reflects a comprehensive, all-hazards approach to emergency management.

The EMA sets out the duties and responsibilities of the minister in providing national leadership by coordinating emergency management for the government of Canada. In particular, this involves:

- Coordinating the federal response to emergencies in Canada and the US;
- Establishing standardized elements for emergency plans within the government of Canada;
- Monitoring, evaluating, and testing the robustness of EM plans of government institutions;
- Enhancing cooperation with other jurisdictions and entities by promoting common standards and information-sharing.

The EMA also outlines the responsibilities of other federal ministers in carrying out their emergency management responsibilities.

The act addresses a common concern within the private sector: the confidentiality of the information shared with government, and specifically its protection from disclosure in response to a request under the Access to Information Act. Such releases could harm the competitive position and business reputation of service providers and prevents the building of trusted partnerships between industry and government. The importance

of information-sharing was recognized in the EMA with the inclusion a consequential amendment to the Access to Information Act that exempts from disclosure critical infrastructure and emergency management information that is shared in confidence with the government [4].

### 5.3 The Department of Public Safety and Emergency Preparedness Act 2005

The Department of Public Safety and Emergency Preparedness Act [16] is Public Safety Canada's enabling legislation that sets out the general powers, duties, and functions for the department. The act establishes the public safety minister's powers and authorities to secure public safety and emergency preparedness, and to provide leadership at the national level.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Claudia Zuccolo, Marta Khan, Michel De Jong, and Suki Wong of Public Safety Canada, who validated the content of this chapter.

## REFERENCES

1. http://publicsafety.gc.ca/prg/em/nciap/about-en.asp, 2008.
2. http://www.publicsafety.gc.ca/abt/index-eng.aspx, 2008.
3. Public Safety Canada (2008). *Working Towards a National Strategy and Action Plan for Critical Infrastructure. Draft for Consultation*, http://www.publicsafety.gc.ca/prg/em/cip/_fl/nat-strat-critical-infrastructure-eng.pdf.
4. http://www.publicsafety.gc.ca/media/nr/2007/bk20070807-eng.aspx, 2008.
5. http://laws.justice.gc.ca/en/showdoc/cs/A-1///en?page=1, 2008.
6. http://www.publicsafety.gc.ca/prg/em/cip/_fl/information-sharing-and-protection-under-the-ema-eng.pdf, 2008.
7. http://www.publicsafety.gc.ca/prg/em/cip/_fl/labelling-sensitive-cip-information-eng.pdf, 2008.
8. http://www.publicsafety.gc.ca/abt/wwa/index-eng.aspx, 2008.
9. http://www.itac-ciem.gc.ca/index-eng.asp, 2008.
10. http://www.itac-ciem.gc.ca/prtnrs/index-eng.asp, 2008.
11. Public Safety Canada *Working Towards a National Strategy*, op. cit., 2008.
12. http://www.publicsafety.gc.ca/prg/em/ccirc/index-eng.aspx, 2008.
13. http://www.publicsafety.gc.ca/prg/em/goc/index-eng.aspx, 2008.
14. http://laws.justice.gc.ca/en/showdoc/cs/C-46/bo-ga:l_IX-gb:s_335//en#anchorbo-ga:l_IX-gb:s_335, 2008.
15. http://laws.justice.gc.ca/en/showdoc/cs/C-46/bo-ga:l_X-gb:s_422//en#anchorbo-ga:l_X-gb:s_422, 2008.
16. http://laws.justice.gc.ca/en/P-31.55/index.html, 2008.

# ESTONIA

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Estonia is one of the most rapidly developing information societies in Central and Eastern Europe. Estonia attracted a lot of attention in 2005 when it carried out its first round of internet-based voting in the local government elections of 2005 (in 2007, Estonia even became the first country in the world to feature e-voting in parliamentary elections). These elections were the results of constant and ambitious efforts to foster the information society.

The uninterrupted functioning of information and communication infrastructures (ICTs) provides the basis for such a highly developed information society. Information security and the protection of critical information infrastructures are therefore essential parts of Estonia's security policy.[1]

There are following critical sectors as defined by the Emergency Preparedness Act (consolidated text July 2002): "Vitally important sectors and the ministries administering these are the following:

- Maintenance of public order, fire extinguishing and rescue work, organization of protection of data banks—the Ministry of Internal Affairs;
- Functioning of the energy and gas system, organization of supply with staple goods; organization of telecommunications and postal services, and transport—the Ministry of Economic Affairs and Communications;
- Organization of supply with foodstuffs—the Ministry of Agriculture;
- Functioning of the financial system—the Ministry of Finance;
- Organization of health care, social insurance and social welfare, provision of psycho-social help, assistance to refugees and the evacuated, labor force calculation—the Ministry of Social Affairs;
- Organization of protection of cultural property—the Ministry of Culture;

[1]Information security and CIIP became even more important after the online attacks on Estonian government sites of April/May 2007, which attracted worldwide attention.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- Organization of environmental protection and monitoring—the Ministry of the Environment.

The Ministry of Internal Affairs is the leading ministry in the field of crisis management" [1].

## 2 PAST AND PRESENT INITIATIVES AND POLICY

"I would not consider it an exaggeration to say that "e" has put Estonia back on the world map" [2]. This statement by Meelis Atonen, the then Minister of Economic Affairs and Communication in the preface of the policy paper Estonian IT Policy: Towards a More Service-Centered and Citizen Friendly State: Estonian Information Policy 2004–2006, outlines the importance of IT for Estonia.

Accordingly, the Estonian government has promoted various initiatives to strengthen the IT-sector. The first policy paper, Principles of Estonian Information Society, was set out in 1998. It was followed by the above-mentioned paper, which defined the principles of the Estonian information policy for 2004–2006; and since January 2007, the Estonian IT policy has been defined by the Estonian Information Society Strategy 2013.

Due to these strategies and their efficient implementation, Estonia succeeded in making considerable progress on the way towards an information society (for example, Estonia successfully launched new ID cards in 2002 that can also be used for issuing digital signatures and for using web-based services of the state) [3].

### 2.1 National Security Concept of the Republic of Estonia 2004

With the nation's rapid transformation into an information society, information security and the protection of communication infrastructure became important issues of national security. The National Security Concept 2004 therefore refers explicitly to the risks stemming from threats to information security. It is stated that "the constantly increasing rate at which electronic information systems are adopted in Estonia, and their connection with and dependence upon worldwide information systems, increases the threat of computer crime as well as the vulnerability of information systems, including spheres of primary importance to national security" [4].

### 2.2 National Information Security Policy

One of the aims of the policy paper for the Estonian information policy 2004–2006 was to define basic principles of a common IT security policy [5]. These basic principles were elaborated by a joint working group representing both the public and the private sectors and formulated in the National Information Security Policy.

The purpose of the Estonian Information Security Policy is to contribute to the development of a secure and security-aware information society. More specifically, the policy includes the following goals: elimination of non-acceptable risks to electronic communication networks and communication systems; defense of basic human rights; raising awareness about IT security and providing the respective training; participation in international initiatives related to e-security; and increasing the competitiveness of the Estonian economy [6].

In order to achieve these goals, the Estonian information security policy comprises five domains:

- *Cooperation and coordination at the national and international levels.* this domain includes initiatives such as the development and maintenance of a computer incident response capacity as well as participation in the European Network and Information Security Agency (ENISA);
- *Crisis management and cybercrime.* this domain includes preparations of crisis management plans and all initiatives designed to fight national and international cybercrime;
- *Education and training.* activities related to awareness-raising in government agencies as well as in the private sector and among the general public;
- *Legislation and regulation related to IT security.* specification, elaboration, and implementation of procedures, documentation, and means for ensuring information security;
- *Activities for the protection of people and assets.* protection of human rights and particularly of personal data.

As the Ministry of Economic Affairs and Communication states in the yearbook 2005 on Information Technology in Public Administration of Estonia [7], the Information Security Policy is designed to address IT security issues in the public sector as well as in the private sector.

In the same yearbook, information security is also clearly defined as part of critical infrastructure protection efforts: "The information security policy contributes to critical information infrastructure protection and takes into account information security aspects in other fields of critical information protection. The various fields of information security policy provide support and basic data for the protection of critical infrastructure and vice versa" [8].

### 2.3 Estonian ID Card

The Estonian ID card is not only a plastic card for the identification of its owner, but also contains a chip with a personal data file and two certificates enabling secure electronic authentication and digital signature [9]. It can be used for internet-based services provided by the Estonian government as well as for several services offered by the private sector.

Ninety per cent of the residents of Estonia already carry the new ID card. However, only a minority uses the ID card as an identification and authentication tool for digital services. The Estonian government, in cooperation with private-sector partners, tries to promote the usage of the ID card (see the chapter on Organizational Overview for the public-private initiative Computer Protection 2009).

### 2.4 Estonian Information Society Strategy 2013

Since January 2007, the new Estonian Information Society Strategy 2013 entered into force, setting out the general framework, objectives, and respective action fields for the development of the information society in Estonia. The strategy emphasizes the importance of cooperation between the public and private sectors and the need for coordination among all ministries involved.

Three objectives are mapped out by the strategy:

- *Development of a citizen-centered and inclusive information society.* the percentage of internet users in Estonia is to be further increased;
- *Development of a knowledge-based economy.* ICT uptake by enterprises is to be promoted and the competitiveness of the ICT sector to be increased;
- Development of citizen-centered, transparent, and efficient public administration by improving the efficiency of the public sector and providing user-friendly e-services in the public sector.

One of the principles for the development of the information society as defined in the document also refers to the importance of information security. It is stated that "the development of the information society must not undermine people's sense of security" [10]. Non-acceptable risk must be avoided, and personal data and identities must be secured.

### 2.5 The Estonian IT Interoperability Framework

The Estonian IT interoperability framework [11] is a set of standards and guidelines aimed at ensuring the provision of services for public administration institutions, enterprises, and citizens both in the national and in the European context. The latest version of the document (available in Estonian) [12] comprises the IT security interoperability framework, which specifies the activities related to CIIP and the use of the system of security measures by organizations.

### 2.6 The Estonian Cybersecurity Strategy

The Estonian Cybersecurity Strategy lays out the priorities and activities aimed at improving the security of country's cyberspace. The Cybersecurity Strategy concentrates on the following areas: the responsibilities of state and private organizations, vulnerability assessments of critical national information infrastructure, the response system, domestic and international legal instruments, international cooperation, and training and awareness-raising issues.[2]

## 3 ORGANIZATIONAL OVERVIEW

In Estonia, there is no single central authority responsible for CIIP. Several ministries and their respective subunits are directly involved. However, the main tasks of CIIP are assigned to the Ministry of Economic Affairs and Communication (MEAC) [13]. The MEAC plays a leading role with regard to information security, since two central agencies for the national IT policy are subordinated to the MEAC: The Department of State Information System (RISO), which is the central body for overall ICT coordination; and the Estonian Informatics Centre (RIA), which constitutes the implementing body under the MEAC. Other important public agencies that are dealing with CIIP are located within the Ministry of the Internal Affairs and within the Ministry of Defense. These two

[2]Information provided by an expert.

ministries are responsible for internal security and crisis management. With the project Computer Protection 2009, there is also an important public-private partnership, which aims to foster the security of the Estonian information society.

### 3.1 Public Agencies

***3.1.1 The Department of State Information System (RISO).*** Within the Ministry of Economic Affairs and Communication (MEAC), the Department of State Information System (RISO) [14] is responsible for overall ICT coordination. With regard to IT security, it ensures the involvement of the private sector and cooperation among the different IT managers of the governmental agencies. In order to improve the security of the governmental communication network, RISO also coordinates the actions of the county and local governments and launches and supports broad public awareness campaigns.

The department also prepares appropriate legislation drafts and defines standard procedures for e-government. These regulative measures are usually developed in coordination with other ministries and with the private sector.

At the international level, RISO participates in the European Network and Information Security Agency (ENISA), and is involved in other cross-border initiatives, such as the development of the International Telecommunication Union (ITU) Global Cybersecurity Agenda.

***3.1.2 The Estonian Informatics Centre (RIA).*** The Estonian Informatics Centre (RIA) was established to develop and manage data communication services for governmental organizations. Thus, the RIA is responsible for the technical security of the state's communication and information infrastructure. That includes measures to ensure the security of the governmental portals (which consists of three platforms on the internet);[3] preventive measures to maintain the security of the governmental data communication network; and monitoring and improving the overall security of IT in Estonia.

In 2005, the Estonian Computer Emergency Response Team (CERT) was established at RIA, in compliance with the obligation to form a national center for IT security, as laid out in the policy paper "Principles of the Estonian Information Policy 2004–2006". With the establishment of the Estonian CERT, the RIA has consolidated its role as the responsible body for the technical facets of CIIP. (For more information on the Estonian CERT, see the chapter on Early Warning and Public Outreach).

***3.1.3 The Estonian National Communications Board.*** The Estonian National Communications Board manages and regulates the postal sector as well as the market for electronic communications in Estonia. It is responsible for the management of limited communication resources (e.g., radio frequencies) as well as for the regulation of the electronic communications market in Estonia [15]. In this function, the National Communication Board oversees the companies operating in the field of electronic communications and ensures the compliance of these companies with security requirements.

[3]http://www.riik.ee, which is the e-government platform; http://www.eesti.ee, which is the information platform; and https://www.esti.ee, which is the citizens' portal.

***3.1.4 The Security Agencies.*** The task of the security agencies—the Security Police Board (belonging to the Ministry of Internal Affairs) and the Information Board (located within the Ministry of Defense)—is to ensure national security and maintain constitutional order through non-military preventive measures [16]. The functions of the Security Police Board are to prevent espionage, protect state secrets, and combat terrorism and corruption. The Information Board, in turn, collects intelligence concerning foreign countries and is responsible for the security of electronically transmitted information.

### 3.2 Public-Private Partnerships

***3.2.1 Computer Protection 2009.*** Computer Protection 2009 is a joint project of the Look@World Foundation and the Ministry of Economics and Communications. The Look@World Foundation was established in 2001 by ten leading companies in Estonia with the goal to foster the development of the IT society in Estonia.

The Computer Protection 2009 project (also called Look@World 2) aims to foster the security of the Estonian information society, so that in 2009, Estonia will be the country "with the most secure information security in the world" [17]. To achieve this ambitious goal, the signing partners of the initiative started broad promotion programs to raise public awareness of IT security. In particular, they try to encourage citizens to use their ID card for electronic personal authentication.

The main activities of the foundation, however, include sharing of information among companies, public agencies, and citizens on how to adequately recognize threats to information security and to protect oneself against them [18]. Improving and promoting internet security-related dialog and cooperation between the public and private sector is a distinctive concern of the Computer Protection 2009 initiative.

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 CERT Estonia

Established in 2005 at the Department for Handling Information Security Incidents of the Estonian Informatics Centre (RIA), the Computer Emergency Response Team of Estonia is responsible for the management of security incidents in the.ee computer networks. Its main task is "to assist internet users in Estonia in the implementation of preventive measures in order to reduce possible damage from security incidents and to help them in responding to security threats" [19]. This means that CERT Estonia offers support for incident handling and acts as an early-warning center for IT security.

The process of incident handling comprises the collection of information on incidents, analysis of attacks, and coordination of the response activities. However, since not all incidents are of the same importance, it is also important to assign priorities to each incident according to the severity level and scope. In assessing this prioritization, CERT Estonia takes the following aspects into account: the number of affected users; the type of incident; the target of an attack as well as the attack's point of origin; and the required resources for handling the incident [19]. Of course, attacks on critical infrastructures that may jeopardize people's lives would be considered to be incidents of highest priority.

In the domain of early warning, CERT Estonia cooperates with various national and international partners. The broad network enables the CERT to recognize new threats and vulnerabilities in a timely manner. Warnings are mainly issued in cases of attacks

with higher level of severity, extremely widespread threats, and highly severe vulnerabilities [20].

In addition, once CERT Estonia has managed to successfully launch the above-mentioned services, it also intends to contribute to the promotion of awareness-raising in the field of IT security [19].

### 4.2 Infosecurity Portal

When the Computer Protection 2009 initiative was launched, a gateway to IT security-related information and discussions was established that is available in Estonian and in Russian [21]. The portals contain numerous links, articles, and news, and enable the users to obtain and share information about threats related to the internet. The goal of the portal is to help citizens to familiarize themselves with the world of information security.

## 5 LAW AND LEGISLATION

Since 1997 Estonia enacted a series of laws with regard to CIIP in general. Estonia was also among the first countries to sign the Council of Europe's Convention on Cybercrime in 2001, and fully enacted it in 2004.

The following legal instruments are relevant to information security and CIIP:

- *Emergency Preparedness Act.* This act provides the legal basis for the organization of emergency preparedness of and for crisis management by the national government, government agencies, and local governments [1];
- *State Secrets Act.* defines state secrets, access to state secrets, and the basic procedure for the processing of state secrets [22];
- *Personal Data Protection Act.* This act determines the principles for processing personal data (Chapter 1). Paragraph 6 defines the principle of security, which is binding for all processors of personal data: "security measures to prevent the involuntary or unauthorized alteration, disclosure or destruction of personal data shall be applied in order to protect the data" [23];
- *Public Information Act.* The purpose of this act is to ensure that the public and every person has the opportunity to access information intended for public use, based on the principles of a democratic and social rule of law and an open society, and to create opportunities for the public to monitor the performance of public duties. The act defines the state information system, describes the organization of databases belonging to a state information system, and lays out the legal basis for providing and using data services. The act provides for an approach integrating different areas of government through legislation that defines the administrative system of the state information system and other support systems for the state information system, as well as the status of databases established within the information system of the public sector [24];
- *Electronic Communications Act.* This act defines the requirements for the publicly available electronic communications networks and communications services. With regard to CIIP, the security requirements are of particular interest: "A communications undertaking must guarantee the security of a communications network and prevent third persons from accessing the data [ . . . ] without legal grounds" [25];

- *Information Society Services Act.* This act provides the requirements for information society service providers, the organization of supervision, and liability for violation of this act [26].

### 5.1 Penal Code

Several articles of the Estonian penal code refer to information security:

- *Article 206 (Computer sabotage).* Unlawful replacement, deletion, damaging or blocking of data or programs in a computer, as well as unlawful entry of data or programs in a computer is punishable by fines or imprisonment.
- *Article 207.* Damaging or obstruction a connection to a computer network or computer system is punishable.
- *Article 208.* Spreading computer viruses is punishable by fines or imprisonment.
- *Article 217.* Unlawful use of a computer, computer system, or computer network by way of removing a code, password, or other protective measures is punishable by fines or imprisonment.
- *Article 284.* Unlawfully handing over the protection codes of a computer, computer system, or computer network, if committed for the purpose of personal gain and in a manner which causes significant damage or results in other serious consequences, is punishable by fines or imprisonment.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Thomas Viira of the Estonian Informatics Center and Jaak Tepandi of the Institute of Informatics, Tallinn University of Technology, who validated the content of this chapter.

## REFERENCES

1. http://www.rescue.ee/index.php?page=143&PHPSESSID=220faec9593e393510ea6f39fef5a197, 2008.
2. Meelis, A., Ministry of Economic Affairs and Communication Preface. In " *Estonian IT Policy: Towards a More Service-Centered and Citizen-Friendly State. Principles of the Estonian Information Policy 2004–2006*, http://www.riso.ee/en/files/Policy.pdf, 2008.
3. http://www.id.ee/?id=11019, 2008.
4. http://web-static.vm.ee/static/failid/067/National_Security_Concept_2004.pdf, 2008.
5. http://www.riso.ee/en/files/Policy.pdf, 2008.
6. http://www.riso.ee/en/information-policy/security, 2008.
7. Ministry of Economic Affairs and Communications of Estonia (2005). *Information Technology in Public Administration of Estonia 2005*, p. 33. http://www.riso.ee/en/pub/yearbook_2005.pdf, 2008.
8. Ministry of Economic Affairs and Communications of Estonia (2005). *Information Technology in Public Administration of Estonia 2005*, p. 48. http://www.riso.ee/en/pub/yearbook_2005.pdf, 2008.

9. Ministry of Economic Affairs and Communications of Estonia (2006). *Information Technology in Public Administration of Estonia 2006*, p. 23. http://www.riso.ee/en/pub/2006it/, 2008.
10. Estonian government *Estonian Information Society Strategy 2013*, p. 4. http://www.riso.ee/en/files/IYA_ENGLISH_v1.pdf, 2008.
11. http://www.riso.ee/en/information-policy/interoperability, 2008.
12. http://www.riso.ee/wiki/Pealeht, 2008.
13. http://www.mkm.ee/index.php, 2008.
14. http://www.riso.ee/en/, 2008.
15. http://www.sa.ee/atp/?id=3476, 2008.
16. Estonian government (2004). *National Security Concept of the Republic of Estonia 2004*, p. 16.
17. http://www.riso.ee/en/node/80, 2008.
18. Ministry of Economic Affairs and Communications of Estonia (2006). *Information Technology in Public Administration of Estonia 2006*, p. 42, 2008.
19. http://www.ria.ee/28201, 2008.
20. Ministry of Economic Affairs and Communications of Estonia (2005). *Information Technology in Public Administration of Estonia 2005*, p. 36, 2008.
21. The Estonian version is available at http://www.arvutikaitse.ee; the Russian one can be found at http://www.infosecurity.ee, 2008.
22. http://www.legaltext.ee/text/en/X30057K7.htm, 2008.
23. http://www.legaltext.ee/text/en/X70030.htm, 2008.
24. http://www.esis.ee/ist2004/106.html, 2008.
25. http://www.legaltext.ee/text/en/X90001K2.htm, Chapter 10, Paragraph 101, 2008.
26. http://www.legaltext.ee/text/en/X80043.htm, 2008.

# FINLAND

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Finland aims to ensure society's ability to function in all circumstances by securing the functioning of both official infrastructures and those administered by individual citizens and businesses. Consequently, as an information society, Finland can only function smoothly if its critical information infrastructure is fully operational, because any disruptions may result in dramatic consequences.

The critical sectors and the protection policies for critical infrastructures are defined in the Security of Supply Act and in the Decree of the National Emergency Supply Agency (NESA) of 1992.[1] Based on these acts, the Finnish government sets official goals for the development of security of supply, which are updated every 5–6 years. The current governmental decision is from 2002, but there is already a proposal for a new decision, which is to be enacted in 2008 (the critical infrastructure will be defined in more detail, but the definition will include the same sectors as in 2002).[2]

Currently, the following infrastructures and services are deemed to be critical in Finland:

[1]The Security of Supply Act is the legal basis for ensuring supplies of various basic materials in the case of emergency situations. Based on this act, the National Emergency Supply Agency (NESA), a subordinate agency to the Ministry of Trade and Industry (now Ministry of Employment and the Economy), was founded in 1993 for the development and maintenance of security of supply. NESA is the national stock-holding agency of Finland.
[2]Information provided by an expert.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- Energy Networks and Supply,
- Electronic Information and Communication Systems, including communication networks, IT systems (including SCADA systems), electronic mass media, and payment systems of banks and insurances,
- Transportation and Logistics Systems,
- Water supply and Other Municipal Utilities,
- Infrastructure Construction and Maintenance,
- Financial Services,
- Food Supply,
- Health Services,
- Print Media.

The government focuses on safeguarding society's critical infrastructure. The objective is to protect fundamental structures by using non-critical technology and organizations, even during disturbances and emergency situations. Accordingly, an essential aspect of safeguarding the technology is ensuring the system's ability to recover.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

### 2.1 Governmental Support for the Information Society

From the early 1990s on, the Finnish government has worked continuously on new programs aimed at promoting the Information Society, its infrastructure, and the protection of the infrastructure. On the basis of their reports, several ministries have produced action plans and provided funding for Information Society projects.

In 2005, the Finnish government issued a strategy resolution, which includes an Information Society Programme [1]. This program promotes the development of the Information Society in the areas of telecommunication infrastructure, digital television, citizens' skills to utilize the Information Society, research and development, and ICT in public administration and business.

As part of the implementation of this program, the government drafted the National Knowledge Society Strategy for 2007–2015 [2]. The vision of the strategy is "good life in information society", and accordingly, it aims to support the "transformation of Finland into an internationally attractive, human-centric and competitive knowledge and service society" [3].

As the previous strategies in regard to the information society, the National Information Society Strategy 2007–2015 emphasizes the security of networks so that citizens can trust the electronic services. In addition it highlights the importance of well-functioning infrastructures: "Information networks are dependent upon basic infrastructure, such as electricity supply. Security of supply in the information society is especially important in crisis situations" [4].

### 2.2 Strategy for Securing the Functions Vital to Society 2006

In order to ensure the security of critical infrastructures, the Finnish government issued the Strategy for Securing the Functions Vital to Society [5]. The strategy was first released in 2003 and was reviewed and updated in 2006 [6].

The strategy paper divides the vital functions into seven broad areas: management of government affairs, international activities, national military defense, internal security, functioning of the economy and infrastructure, the population's income security and capability to function, and psychological crisis tolerance.

Electronic information and communication systems are recognized as an important part of a well-functioning society. It is vital to secure electronic communication networks and their information security, to determine basic security levels for services and technical systems, and to ensure that the regulations on construction and maintenance of systems are observed. In addition, it is critical to coordinate the development of networks used by the authorities, to safeguard the state's information-processing capacity, and to provide guidelines for public electronic services, the public data administration, and information security. Among vital threats to society, the strategy paper lists threats to information and communication systems first.

### 2.3 Security and Defense Policy 2004

The Finnish government submits a Security and Defense Policy report to parliament every three or four years. The next report will be published in 2008. In 2004 [7], the report emphasized the growing importance of electronic information and communications technology systems for the functioning of modern society. It is no longer possible to shift to the use of manual reserve systems.

Along with the rest of society, criminals also use networks and systems. Therefore, specific chapters in this policy paper are devoted to combating cyber-crime and to securing society's electronic communications and information systems. According to the report, the capacity of the police for protecting information systems, telecommunication connections, and electronic transactions, as well as for combating cyber-crime, will be expanded. Cooperation between the police and the Finnish Communications Regulatory Authority (FICORA) will raise the level of information systems protection required in an open network environment.

The security level of communication networks is being increased. ICT used by major government agencies, security authorities, and vital industries are safeguarded by prioritization and by the construction of communication networks and data systems for special use. One example is Finland's Public Authority Network VIRVE.[3]

### 2.4 National Information Security Strategy

In 2001, the government set up an Advisory Committee for Information Security (ACIS) under the Finnish Communications Regulatory Authority (FICORA) as a point of contact for citizens, companies, organizations, and authorities on information security issues.

In 2002, ACIS released its "National Information Security Strategy Proposal" [8], which was approved by the government in 2003. The paper lists detailed policy objectives and measures to be implemented as well as the responsibilities of the various stakeholders. The priority areas of the strategy are to secure electronic services, to secure biometric identification, to protect critical infrastructure, to combat cyber-crime, to protect the national information assets, to enhance information security awareness by promoting

[3]Finland's Public Authority Network VIRVE, based on TETRA (Terrestrial Trunked Radio) technology, is being expanded by increasing the number of users. Among the user groups are fire and rescue services, police, border guards, customs, the military, and health services. http://www.virve.com.

the annual National Information Security Day, and to improve awareness in business enterprises.

The most visible result of the implementation of the strategy has been National Information Security Day on 11 February, held for the fifth time in 2008. The day promotes secure internet usage, particularly for schoolchildren and their parents. Another important result is the strengthening of the national Computer Emergency Response Team (CERT-FI) to give special service for actors in critical sectors in Finland.[2]

## 3 ORGANIZATIONAL OVERVIEW

In Finland, there are three major public agencies dealing with CIIP. The Finnish Communications Regulatory Authority (FICORA) promotes the Information Society, as well as technical regulation and standardizations; the National Emergency Supply Agency (NESA) analyzes threats and risk against critical (information) infrastructures; and finally, the Steering Committee for Data Security in State Administration (VAHTI) develops policy guidelines and practical guides for the security of information systems.

In addition, there are three important public-private partnerships in the field of CIIP: The National Emergency Supply Council (NESC), the Ubiquitous Information Society Advisory Board, and the Finnish Information Society Development Centre (TIEKE).

### 3.1 Public Agencies

***3.1.1 Finnish Communications Regulatory Authority (FICORA).*** The Finnish Communications Regulatory Authority (FICORA) [9] belongs to the Ministry of Transport and Communications. FICORA is a general administrative authority for issues concerning electronic communications and Information Society services. Its mission is to promote the development of the Information Society in Finland. The specific duty of FICORA is to safeguard the functionality and efficiency of the communications markets in order to ensure that consumers have access to competitive and technically advanced communications services that are affordable as well as of good quality.

FICORA's mission includes issuing technical regulations and coordinating standardization at the national level. It also oversees the protection of privacy and securing data in electronic communications. In addition, FICORA encourages national and international co-operation.

FICORA also ensures that telecommunications operators are prepared for emergencies. The operators must report significant information security incidents as well as any threats, faults, or disturbances in telecommunication networks and services to FICORA. FICORA checks the operators for compliance with the Communications Market Act and the Act on the Protection of Privacy in Electronic Communications and monitors compliance with the relevant technical regulations and standards. In pursuing this task, FICORA collects information from the operators and conducts inspections.

Finally, FICORA operates the CERT-FI (see the chapter on Early Warning and Public Outreach), which is tasked with the detection and resolution of data security infringements [10].

***3.1.2 National Emergency Supply Agency (NESA).*** The National Emergency Supply Agency (NESA) [11] is the cross-administrative operative authority for the security of

supply in Finland. NESA works under the auspices of the Ministry of Employment and the Economy. In addition, NESA serves to develop cooperation between the public and private sectors in the field of economic preparedness, in coordinating preparations within the public administration, and in developing and maintaining the security of supply.

NESA and the National Emergency Supply Council (NESC, see below) analyze threats and risks that may affect the critical infrastructure. NESA itself conducts research and finances research commissioned by outside organizations. NESA and NESC formulate plans and guidelines for public authorities and businesses with respect to the management and control of such threats and risks.

NESA has a growing role in securing the critical national infrastructure by developing and financing both technical backup systems and electromagnetic pulse (EMP)-secure premises for systems. Finland's vital communication and IT systems are located in the capital region. This is a risky concentration. Therefore, NESA owns two computer backup/colocation centers outside the capital region in order to secure society's critical IT systems in exceptional conditions.[2]

The National Fixed Line Telephone Backup Network is a digital, nation-wide separate network that was built to secure the lines of communication of vital public organizations, as well as other key subscribers, in exceptional situations and crises. The Ministry of Transport and Communications and NESA are jointly developing the network so that it can also secure other telecommunication services than voice services. NESA is involved in the development and maintenance of Finland's Public Authority Network VIRVE.

In addition, NESA has financed several projects to secure the communication and broadcast systems. These projects and activities are related to reserve systems, emergency and warning message broadcasting systems, and the construction of circuitous routes for critical nodes of networks.

In CIIP matters, NESA has participated in the preparation of European Programme for Critical Infrastructure Protection (EPCIP) and Critical Infrastructure Warning Information Network (CIWIN).[2]

***3.1.3 Steering Committee for Data Security in State Administration (VAHTI).*** The central government's data-security and information-management policies are steered and developed by the Ministry of Finance. Guidelines are developed by the Steering Committee for Data Security in State Administration (VAHTI) [12], a broad group of experts.

For the central government, the issue of data security includes a number of areas such as the use of the internet, data management outsourcing, remote work, e-mail, protection from viruses, personnel security, physical security, data communication security, and database security. The Ministry of Finance works in close cooperation with other ministries and agencies to support and facilitate cooperation in the development of e-government and electronic services in the state sector.

VAHTI has published an extensive collection of practical guides (some of them in English) for information system security. The guides are intended for the state administration, but they are also used by many private organizations.[2]

## 3.2 Public-Private Partnerships

***3.2.1 National Emergency Supply Council (NESC).*** Established in 1955, the National Emergency Supply Council (NESC, previously National Board of Economic Defense)

[13], under the auspices of the Ministry of Employment and the Economy, supports and assists NESA activities (see also chapter on Law and Legislation). NESC also plans and coordinates economic preparations for implementation in case of exceptional circumstances in Finland.

NESC is a network of committees consisting of the leading experts from both the public administration and the business world. Its tasks are to analyze threats against the country's security of supply, to plan measures to control these threats, and to promote readiness planning in individual industrial sites.

NESC's areas of responsibility include the Information Society, transport logistics, food supply, energy supply, health care services, financial services, and defense-related and other critical industrial sectors. NESC members include representatives of ministries, government agencies, the private business sector, and various industrial organizations. Approximately 800 people work within the NESC.

NESC has several planning bodies in the area of information infrastructure. They have prepared instructions and basic plans for the ICT sector as well as for other vital branches of the infrastructure. In addition, NESC studies and follows up on risks and threats to the critical infrastructure and security of supply. Databases and methods have been developed to support and improve the level of readiness to act in exceptional situations.

***3.2.2 Ubiquitous Information Society Advisory Board.*** The Ubiquitous Information Society Advisory Board [14] is a body with members from ministries, public administration, NGOs, and business life. Its task is to ensure that the National Information Society Strategy will be put into practice.

One of the six working groups in the board has the task of outlining a new national information security strategy and of coordinating its implementation. The working group's term of office will last from September 2007 to February 2011.[2]

***3.2.3 Finnish Information Society Development Centre (TIEKE).*** Since 1998, the Finnish Information Society Development Centre (TIEKE) [15] has been a key player in the development of the Information Society in Finland. TIEKE's goal is to create viable tools and expertise for use in the Information Society. Specifically, TIEKE's main focus is on the development of networking and interoperability.

TIEKE's membership includes more than 100 organizations and companies involved in the Information Society. The members operate in the areas of trade, industry, and public administration, and thus also serve individual citizens.

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 Computer Emergency Response Team Finland (CERT-FI)

FICORA's CERT-FI [10] group prevents, observes, and solves information security violations and gathers information on threats to information security. CERT-FI cooperates with national and international CERT actors and representatives of trade and industry. It is in contact with suppliers of equipment, networks, and software as well as with the police and other authorities.

CERT-FI receives notifications from telecommunications operators concerning information security incidents and threats. In addition, CERT-FI continuously follows up

current global events related to information security, security problems of information systems, security incidents, and responses to them.

In 2007, CERT-FI was contacted 2664 times. The information security helpline for customers operates during business hours, but the threats and incidents are supervised around the clock, seven days a week.

Starting in 2007, CERT-FI's manpower was substantially increased. CERT-FI now also provides special service for actors in critical sectors in Finland. The special service includes a 24/7 incident warning and handling service (available also via SMS and via the VIRVE Public Authority Network), personal advice, and focused product vulnerability warnings.

## 5 LAW AND LEGISLATION[4]

### 5.1 Bill for National Emergency Supply Council 2008 / Act on the National Board of Economic Defense 1960

The Act on the National Board of Economic Defense (NBED) (238/1960) [16] is the legal basis for the National Emergency Supply Council (NESC). It obliges the NBED to plan and organize activities needed to secure the economy and the livelihood of the population in exceptional situations. NBED has the legal right to obtain, from enterprises and other important actors, information that is necessary for performing its planning and organizational tasks.

In 2008, a bill for amendment of the Act on the National Board of Economic Defense was introduced to the parliament. According to the bill, the name of the board will be changed to National Emergency Supply Council (NESC). The board of directors will be shared with the National Emergency Supply Agency (NESA). The committee network and the legal jurisdiction will remain unchanged.

### 5.2 Emergency Powers Act 1991

In case of serious disturbances and in emergencies, public authorities need special powers to safeguard society's essential activities. The most important provisions are contained in the Emergency Powers Act (1080/1991). [17] In crisis situations, this law empowers the government to issue provisions concerning the critical infrastructures and other functions of society.

In 2008, a bill for amendment of the Emergency Powers Act was introduced to the parliament. Under the provisions of the bill, the conditions in which the emergency powers can be implemented are specified in more detail than in the existing act, in harmony with the new Constitution of Finland of 2000.[2]

### 5.3 Security of Supply Act 1992/2005

Critical infrastructure protection actions are based on both the Security of Supply Act (1390/1992) [18] and the Decree of the National Emergency Supply Agency (NESA)

[4]The official texts of Finnish legislation have been published in Finnish and Swedish. Some laws have an unofficial English translation. Unless otherwise indicated, we refer to the official texts.

(1391/1992). [19] The Finnish government specified the development of security of supply as one of the official goals for 2002. [20] The Security of Supply Act was amended in 2005 (688/2005). [21] The amendment refers to severe disturbances in otherwise normal circumstances (not only in crisis situations as defined in the Emergency Powers Act). The amendment emphasizes the securing of technical systems.

### 5.4 Penal Code

In the Finnish Penal Code, Chapter 38, Amendments 578/1995[22] and 540/2007 [23] specifically outlaw the endangering of information systems, and tampering with telecommunication systems.

### 5.5 Act on Television and Radio Operations 1998

This act (744/1998) [24] obliges television or radio broadcasters to ensure that they can continue transmitting with minimum disruption even in the exceptional circumstances referred to in the Emergency Powers Act. Additionally, broadcasters must transmit information from the authorities to the public if it is necessary to save human lives, protect property, or safeguard the functioning of society.

### 5.6 Act on Provision of Information Society Services 2002

This act (458/2002) [25] defines the rules of offering electronic services and the right of the authorities to limit the services if they constitute threats to consumers or to public security.

### 5.7 Communications Market Act 2003

This act (393/2003) [26] obliges the communications operators to ensure the functioning of their services, regardless of whether the disturbances occur during normal times, exceptional situations, or in times of crises. The act assures the telecommunications operators that any extra expenses incurred through such preparatory measures will be reimbursed to the operators by the National Emergency Supply Agency (NESA).

An amendment is being prepared which would specify the roles and authority of the Ministry of Transport and Communications and FICORA in detail, in accordance with the new Emergency Powers Act.

### 5.8 Act on the Protection of Privacy in Electronic Communications 2004

This Act (516/2004) [27] states that telecommunications operators or service providers must secure their services and inform the authorities about any violations. The operators or providers have the right to eliminate any programs that threaten information security. They may also limit or stop the traffic when necessary for the protection of information security.

The Amendment (198/2006) [28] obligates the operator also to transmit authority originated emergency SMS messages that are addressed to specified recipient groups.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Veli-Pekka Kuparinen, Ilkka Kananen, and Hannu Sivonen of the National Emergency Supply Agency who validated the content of this article.

## REFERENCES

1. The Finnish Government (2005). *Information Society Programme,* (April). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/11233297000000607/default/tietoyhteiskuntaojelma_en_2005.pdf.
2. The Finnish Government (2006). *National Knowledge Society Strategy for 2007–2015,* (September). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/762226-90188788831/default/Strategia.
3. The Finnish Government (2006). *National Knowledge Society Strategy for 2007–2015,* (September). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/762226-90188788831/default/Strategia, p. 4.
4. The Finnish Government (2006). *National Knowledge Society Strategy for 2007–2015,* (September). http://www.tietoyhteiskuntaohjelma.fi/esittely/en_GB/introduction/_files/762226-90188788831/default/Strategia, p. 12.
5. The Finnish Government (2003). " *Strategy for Securing the Functions Vital to Society*, http://www.defmin.fi/files/168/2587_2047_Government_Resolution_On_Securing_The_Functions_Vital_To_Society_1_.pdf.
6. The Finnish Government (2006). " *Strategy for Securing the Functions Vital to Security*, http://www.defmin.fi/files/858/06_12_12_YETTS_in_english.pdf.
7. The Finnish Government (2004). *Finnish Security and Defence Policy,* http://www.defmin.fi/files/311/2574_2160_English_White_paper_2004_1_.pdf.
8. Advisory Committee for Information Security (2002). *National Information Security Strategy Proposal*, http://www.ficora.fi/englanti/document/infos.pdf.
9. http://www.ficora.fi/en/index/viestintavirasto/esittely.html, 2008.
10. http://www.cert.fi/en/index.html, 2008.
11. http://www.nesa.fi, 2008.
12. http://www.vm.fi/vm/en/13_public_management_reforms16746/051_state_it/001_state_it_organisation/index.jsp, 2008.
13. http://www.nesa.fi/organisation/national-board-of-economic-defence, 2008.
14. http://www.arjentietoyhteiskunta.fi/inenglish, 2008.
15. http://www.tieke.fi/in_english/about_tieke, 2008.
16. Act on the National Board of Economic Defence (NBED) (238/1960). http://www.finlex.fi/fi/laki/alkup/1960/19600238, 2008.
17. Emergency Powers Act (1080/1991) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/1991/en19911080.pdf, 2008.
18. Security of Supply Act (1390/1992). http://www.finlex.fi/fi/laki/ajantasa/1992/19921390.
19. The Decree of the National Emergency Supply Agency (NESA) (1391/1992). http://www.finlex.fi/fi/laki/ajantasa/1992/19921391.

20. Government decision on the Goals of Security of Supply (2002). http://www.finlex.fi/fi/laki/alkup/2002/20020350.
21. The Amendment of the Security of Supply Act (688/2005). http://www.finlex.fi/fi/esitykset/he/2005/20050044.
22. Penal Code Chapter 38 Amendment (578/1995) (unofficial English translation). http://www.finlex.fi/pdf/saadkaan/E8890039.PDF.
23. http://www.finlex.fi/fi/laki/alkup/2007/20070540?search%5Btype%5D=pika&search%5Bpika%5D=540%2F2007.
24. Act on Television and Radio Operations (744/1998) (unofficial English translation). http://www.finlex.fi/fi/laki/kaannokset/1998/en19980744.pdf.
25. Act on Provision of Information Society Services (458/2002) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/2002/en20020458.pdf.
26. Communications Market Act (393/2003) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf.
27. Act on the Protection of Privacy in Electronic Communications (516/2004) (unofficial English translation). http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf.
28. http://www.finlex.fi/fi/laki/alkup/2006/20060198?search%5Btype%5D=pika&search%5Bpika%5D=198%2F2006.

# FRANCE

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

All infrastructures that are vital to the maintenance of primary social and economic processes are considered critical sectors in France. These critical sectors are the following:[1]

[1]Decree No. 2006-212 dated 23 February 2006 on the protection of essential economic sectors. Information provided by an expert.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- Finance,
- Industry,
- Energy,
- The work of the judiciary,
- Public Health,
- The work of national civil authorities,
- Electronic Communication, Audiovisual Media, and Information Technology,
- Transport Systems,
- Water Supply,
- Food,
- Space and Research,
- The Armed Forces.

A decree was issued in 2006 on the protection of essential economic sectors;[1] it aims to upgrade regulations pertaining to vulnerabilities by harmonizing the interagency state approach for analyzing hazards in terms of the nature of the threat, while expanding the list of issues to be taken into account and by including the flexible measures provided for within the framework of the Vigipirate plan.[2] Thus, each of the 12 essential economic sectors will include a national security directive for essential operators, who are in turn tasked with setting up their own operator security plan under the supervision of the ministry they are subordinated to; this plan is also intended for other major agencies to set up their own protection plans.

The French regulatory framework has been updated accordingly. Its approach is based on risk management and prevention/reaction plans. The national committee, the interdepartmental commission, and the defense and security delegates are encouraged to share information. The above-mentioned 12 sectors and the actors therein have to elaborate a national security directive, and all operators are instructed to refine the national security directive into an operator security plan for their specific context. For each critical point, the operators have to refine the operator security plan into particular protection plans, and the authorities are directed to elaborate an external protection plan.[3]

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

### 2.1 Government Action Program for an Information Society (PAGSI)

In August 1997, the prime minister of France designated the information and communication society as a priority for government action. The objective was to build an information society for all, to prevent a digital divide, and to help France catch up with other countries in terms of internet usage. Making government services available online has been the main goal of the formation of the Government Action Program for an Information Society (PAGSI) [1] (adopted at the meeting of the Inter-ministerial Committee

[2]Vigipirate is France's national security alert system. Created in 1978, it has since been activated three times, in 1995, 2000, and 2004. For more information, see: http://www.archives.premier-ministre.gouv.fr/raffarin_version2/information/fiches_52/plan_vigipirate_50932.html.

[3]Information provided by an expert.

for Information Society (CISI) in January 1998) [2]. In addition to the improvement of general public services, standardization, and training for civil servants, the action plan supported projects in the fields of education, culture, electronic commerce, and research and innovation, and established appropriate regulations for the safer use of information technologies and networks. Two of the main priorities of the action plan were managing the Security of Information Systems (SSI) and combating cyberthreats [3].

### 2.2 Expression of the Needs and Identification of Security Objects (EBIOS)

In 1997, the Central Information Systems Security Division (DCSSI) developed and published the first version of the guide Expression of the Needs and Identification of Security Objects (EBIOS). Since then, it has been regularly updated and expanded [4]. EBIOS outlines methodological tools for risk analysis concerning the security of information systems. The method allows for communication about information systems security within organizations and between the individuals concerned. The methodological framework of EBIOS consists of tools for apprehending the method, for training, and for contributing to its shared development [5].

### 2.3 State Information System Security Reinforcement Plan (2004–2007)

The director of the French Prime Minister's Office instructed the ministerial departments and the General Secretariat of National Defense to prepare a specific plan of action by October 2003 to "secure the main central and local governmental networks, and those used for vital infrastructure management" [6]. This plan of action was approved on 16 December of the same year. The so-called "State Information System Security Reinforcement Plan" had the following four objectives [5]:

- To secure communication channels for senior state officials; that is, to ensure, under all circumstances, the security of all protected communication means for the use of senior authorities, based on supervision under the direct control of state authorities;
- To secure government information systems; that is, to secure the new e-government functions in accordance with the Agency for the Development of Electronic Administration's (ADAE) [7] strategic e-government plan and guidelines, and to explain security policies;
- To set up operational capabilities to respond to computer attacks;
- To include the French information system security policy within the scope of the French security policy in the EU.

### 2.4 Plan RE/SO 2007

The Plan for a Digital Republic within the Information Society (Plan pour une République numérique dans la societé de l'information) was presented by the prime minister in 2002. Acknowledging the necessity and importance of information and communication technologies for French economic growth, employment, and overall "influence in the world", this plan aims at giving a new impetus to the information society by focusing on the efficient development and use of an ICT infrastructure. Specifically, it strives to simplify the rules governing the internet, to restore the trust of the users, and to clarify the responsibilities of all actors within the information society [8].

### 2.5 Defense and National Security Whitebook

In June 2008, French President Nicolas Sarkozy announced the most wide-ranging reform of the French armed forces since 1994. The Defense and National Security Whitebook (Défense et Sécurité nationale: Le Livre Blanc) [9] states that global terrorism poses the most virulent threat to the security of France and its citizens. The document outlines the French military strategy to face this challenge until 2020 [10]. It not only anticipates a major reduction in the personnel strength of the armed forces, but also simultaneously foresees a substantial increase in their funding. Funding for military intelligence, for example, will be doubled. These funds are intended to be used to strengthen satellite surveillance and ICT in general in order to prevent cyber-attacks. France also plans to develop offensive means to prevent cyber-attacks. Under the terms outlined in the whitepaper, up to 10,000 troops will be dedicated to the prevention of pandemics induced by chemical and biological attacks, and of cyber-attacks. The Defense and National Security Whitebook is scheduled to be discussed in the French parliament in June 2008 [11].

## 3 ORGANIZATIONAL OVERVIEW

In France, the secretary-general of national defense (SGDN) [12], a secretary attached to the Prime Minister's Office, bears complete responsibility for organizing CIP.

Furthermore, within the Ministry of Defense, the key organizations responsible for CIP/CIIP are the Central Directorate for Information Systems Security (DCSSI),[4] the Inter-Ministerial Commission for the Security of Information Systems (CISSI),[5] and the Advisory Office, whereas the Central Office for the Fight Against Hi-Tech Crime plays a leading role within the Ministry of the Interior.

As a public-private partnership, the Strategic Advisory Board on Information Technologies (CSTI) strives to bring together government officials, business and industry executives, and representative of the research and development community.

### 3.1 Public Agencies

***3.1.1 Secretariat-General for National Defense (SGDN).*** The secretary-general for national defense (SGDN) deals with national and international security affairs. The organization was first called into action with regard to information security for Y2K. A specific network of contacts among different bodies from the public and private sectors became involved under the coordination of the SGDN. The SGDN is directly subordinated to the French prime minister and assists the prime minister's office in the co-ordination of the preparation, implementation, and follow-up of the government's decisions regarding defense and security policy, including the security of information systems.

The SGDN also promotes and co-ordinates the activities between ministries involved in CIIP. This includes responsibility for the security of information systems (since 1996) and chairing the CISSI, as well as responsibility for the protection of classified and sensitive military information. The SGDN deals with the impact of the scientific and technical revolution on defense and security policy, focusing on securitization of information and communication technology relating to military as well as civilian matters. In this area, the SGDN works closely together with DCSSI.

[4]Direction centrale de la sécurité des systèmes d'information (DCSSI).
[5]Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI).

***3.1.2 Central Directorate for Information Systems Security (DCSSI).*** The DCSSI was instituted by Decree No. 2001-693 of 31 July 2001 [13] under the authority of the SGDN. It succeeded the Central Information Systems Security Division as the state's focal center for Information Systems Security.

The DCSSI has two main objectives: To guarantee the security of the information systems of the French state (including critical infrastructures in times of crisis); and to create a trusted environment to promote and facilitate the development of the information society. The DCSSI's principal missions are [14]:

- To contribute to interdepartmental and international definitions of governmental policy as regards information security;
- To serve as a national regulatory authority for information security by issuing approvals, guarantees, and certificates for national information systems, encryption processes, and products used by public bodies and services; and by controlling information technology security evaluation centers (CESTI);
- To assist public services in information security (consult, audit, issue warnings, and conduct incident management, including crisis management);
- To develop scientific and technical expertise in the field of information security for the benefit of the administration and public services;
- To run training courses and increase awareness in information security (Information Systems Security Training Centre/CFSSI).

The DCSSI also administers the Security of Information Systems (SSI) website [15] and co-ordinates its activities. The SSI website comprises information on the Computer Emergency Response Team (CERTA) [16], information on regulation, certification, authorization, electronic signatures, and cryptography, and provides technical advice.

***3.1.3 Information Systems Security Training Center (CFSSI).*** Attached to DCSSI, the Information Systems Security Training Center's (CFSSI) [17] objectives are to increase awareness on information systems security and to train experts capable of designing, evaluating, and making recommendations on the following aspects of information systems security:

- Communications security,
- Protection against compromising viruses,
- Computer security.

The CFSSI continues training actions undertaken by the CESSSI (Center for Training and Advanced Studies on Information Systems Security) since 1986. It will become the central player in a network designed to increase awareness on information systems security problems and provide training in the various aspects of this area, for the benefit of all government authorities.

The CFSSI also develops partnerships with higher education and further training centers. The activities of the CFSSI and the education it provides are controlled and monitored by an improvement committee chaired by the secretary-general for national defense and composed of civil servants and military staff.

***3.1.4 Operational Center (COSSI).*** In order to defend governmental networks and information systems, the SGDN runs the Information System Security Operation center (COSSI) which, in addition to its general preventive tasks, coordinates the action of ministries and draws up protection and reaction measures. The centre also prepares and implements the Vigipirate plan against terrorist threats. COSSI operates around the clock, 365 days a year.[3]

***3.1.5 Central Office for the Fight Against Hi-Tech Crime.*** In May 2000, the Ministry of the Interior opened the Central Office for the Fight against Cyber-Crime [18]. It co-operates with Interpol and deals with unauthorized intrusions and crime in the field of information and communication technologies and supports legal investigations in this field. The Central Office has nationwide jurisdiction in this matter and works closely together with the national police as well as the private sector. It provides assistance to all agencies responsible for fighting computer crime, such as the police and gendarmerie, and sensitizes the actors.

### 3.2 Public-Private Partnerships

***3.2.1 Strategic Advisory Board on Information Technologies (CSTI).*** The Strategic Advisory Board on Information Technologies (CSTI) [19] was created in July 2000 at a meeting of the government committee on the Information Society. It is chaired by the French prime minister. The CSTI is composed of business and industry executives and leading representatives of the research and development community. It is responsible for recommendations to government concerning CIIP topics and the French contribution to the 6$^{th}$ European Framework Research and Development Program. The CSTI, in particular, has the following duties [20]:

- To communicate opinions and recommendations to the government on the studies and documents commissioned;
- To maintain a permanent dialog with representatives of industry and to improve co-ordination between private and public researchers (and the industry);
- To define national priorities and to select areas where more action is required;
- To provide general monitoring and warning services in the area of CIIP.

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 Computer Emergency Response Teams (CERTs)

In France, there are three different Computer Emergency Response Teams (CERTs), and each of them addresses a different constituency: CERT-RENATER, CERTA, and CERT-IST.

- CERT-RENATER [21], founded in 1993, specifically addresses research centers and academic institutions. CERT-RENATER gathers and provides information about information security and is dedicated to the membership of GIP[6] RENATER, the National Network of Telecommunications for Technology, Education, and Research;

[6]Groupement d'Intérêt Publique (Public Interest Group).

- The Computer Emergency Response Team CERTA [22] has been hosted by DCSSI since 2000. CERTA deals in particular with the French administration services. As a center of expertise, it evaluates CIIP threats and gives advice, issues warnings, and provides information on how to prevent, respond to, and handle an attack against information systems. High-level staff, mainly engineers, work at CERTA. The CERTA is part of the Central Directorate for the Security of Information Systems (DCSSI) and acts as the technical cell of the permanent operational center (ITSOC) operating around the clock, seven days a week. CERTA is also the expertise cell from COSSI;[3]
- CERT-IST (CERT-Industry, Services, and Tertiary) was launched in 1999 by Alcatel (a telecom company), CNES (the French Space Agency), France Telecom, and the TotalFinaElf energy group. It serves France's private sector as a contact point for security incident response. CERT-IST provides alerts and means of protection against computer attacks aimed at French enterprises. It also helps the association members with incident handling [23]. CERT-IST interacts with the French national security organizations SGDN and DCSSI, in conjunction with CERT-RENATER and CERTA [24].

### 4.2 Web Portal for Citizens and SMEs

In the wake of a prime ministerial decision to bring security to citizens and small and medium enterprises, the DCSSI has built a web portal dedicated to enduser computer security [25].

The prime minister's decision, which the portal serves to promote, consists of four main points:

- To coordinate the existing initiatives such as "internet sans crainte" (internet without fear);
- To keep citizens and SMEs informed about risks, recommendations, workarounds, and best practices;
- To alert citizens and SMEs when needed, and to provide timely and relevant information;
- To build and foster a contact network around the country.

## 5 LAW AND LEGISLATION

### 5.1 Penal Code 2004

Amended as Law no.2004-575 of 21 June 2004, entered into force on 23 June 2004.

- *Article 323-1.* Fraudulent accessing or remaining within all or part of an automated data processing system is punishable by a sentence not exceeding two years' imprisonment and a fine. Where this behavior causes the suppression or modification of data contained in that system, or any alteration of the functioning of that system, the sentence shall not exceed three years' imprisonment and a fine.

- *Article 323-2.* Obstruction or interference with the functioning of an automated data processing system is punished by a sentence not exceeding five years' imprisonment and a fine.
- *Article 323-3.* The fraudulent introduction of data into an automated data processing system or the fraudulent suppression or modification of the data that it contains is punished by a sentence not exceeding five years imprisonment and a fine.
- *Article 323-3-1.* Fraudulently, and without legitimate motive, importing, holding, offering, selling or making available any equipment, tool, computer program or any data designed or particularly adapted to commit one or more offences provided for by articles 323-1 to 323-3, is punishable by the sentences prescribed for offences in preparation or the one that carries the heaviest penalty [26].

Moreover, France ratified the Council of Europe Convention on Cybercrime on 10 January 2006.

## ACKNOWLEDGMENT

We acknowledge the contribution of the expert, Stanislas de Maupeou of the Secretariat-General for National Defense, who validated the content of this chapter.

## REFERENCES

1. http://www.education.gouv.fr/realisations/communication/samra.htm, 2008.
2. http://www.internet.gouv.fr, 2008.
3. Service d'Information du Gouvernement (2001). *Four Years of Government Measures to Promote the Information Society*, (August).
4. All consecutive versions are available on the site of the Prime Minister's Office. *Serveur thématique sur la sécurité des systèmes d'information*, http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html, 2008.
5. http://www.ssi.gouv.fr/fr/confiance/methodes.html, 2008.
6. Prime Minister's Office (2004). *State Information System Security Reinforcement Plan (2004–2007)*, (10 March). http://www.ssi.gouv.fr/site_documents/PRSSI/PRSSI-en.pdf.
7. Agence pour le Dévéloppement de l'Administration Électronique (ADAE) See: Administration 24h/24. *le portail des démarches en ligne*, http://www.administration24h24.gouv.fr, 2008.
8. http://www.internet.gouv.fr/informations/information/plan_reso2007, 2008.
9. Jacob, O. (2008). Préface du President Nicolas Sarkozy, Président de la République. *Défense et Sécurité nationale LE LIVRE BLANC. Odile Jacob*, (2008). La Documentation Française, Paris (June).
10. Neue Zürcher Zeitung (2008). *Weniger Personal, mehr Geld für militärische Raumfahrt. Frankreichs Präsident Sarkozy präsentiert Pläne für den Umbau der Armee*, (16 June). http://www.nzz.ch/nachrichten/international/frankreich_sarkozy_armee_plaene_1.760795.html.
11. Neue Zürcher Zeitung (2008). *Frankreich fürchtet sich vor Cyber-Attacken. Aufklärung laut Verteidigungs-Weissbuch wichtigster Budgetposten*, (17 June). http://www.nzz.ch/nachrichten/international/frankreich_fuerchtet_sich_vor_cyber-attacken_1.761740.html.
12. *Secrétariat Général de la Défense Nationale*, http://www.sgdn.gouv.fr/sommaire_en.php, 2008.
13. http://www.ssi.gouv.fr/fr/dcssi/decretdcssicissi.html.
14. http://www.cases.public.lu/fr/documentation/documents_de_reference/technique/index.html#1.

15. *Sécurité de Systèmes d'Information*, http://www.ssi.gouv.fr/en/index.html.
16. *Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques*, http://www.ssi.gouv.fr/fr/index.html.
17. *Centre de formation à la sécurité des systèmes d'information*, http://www.ssi.gouv.fr/en/formation.html.
18. Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (L'O.C.L.C.T.I.C.) http://www.securiteinfo.com/legal/OCLCTIC.shtml. See also: http://www.interieur.gouv.fr/sections/contact/police/questions-cybercriminalite/view.
19. Conseil Stratégique des Technologies de l'Information http://www.csti.pm.gouv.fr/.
20. http://www.csti.pm.gouv.fr/uk/enbref.html.
21. *Réseau National de Télécommunications pour la Technologie, l'Enseignement et la Recherche*, http://www.renater.fr, For CERT-Renater in particular, see: http://www.renater.fr/spip.php?rubrique19.
22. *Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques Informatiques*, http://www.certa.ssi.gouv.fr/.
23. http://www.cert-ist.com/, 2008.
24. RAND Europe. Dependability Development Support Initiative (DDSI) (2002). *National Dependability Policy Environments, France*, (November), p. 7, http://www.ddsi.org/htdocs/Documents/final%20docs/DDSI_Country_Reports_Final_France.pdf.
25. http://www.securite-informatique.gouv.fr, 2008.
26. http://www.cybercrimelaw.net/laws/countries/france.html, 2008.

# GERMANY

Manuel Suter and Elgin Brunner
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

The main assumption underlying CIP/CIIP in Germany is that both the government and society as a whole depend heavily on a secure infrastructure. Organizations or facilities

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

whose failure or impairment would cause a sustained storage of supplies, significant disruptions of public order, or other dramatic consequences for large parts of the population are defined as critical. According to the German constitution, it is the state's task to guarantee public security and order and to ensure that the population is provided with essential goods.

The following are the infrastructure sectors defined as critical in Germany: [1]

- Transportation and Traffic,
- Energy,
- Hazardous Materials,
- Telecommunications and Information Technology,
- Financial, monetary and insurance systems,
- Supply (including water supply, food supply, healthcare, emergency and rescue services),
- Government Agencies, Administration, and Justice,
- Media, research facilities, cultural property.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

In the past ten years, many activities have been undertaken that were directly or indirectly related to the issue of critical infrastructure protection. They emerged from inter-ministerial activities begun in 1997 at the initiative of the Federal Minister of the Interior, motivated in part by the study produced by the US President's Commission on Critical Infrastructure Protection (PCCIP). The events of 11 September 2001 added urgency to ongoing efforts and, as part of the campaign against terrorism, contributed to widening the scope of national activities and intensifying the international dialog.

In 2005, two key documents were presented:

- The National Plan for Information Infrastructure Protection (NPSI) [2], enacted by a cabinet decision of the federal government, and
- The Protection of Critical Infrastructures—Baseline Protection Concept [3], followed by the Protecting Critical Infrastructures—Risk and Crisis Management. A Guide for Companies and Government Authorities [4] in 2008.

These documents can be considered as initial milestones for a number of activities for establishing both CIIP and CIP processes throughout the country.

## 3 AG KRITIS

Initiated by the PCCIP report in the US, an inter-ministerial working group on critical infrastructures (AG KRITIS) was established in 1997 by the Federal Minister of the Interior. It consisted of the ministerial representatives, a steering committee, and a permanent office at the Federal Office for Information Security (BSI). The mandate of AG KRITIS was to:

- Describe possible threat scenarios for Germany;
- Conduct a vulnerability analysis of Germany's crucial sectors;
- Suggest countermeasures;
- Sketch an early-warning system.

The work of AG KRITIS [5] was an important basis for all further activities of public agencies in Germany.[1]

### 3.1 Situational Analysis of Threats and Hazards/CIP-Initiatives

CIP/CIIP activities were intensified after the events of 11 September 2001. The need for more coordinated CIP efforts was underpinned by lessons identified after the floods of the Danube, Oder, and Elbe rivers in the following years. The following sections provide summaries of CIP-related reports, recommendations, and activities. CIIP-related initiatives and reports are described in the next section.

***3.1.1 Comprehensive Report on Threats and Hazards.*** In March 2006, the Ministry of the Interior published a second comprehensive threat analysis for Germany [6]. The IT section in this report is founded on previous reports and continues to answer questions identified by the AG KRITIS work. Together with other national assets, information security is defined as crucial for the security of the German society and for the success of its economy.

***3.1.2 Kirchbach Report.*** The Kirchbach Commission, established in Saxony after the devastating flood of 2002, analyzed the overall structure of the German emergency protection system. Besides the focus on the flood disaster, the Kirchbach report provided a comprehensive analysis of existing facilities and recommendations for future capacities to secure information and communications technology in cases of emergency [7]. This disaster and the conclusions of the Kirchbach report triggered a broad range of measures in several ministries and agencies.

***3.1.3 Critical Infrastructure Protection—Baseline Protection Concept.*** The CIP baseline protection concept was developed in close cooperation between the Federal Ministry of the Interior (BMI), the Federal Office of Civil Protection and Disaster Assistance (BBK), the Federal Criminal Police Agency (BKA), and the private sector. It provides guidance for the analysis of potential hazards such as terrorist attacks, criminal acts, and natural disasters, as well as recommendations for companies on adequate protective measures [8].

***3.1.4 Protecting Critical Infrastructures—Risk and Crisis Management. A Guide for Companies and Government Authorities.*** The CIP baseline protection concept was complemented by a guideline Protecting Critical Infrastructures—Risk and Crisis Management. A Guide for Companies and Government Authorities [9], which was published in December 2007 and presented in January 2008. This guideline provides methods to support the implementation of risk management and crisis management in enterprises and government organizations and offers checklists and examples.

[1]The report of AG KRITIS was, however, never published. A draft version in German can be found in Ref. [5].

### 3.2 CIIP Initiatives

As already mentioned, the attacks in the US on 11 September 2001 lead to a considerable intensifying of activities in the area of CIIP as well.

***3.2.1 CIIP at the BSI.*** After 2001, several departments at the Federal Office for Information Security (BSI) were expanded and given additional tasks to support critical information infrastructure protection.

On its website, the BSI regularly updates information and practical advice on critical infrastructures [10].

In mid-2002, BMI and BSI commissioned a series of systematic infrastructure analysis studies on the influence of ICT on the CI sectors. The results of these studies, though unpublished, induced a number of further activities both in intensifying the dialog between public and private sectors and in developing and implementing CIIP-related strategies and policies, as described in the following subsections.

***3.2.2 National Plan for Information Infrastructure Protection (NPSI).*** The National Plan for the Protection of Information Infrastructures (NPSI), issued in 2005, is the federal government's umbrella strategy for a comprehensive approach to the protection of ICT and ICT-dependent assets [11]. It aims at strengthening IT security in the nation's IT-dependent infrastructures and at enabling swift responses to IT-related crises.

The NPSI pursues three strategic objectives:

- *Prevention.* protecting information infrastructures adequately;
- *Preparedness.* responding effectively to IT security incidents;
- *Sustainability.* enhancing German competence in IT security and setting international standards.

This strategy addresses public authorities as well as businesses and individuals. The NPSI announced two implementation plans, one for the federal administration and one for critical infrastructures, both of which were finalized in 2007 [12]. By cabinet decision, the implementation plan for the federal administration presents a mandatory IT security guideline. Implementing the designated measures will ensure a high level of IT security throughout the federal administration in a mid- to long-term perspective.

***3.2.3 CIP Implementation Plan.*** The CIP implementation plan [13] was prepared in close cooperation between representatives of critical infrastructure operators and service providers as well as experts from the federal administration. The plan aims at implementing measures that make it possible to bring the goals of operators in the private industry in line with the higher-level (safeguarding) interests of the community.

The plan addresses the need for measures that meet security requirements extending beyond the security and business continuity responsibilities within the enterprises, as well as the aim of encouraging industries to scrutinize their own security and risk management approaches.

This implementation plan also introduces a roadmap to the future: the following topics will be pursued in direct follow-up activities:

- Emergency and crisis exercises;
- Crisis response and management;

- Maintaining critical infrastructure services;
- National and international cooperation.

In future there will be regular reporting on progress and results, as well as updates of the implementation plan in response to progress and changes in the IT and threat environment.

***3.2.4 IT and Internet Security Situation in Germany.*** In order to provide general information on the IT security and internet security situation in Germany, the BSI started to publish a report on the IT Security Situation in Germany in 2005 (with a second edition following in 2007), which provides a survey of current threats to information and information systems, of the challenges to be met in order to secure information infrastructures, and of trends related to new information technologies and evolving threats. Furthermore, the BSI has started to issue a quarterly summary of the internet threat situation in 2007 [14].

***3.2.5 IT Security Guidelines.*** The IT Security Guidelines published by the BSI are intended to satisfy the needs of small and medium-sized businesses, summarizing the most important IT security measures in a compact overview that is intelligible to the non-expert. The focus is on organizational safeguards and on illustrating threats through practical examples [15].

### 3.3 E-Government Initiatives

The German e-Government initiative [16] aims to use modern information and communications technologies consistently in order to make administrative processes more efficient, and to facilitate an exchange between the business community, the public, and the administration. In short: e-Government should ensure that each agency within the federal administration is just one mouse click away for the citizen.

The BundOnline 2005 initiative—to make all suitable government services of the federal administration available to the public through the internet—was successfully concluded in August 2005.[2] The BSI had been tasked with developing the basic IT security components and with setting up the data security competence center. The BSI also published the e-Government Manual [18] covering all aspects of secure e-Government and presenting pragmatic approaches. In September 2006, the federal government initiated the E-Government 2.0 program for the further enhancement of e-Government services until 2010 [19].

As a related activity, Germany Online is the national e-government strategy pursued by the federal government, governments of federal states, and municipal administrations, initiated in 2003 [20].The goal was to establish a secure communications network for the entire German administration, and particularly for communication between the different state levels, i.e., the municipalities, the states, and the federal government. In June 2006, Chancellor Angela Merkel, together with the heads of the federal states' governments, adopted the Action Plan Germany Online, which was extended in June 2007 [21]. Among the six prioritized projects, the establishment of the communications infrastructure is the most relevant one from a CIIP perspective [21].

[2]For the final report, see [17].

### 3.4 International Collaboration

A joint initiative of the German Ministry of the Interior [22] and the US Department of Homeland Security [23] at the ministerial level in 2003 laid the groundwork for cooperation in several CIIP-related activities [24]. Among others, both parties agreed to foster regular consultations in international organizations in order to enhance multilateral cooperation. This bilateral initiative complements the already ongoing counter-terrorism efforts. As a mid-term result, the International Watch and Warning Network (IWWN) has been established, currently involving 15 participants from all continents.

Multilateral conferences such as the International Watch, Warning and Incident Response Workshop held in Berlin in October 2004, the International Watch and Warning Network Conference in Washington, D.C. in June 2006 (both co-hosted by the US and Germany), or the European IT security conference Innovation and Responsibility in Berlin during the German EU presidency 2007, with one of the six tracks dedicated to CIIP, have contributed to the development and improvement of methods for multinational cooperation. Furthermore, Germany is actively participating in efforts aimed at bringing forward the European Programme for Critical Infrastructure Protection (EPCIP) [25]. Germany's international CIIP activities also include participation in CIIP-relevant projects and working groups, such as the European SCADA and Control Systems Information Exchange (E-SCSIE) [26].

Moreover, Germany participates in efforts to identify, develop, and share CIIP good practice recommendations, e.g., the "Best Practices for Improving CIIP in Collaboration of Governmental Bodies with Operators of Critical Information Infrastructures" currently being discussed by the G8 High-Tech Crime Subgroup (HTCSG).

## 4 ORGANIZATIONAL OVERVIEW

Overall responsibility for, and coordination of, major CIP- and CIIP-related activities rests with the Federal Ministry of the Interior (BMI), together with several of its subordinated agencies, such as the Federal Office for Information Security (BSI) [27], the Federal Office of Civil Protection and Disaster Assistance (BBK) [28], the Federal Criminal Police Agency (BKA) [29], and the Federal Police (BPOL) [30]. For coordination within the ministry and the subordinated agencies, a task force for critical infrastructure protection (AG KRITIS) was established at the BMI in 2002. Strategy development and implementation are also coordinated with other federal ministries, especially the Federal Ministry of Economics and Technology [31], the Federal Chancellery [32], the Federal Ministry of Justice, the Federal Ministry of Foreign Affairs, the Federal Ministry of Defense, and other relevant agencies, such as the Federal Network Agency [33]. Furthermore, strategic partners from the private sector are consulted.

### 4.1 Public Agencies

***4.1.1 Federal Ministry of the Interior (BMI).*** As the government agency responsible for ensuring Germany's internal security, the Federal Ministry of the Interior (BMI) is closely involved with CIP/CIIP. This agency deals with and coordinates the relevant topics, such as physical protection within the context of civil protection and disaster response, threat prevention within the context of law enforcement, and all areas of IT and IT dependence. The authority in charge of IT-related issues with regard to CIIP

is Division IT 3 (Information Technology Security) under the Federal Ministry of the Interior's Chief Information Officer [34]. Responsibility for CIP resides with Division KM 4 (Critical Infrastructure Protection) [35].

***4.1.2 The Federal Office for Information Security (BSI).*** The Federal Office for Information Security (BSI), one of the agencies under the Federal Ministry of the Interior, plays an especially important role in CIIP. The BSI deals with all areas related to security in cyberspace and takes preventive action by analyzing IT weaknesses and developing protective measures, including the following:

- Security of applications and critical infrastructures,
- Security of networks (including CERT Bund, IT situation center, and IT crisis management center, and early warning systems),
- Cryptographic technology,
- New technologies (e.g., biometrics, RFID).

The BSI investigates security risks associated with the use of IT and develops preventive security measures. It provides information on risks and threats relating to the use of information technology and develops appropriate solutions. This work includes IT security testing and assessment of IT systems, including their development, in co-operation with industry. It also analyses developments and trends in information technology. The BSI's services address a broad audience: the federal administration as well as manufacturers, distributors, and private users of information technology [36].

Of special relevance in the CIIP context is the CERT-Bund 24-h on-call availability for the federal administration, and the operation of the IT situation center, where the IT threat situation is assessed on a continuous basis.[3]

***4.1.3 Federal Office of Civil Protection and Disaster Assistance (BBK).*** The Federal Office of Civil Protection and Disaster Assistance (BBK) was established on 1 May 2004 under the Federal Ministry of the Interior [37]. One of the main functions of this agency is information-sharing and resource allocation between the different levels of public authority in case of emergencies.

The BBK has a special focus on CIP.[4] It operates in close cooperation with the BSI and the Federal Network Agency (Bundesnetzagentur) in the field of CIIP. Moreover, contingency plans and appropriate measures are being developed according to case studies [38].

The BBK established the German Emergency Preparedness Information System (deNIS) as a special service for public authorities, emergency responders, and the general public [39]. For the public, deNIS provides general information about organizations and potential emergencies, and offers web links on emergency precaution and preparedness. For a closed user group of emergency responders and crisis management professionals, a secure and classified system called deNIS IIplus has been established [40].

Furthermore, on 1 October 2002, the Joint Reporting and Situation Center (Gemeinsames Melde- und Lagezentrum, GMLZ) took up operation with the objective of enhancing cooperation between federal, state, and local authorities as well as national,

[3]See also the chapter on Early Warning and Public Outreach.

[4]The BBK's main CIP-related output have been the publications on "Critical Infrastructure Protection—Baseline Protection Concept" and "Protecting Critical Infrastructures—Risk and Crisis Management". A Guide for companies and government authorities.

international, and supranational organizations in situations of severe damage and hazards. The tasks include continuous situation assessment; the receipt, acquisition, analysis, processing, coordination, and dissemination of information; and forecasts of damage progression in case of events. International request for emergency support from Germany will be handled through GMLZ.

***4.1.4 The Federal Criminal Police Agency (BKA).*** The Federal Criminal Police Agency (BKA) [41] is responsible in the first instance for prosecuting crimes against the internal or external security of the Federal Republic of Germany and crimes involving damage to or the destruction of critical infrastructures that could result in a serious threat to life, health, or the functioning of society. Further, the BKA is the central agency for investigating crimes involving information and communications technology.

***4.1.5 Federal Ministry of Economics and Technology (BMWi).*** With roughly 85 per cent of Germany's critical infrastructure being privately owned, the Federal Ministry of Economics and Technology (BMWi) [42] also plays a role, as its brief includes economic policy on the one hand, but also oversight over several CI sectors on the other (through the Federal Network Agency, see below). With regard to the energy sector, one of the BMWi's tasks is developing the framework for securing the energy supply. According to Article 87f of the German constitution, the BMWi is also responsible for ensuring the availability of adequate telecommunications infrastructure and services.

***4.1.6 Federal Network Agency.*** In July 2005, the Regulatory Authority for Telecommunications and Posts was renamed the Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railway. The Federal Network Agency is a higher federal authority within the scope of business of the Federal Ministry of Economics and Technology. The Federal Network Agency's task is to provide, by liberalization and deregulation, for the further development of the electricity, gas, telecommunications, and postal markets and, as of January 2006, of the railway infrastructure market as well [43].

***4.1.7 Other ministries involved.*** The Federal Ministry of Justice (BMJ) [44] is responsible for relevant legislation, in particular for ensuring that national laws comply with relevant EU legislation such as the EU Council Framework Decision on attacks against information systems [45].

The Federal Ministry of Defense (BMVg) [46] is involved in the context of its responsibility for national defense and for maintaining troop readiness and performance.

The Federal Chancellery plays a coordinating role at the ministerial level. Additional ministries with specific areas of responsibility are also involved in CIP.

Responsibilities are also shared among the agencies within the remit of the various ministries. The Federal Intelligence Service (Bundesnachrichtendienst, BND) and the Federal Office for the Protection of the Constitution (Bundesamt für Verfassungsschutz, BfV) provide important information regarding the threat situation and possible domestic targets.

## 4.2 Public-Private Partnerships

***4.2.1 CIP Implementation Plan.*** The latest example of public-private cooperation was the development of the CIP implementation plan (see chapter on Past and Present Initiatives and Policies), followed by a set of ongoing activities to actually implement measures.

***4.2.2 Germany Secure in the Web Campaign.*** The campaign Germany Secure in the Web (Deutschland sicher im Netz, DsiN) [47] is an initiative undertaken under the auspices of the Federal Minister of the Interior. Members include private enterprises as well as associations and non-profit organizations. Its main objective is to improve the security of both private and commercial IT users, to provide private users and small and medium-sized enterprises with a sound basis of information that encourages the use of, and confidence in, the internet and internet-based services, and to raise awareness of all relevant IT security issues. The association also targets children and adolescents specifically, with the objective of raising their awareness and that of their parents of IT-security related issues, but also to protect them from, and prevent them from accessing, criminal and abusive contents.

***4.2.3 Initiative D21.*** Launched in 1999, Initiative D21 [48] is the largest public-private partnership in Germany. This economic initiative also deals with information security. Initiative D21 is a neutral platform, independent of party allegiance and of individual industrial sectors. D21 has more than 200 participants from enterprises, associations, parties, political institutions, and other organizations. Initiative D21 pursues a steadily growing number of projects. Initiative D21 is organized into three subject areas (steering groups):

- Digital Integration,
- Digital Competence,
- Digital Excellence [48].

## 5 EARLY WARNING AND PUBLIC OUTREACH

### 5.1 CERT-Bund

The CERT-Bund unit was established on 1 September 2001 at the Federal Office for Information Security (BSI). CERT-Bund is a central contact point charged with protecting the security of data processes and networks of the federal public administration. CERT-Bund also offers some of its services to clients from the private sector. However, several services are only available to the federal administration (e.g., incident response) [49]. CERT-Bund's main tasks include warning and information-sharing, data collection, analysis and processing of information, documentation and dissemination, sensitization of IT decisionmakers, and cooperation with existing CERTs [50].

### 5.2 CERT-Network

The CERT-Verbund (CERT Network) is an alliance of German security and computer emergency teams [51]. The alliance provides a common base for cooperation between the teams and also allows the pursuit of the overarching objectives, namely to ensure the protection of national IT networks or to prepare for swift and coordinated reaction in case of larger IT security incidents.

### 5.3 IT Situation Center

The IT Situation Center collects, assesses, and summarizes information on the IT situation in Germany as a continuously updated situational picture. The processes of

gathering information and establishing an information exchange in cooperation with relevant partners, e.g., from critical infrastructures, are constantly being further developed. Procedures are emerging to share assessment results, including alerts and warnings, in a target-oriented way with a variety of audiences, including government agencies, critical infrastructure operators, and the general public.[5]

### 5.4 IT Crisis Response Center

To be prepared for national crisis situations affecting information infrastructures, Germany has established an IT Crisis Response Center as a non-standing organization located at the BSI, closely related to the IT situation center. Situational crisis indicators will activate IT crisis response functions to warn and alarm potentially affected parties and to develop countermeasures. Moreover, the center supports a coordination board for the IT security of the federal ministries in organizing timely responses to minimize and to contain damage, and to return swiftly to the safe and secure operation of affected information infrastructures [52].

### 5.5 Services for Citizens and SMEs

***5.5.1 Citizens' CERT (Bürger-CERT).*** The Citizens' CERT [53] project aims at informing and warning citizens and small enterprises of the threats stemming from worms, viruses, and security loopholes in IT systems not only rapidly and competently, but also from an explicitly neutral perspective and at no cost. The Citizens' CERT project was initiated jointly by the BSI and Mcert[6] in 2006. Since June 2007, Citizens' CERT has been maintained exclusively by the BSI. Every citizen can subscribe to the services of the Citizens' CERT project, which include technical warnings, a bi-weekly newsletter, and special editions of the newsletter. Thus, the project aims to make as many people as possible aware of the issues the importance of IT security [54]. For general information on IT security, there is a direct link to the website "BSI for the Citizen".

***5.5.2 BSI for the Citizen.*** The internet service "BSI for the citizen" [54] aims at providing easy-to-understand background information on IT security and the internet. The service offers guidance on how to surf the internet and use internet-based applications securely. For up-to-date warnings on new internet threats and a newsletter, users can follow a direct link to the Citizens' CERT webpage, which serves as a warning and information service for citizens.

## 6 LAW AND LEGISLATION

### 6.1 Telecommunications Act

First enacted in 1996, this act was revised in 2004 and last amended in 2007 [55]. Its purpose is to provide legal provisions for the liberalization and deregulation of the telecommunications market.

[5]Information provided by an expert.

[6]Mcert began as a CERT for SMEs in 2003 and suspended its services in June 2007, with key tasks being continued by Citizens' CERT and the initiative "Germany Secure in the Web" (see above).

### 6.2 Telecommunications and Media Act 2007

The Information and Telecommunications Services Act (Informations- und Kommunikationsdienste-Gesetz, IuKDG) of 1997 [56] was the starting point for the liberalization of the German telecommunications market [57]. The IuKDG and all related acts expired in 2007 with the enacting of the Telecommunications and Media Act (Telemediengesetz, TMG) [58].

### 6.3 Electronic Signature Act 2001

In May 2001, this act (which conforms to EU regulations) replaced the existing pioneer Digital Signature Act of 1997. The main purpose of the act is to define a framework for the handling of electronic signatures [59]. The act was last amended on 26 February 2007.

### 6.4 Penal Code

To implement the EU Council Framework decision on 2005/222/JHA of 24 February 2005 on attacks against information systems, the German penal code was amended on 7 August 2007, affecting §202a on data espionage, §202b on data interception, §202c on the preparation of data espionage and interception, §303a on alteration of data, and §303b on computer sabotage [60, 61].

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Susanne Jantsch and Monika John-Koch of the Federal Office of Civil Protection and Disaster Assistance, who validated the content of this chapter.

## REFERENCES

1. http://www.bsi.bund.de/english/topics/kritis/kritis_e.htm, and http://www.bbk.bund.de/cln_027/nn_1048112/EN/02_themes/05_critical-infrastructures/01_sectors-start/sectors_node.html_nnn=true, 2008.
2. Federal Ministry of the Interior. (2005). *National Plan for Information Infrastructure Protection*, Berlin .http://www.bmi.bund.de/cln_012/nn_148138/Internet/Content/Common/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National_Plan_for_Information_Infrastructure_Protection,templateId=raw,property=publicationFile.pdf/National_Plan_for_Information_Infrastructure_Protection.
3. Federal Ministry of the Interior. (2005). *Protection of Critical Infrastructures—Baseline Protection Concept*, Berlin. http://www.bmi.bund.de/nn_121894/Internet/Content/Common/Anlagen/Broschueren/2007/Basisschutzkonzept_kritische_Infrastrukturen_en,templateId=raw,property=publicationFile.pdf/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf, 2008.
4. Federal Ministry of the Interior (2008). *Protecting Critical Infrastructures—Risk and Crisis Management. A Guide for Companies and Government Authorities*, Berlin, http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2008/Leitfaden_Schutz_kritischer_

Infrastrukturen_en,templateId=raw,property=publicationFile.pdf/Leitfaden_Schutz_kritische r_Infrastrukturen_en.pdf.

5. http://userpage.fu-berlin.de/~bendrath/Kritis-12-1999.html, 2008.
6. Federal Ministry of the Interior. (2006). *Dritter Gefahrenbericht der Schutzkommission beim Bundesminister des Innern. Bericht über mögliche Gefahren für die Bevölkerung bei Grobetakatastrophen und im Verteidigungsfall*, Bonn, English Summary: http://www.bbk.bund.dec/ln_027/nn_529818/Schutzkommission/DE/03_Publikationen/01_Gefahrenberichte/Summary_203._20GB_20englisch.html.
7. von Kirchbach, H. P., Franke, S., and Biele, H. (2003). *Bericht der Unabhaumlngigen Kommission der Saumlchsischen Staatsregierung. Flutkatastrophe 2002*, 2nd ed. http://home.arcor.de/schlaudi/Kirchbachbericht.pdf.
8. Federal Ministry of the Interior. *Protection of Critical Infrastructures—Baseline Protection Concept*, op. cit.
9. Federal Ministry of the Interior. *Protecting Critical Infrastructures—Risk and Crisis Management. A Guide for Companies and Government Authorities*, op. cit.
10. http://www.bsi.bund.de/fachthem/kritis/index.htm (German) and http://www.bsi.bund.de/english/topics/kritis/kritis_e.htm (English), 2008.
11. Federal Ministry of the Interior. *National Plan for Information Infrastructure Protection*, op. cit.
12. See press release (in German): http://www.bmi.bund.de/cln_012/nn_122688/sid_805F7477F227F34F95AFF8D45906FAD9/Internet/Content/Nachrichten/Pressemitteilungen/2007/09/IT_Sicherheit.html, 2008.
13. Federal Ministry of the Interior. (2007). *Umsetzungsplan KRITIS des Nationalen Plans zum Schutz der Informationsinfrastrukturen*, Berlin, http://www.bmi.bund.de/cln_012/nn_122688/Internet/Content/Broschueren/2007/Kritis.html, currently only available in German, English version in preparation.
14. http://www.bsi.bund.de/literat/lagebericht/index.htm, 2008.
15. Federal Office for Information Security (BSI). (2004). *IT Security Guidelines: IT Baseline Protection in Brief*, Bonn, http://www.bsi.bund.de/english/gshb/guidelines/guidelines.pdf.
16. http://www.kbst.bund.de/nn_836956/Content/Egov/egov.html_nnn=true, 2008.
17. http://www.kbst.bund.de/cln_012/nn_945224/SharedDocs/Publikationen/Oeffentlichkeitsarbeit/Umsetzungsplan/current_20status_20and_20outlook_2006,templateId=raw,property=publicationFile.pdf/current%20status%20and%20outlook_2006.pdf, 2008.
18. http://www.e-government-manual.de, 2008.
19. http://www.kbst.bund.de/cln_012/nn_836958/Content/Egov/Initiativen/EGov2/EGov2.html_nnn=true, 2008.
20. http://www.kbst.bund.de/cln_028/nn_839178/Content/Egov/Initiativen/D_online/d_online.html_nnn=true and http://www.deutschland-online.de/DOL_en_Internet/broker.jsp, 2008.
21. See download section under http://www.deutschland-online.de/DOL_en_Internet/broker.jsp, 2008.
22. http://www.bmi.bund.de, 2008.
23. http://www.dhs.gov/index.shtm, 2008.
24. Federal Ministry of the Interior (BMI). (2003). *Schily und Ridge vereinbaren Kooperation beim Schutz von Computersystemen*. http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Nachrichten/Archiv/Pressemitteilungen/2003/06/Schily_und_Ridge_vereinbaren_Kooperation_Id_92348_de.html.
25. http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm, 2008.

26. https://espace.cern.ch/EuroSCSIE/default.aspx, 2008.
27. *Bundesamt für Sicherheit in der Informationstechnik*, http://www.bsi.bund.de, 2008.
28. *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe*, http://www.bbk.bund.de, 2008.
29. *Bundeskriminalamt*, http://www.bka.de, 2008.
30. Bundespolizei, http://www.bundespolizei.de/cln_049/DE/Home/home_node.html?_nnn=true, 2008.
31. http://www.bmwi.de/English/Navigation/root.html, 2008.
32. *Bundeskanzleramt*, http://www.bundeskanzlerin.de/Webs/BK/DE/Homepage/home.html, 2008.
33. *Bundesnetzagentur*, http://www.bundesnetzagentur.de/enid/6c28cf7e908c093de1d8973191d1ed59,0/xn.html, 2008.
34. http://www.bmi.bund.de/Internet/Content/Ministerium/Organigramm_Neu/Referate/itstab_engl.html, 2008.
35. http://www.bmi.bund.de/Internet/Content/Ministerium/Organigramm_Neu/Referate/abteilung_km_engl.html, 2008.
36. http://www.bsi.de/english/functions.htm, 2008.
37. http://www.bbk.bund.de/cln_007/nn_402322/EN/00_Home/homepage_node.html_nnn=true, 2008.
38. http://www.bbk.bund.de/cln_027/nn_398882/DE/02_Themen/06_SchutzKritischerInfrastrukturen/01_Themen/02_InformationstechnikundTelekommunikation/Informationstechnikund-Telekommunikation_node.html_nnn=true, 2008.
39. http://www.bbk.bund.de/cln_007/nn_398880/DE/02_Themen/05_Krisenmanagement/01_deNIS/deNIS_node.html_nnn=true, http://www.denis.bund.de, 2008.
40. http://www.bbk.bund.de/cln_007/nn_401142/DE/02_Themen/05_Krisenmanagement/01_deNIS/02_deNISII/deNISII_node.html_nnn=true, 2008.
41. http://www.bka.de, 2008.
42. http://www.bmwi.de, 2008.
43. http://www.bundesnetzagentur.de/enid/0a888f9d9a85f3748b2d8fb635f752e7,0/xn.html, 2008.
44. http://www.bmj.bund.de/enid/4e02aa38526e9a3069072ac5fa5dbc01,0/aktuelles_13h.html, 2008.
45. Official Journal of the European Union. (2005). L 69/67-71, http://eur-lex.europa.eu/JOHtml.do?uri=OJ:L:2005:069:SOM:en:html.
46. http://www.bmvg.de/portal/a/bmvg, 2008.
47. https://www.sicher-im-netz.de/default.aspx?, 2008
48. http://www.initiatived21.de/en/English.104.0.html, 2008.
49. Ennen, G. (2001). CERT-Bund—eine neue Aufgabe des BSI. In *KES Zeitschrift für Kommunikations- und EDV-Sicherheit*, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, p. 35, http://www.bsi.bund.de/certbund/index.htm.
50. Ennen, *CERT-Bund—eine neue Aufgabe des BSI*, op. cit., p. 35.
51. http://www.cert-verbund.de/index.html, 2008.
52. *The IT Security Situation in Germany 2007*, op. cit., section 7.3.
53. https://www.buerger-cert.de, 2008.
54. http://www.buerger-cert.de/ueberuns.aspx, 2008.
55. http://www.gesetze-im-internet.de/tkg_2004/BJNR119000004.html, 2008.
56. Informations- und Kommunikationsdienste Gesetz (IuKDG). http://www.artikel5.de/gesetze/iukdg.html#fn.

57. Suter, M. (2002). *Interview with a Representative of the Consulting Company Industrieanlagen-Betriebsgesellschaft (IABG)*.
58. http://bundesrecht.juris.de/tmg/BJNR017910007.html, 2008.
59. der Justiz, B. *Gesetz über Rahmenbedingunge für elektronische Signaturen (Signaturgesetz—SigG)*, http://www.gesetze-im-internet.de/sigg_2001/BJNR087610001.html, 2008.
60. Cybercrimelaw. Country Survey Germany, http://www.cybercrimelaw.net/countries/germany.html, and Bundesministerium der Justiz. German Penal Code (Strafgesetzbuch), http://www.gesetze-im-internet.de/stgb/index.html.
61. Jahrgang B. (2007). *Teil I Nr. 38, ausgegeben zu Bonn am 10*, pp. 1786–1787, http://www.computerundrecht.de/6758.html.

# HUNGARY

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

In 2005, Hungary welcomed the EU program for Critical Infrastructure Protection (EPCIP). Even though some policies in the field of CIP had already been implemented before, the EU program highly influenced the further development of Hungary's CIP and CIIP policies. Accordingly, the Hungarian definition of the concept of critical infrastructure corresponds to the definitions of the EU as formulated in the Green Paper of the EU Commission [1].[1] Critical Infrastructures, according to the Hungarian Green Book, are defined as interconnected, interactive, and interdependent infrastructure elements, establishments, services, and systems that are vital for the operation of the national economy and public utilities to maintain an acceptable level of security for the nation, individual lives, and private property, as well as concerning the maintenance of

[1]Cf. the article on the EU in this volume.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

the economy, the public health services, and the environment.[2] The CI sectors in the Green Book include the following:

- Information and Telecommunication Systems,
- Energy,
- Water Supply,
- Transport,
- Public Health,
- Food-Products Supply,
- Banking and Financial Sector,
- Industry,
- Government Institutions,
- Public Security and Homeland Defense.[2]

In addition, a legal definition has been agreed that includes e-communications and postal services among the nation's critical infrastructures. According to article 2, no. 11 of ministerial decree no. 27/2004 of the Ministry of Informatics and Communications on the National Alert Service of the Postal and Communications Sector and the Tasks of the Designated Service Providers, a critical information infrastructure can be "any object or service, including e-communications and informatics systems, of which inoperability or destruction can severely impair, either separately or in conjunction with other inoperable or destroyed critical infrastructure, national security, the life and property of citizens, the proper functioning of national economy and public services".[2]

## 2 PAST AND PRESENT INITIATIVES AND POLICY

The increasing importance of ICT in the Hungarian economy has prompted the government to increase its commitment to the security of information systems and networks in general and of CIIP in particular. These efforts were fostered by the EU, which has implemented various programs to strengthen the information society in its member states. Thus, Hungary has initiated different initiatives and policies aiming to promote the information society in recent years. This section presents the most important initiatives and policies with regard to CIIP and information security.

### 2.1 The National Security Strategy of the Republic of Hungary

The protection of important information systems and critical information infrastructures is an integral part of the National Security Strategy of the Republic of Hungary. The challenges of the information society and the vulnerabilities of the new communication technologies are explicitly mentioned as risk factors for the country [2].

The National Security Strategy also clearly points out the need for collaboration with international and private partners in the field of protection of information systems: "Successful protection [of information systems] requires close co-ordination with allies, as well as information and telecommunication providers and research centers" [3].

[2]Information provided by an expert.

On 18 December 2007 the National Security Cabinet of the government decided to establish a new Information Security Inspectorate (ISI), into whose jurisdiction CIIP will also fall, to issue new regulation on ISI, and to set up a coordination body for information security and CIIP. These tasks are to be fulfilled until the end of 2008.

### 2.2 The Hungarian Information Society Strategy

Despite of the rapid evolvement in the last years [4], internet penetration in Hungary is still relatively low, and the number of "digital illiterates" is considered to be too high. Hence, the focus of the strategy is the development of a modern society and a competitive economy based on a widespread usage of information and communication technologies.

The Information Society Strategy consists of two pillars: the introduction of information technologies into (economic) processes, and the implementation of public electronic services.

Information security and the protection of privacy are seen as essential parts of the development towards an information society, since the extent to with ICT is used is determined by the extent to which people trust new technology. The strategy therefore identifies IT security as a field of governmental intervention and highlights the necessity of regulatory, organizational, and technological measures.

### 2.3 The National Information Infrastructure Development Program (NIIF)

The National Information Infrastructure Development Program [5] was initiated to operate and advance the network of research bodies in Hungary. The program, which has been running since 1986, is the oldest and best established program for information and communication technology in Hungary. As a research program, the NIIF is essential for the development of the information society. By providing up-to-date information infrastructure for the academic and research community, the program introduces advanced network technology in Hungary.

The technical expertise of the NIIF and its broad network of national and international contacts are important for CIIP. The NIIF also operates a Computer Incident Response Team (CSIRT, see chapter on Early Warning and Public Outreach), and cooperates closely with other institutions involved in research on network security.

### 2.4 Security Evaluation and Certification Scheme

Based on international standards like the Common Criteria and the Common Evaluation Methodology [6], the Ministry of Informatics and Communications launched the Hungarian Information Security Evaluation and Certification Scheme (MIBETS) [7]. MIBETS assists in evaluating and testing the security of software.

In addition, the ministry introduced the Information Security Management Framework (MIBIK), which aims to evaluate security measures at the organizational level.

The current government scheme includes an updated version of the MIBETS and MIBIK, now jointly abbreviated as MIBA. Government IT systems must be in compliance with the recommendations of the scheme, and a supervisory body will begin operating within the Prime Minister's Office Electronic Government Center from the first half of 2008.

## 3 ORGANIZATIONAL OVERVIEW

After the parliamentary elections of April-May 2006, the organization of the government was restructured. With regard to CIIP and the development of the information society, the most important change was the integration of the Ministry of Informatics and Communication-which was the central body for questions related to information and communication technology-into the Ministry of Economy and Transport and the Prime Minister's Office. The major tasks of CIIP are now mainly allocated in different ministries:

- *Ministry of Economy and Transport [8].* As the ministry responsible for the maintenance and development of economic infrastructure—including the information infrastructure—the Ministry of Economy and Transport coordinates the various efforts in the field of CIP and CIIP;
- *Prime Minister's Office [9].* Through the Electronic Government Center [10], the Prime Minister's Office coordinates the efforts with regard to e-Government, as well as other CIIP-related issues;
- *Ministry of Defense [11].* This ministry is responsible for national security, including the security of information. In particular, it is responsible for protecting state secrets and public data;
- *Ministry of Justice and Law Enforcement [12].* The duties and responsibilities of this ministry include crime prevention and data protection. It controls the Public Administration and Central Electronic Public Services Office, which is the central body for all tasks relating to the provision of e-government services and the management of electronic records and documents.

Since information security and CIIP is a horizontal issue that cuts across the responsibilities of individual government departments, Hungary has established a number of inter-ministerial bodies dealing with these tasks. In addition, Theodore Puskás Foundation, which works as a public-private partnership, plays an important role in CIIP, since it operates the national Computer Emergency Response Team (CERT-Hungary).

### 3.1 Public Agencies

***3.1.1 The National Communications Authority (NCA).*** Based on the Electronic Communications Act of 2003, the National Communications Authority was established in 2004 as an independent regulatory body for communications. The NCA's main task is to support the development of the communications market and to ensure that every citizen has access to affordable and reliable communications services. The NCA constantly analyzes the market and exchanges information with national and international experts, and adapts its capabilities, methods, and operations accordingly.

The NCA is also responsible for the National Alert Service (NAS) in the postal and communication sectors, the operation of which has been outsourced to the CERT-Hungary Center of the Theodore Puskás Foundation (see chapter on Early Warning and Public Outreach). The NAS is based upon the co-operation of designated service providers who report the incidents affecting their services to the NAS. The main task of NAS is to gather and distribute these reports and to co-ordinate among service providers in case of

emergency in affected regions, most frequently in case of spring floods in North-Eastern Hungary.[3]

***3.1.2 The National Board for Communications and Information Technology.*** The National Frequency Allocation Board—the legal predecessor of the National Board for Communications and Information Technology [13]—was established in 1993 by the government as an independent consulting and recommendation-making body for the allocation of radio and television frequencies. Over the years, its jurisdiction has been expanded, and today, the board is engaged in the fields of information technology, telecommunication, and media.

Some of the members of the board are appointed by the government (e.g., the chairman, who is appointed by the President of the Republic), but there are also members appointed by scientific institutions and by the lobbies of the telecommunication companies. This heterogeneous composition ensures that the most important interests are represented, so that the board's recommendations are well-balanced.

The board elaborates drafts of laws and decrees related to IT or telecommunication and aims to foster the development of the information infrastructure.

### 3.2 Public-Private Partnerships

***3.2.1 Theodore Puskás Foundation.*** The Theodore Puskás Foundation [14] was established in 1992. It was co-founded by the government of Hungary and several distinguished institutions and businesses. It operates as a non-profit, public benefit organization. Its main objective is the dissemination of advanced technologies in Hungary. The foundation's activities include scientific research, consultations, and instruction in the field of information technologies.

In 2004, the Ministry of Informatics and Communication contracted the foundation to operate the national Computer Emergency Response Team (CERT-Hungary, see below), in consideration of its good reputation of the foundation and its research experiences in the field of information technology.

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 Computer Emergency Response Teams (CERTs)

In Hungary, there are three important CERTs. Each of them serves a different constituency.

***4.1.1 CERT-Hungary.*** CERT-Hungary [15] is the governmental and national CERT. It is operated by the Theodore Puskás Foundation and was established in 2005. In its function as governmental CERT, it aims to improve information security of public agencies and is responsible for the technical aspects of CIIP. In order to combat high-tech crime efficiently, CERT-Hungary has developed direct communication channels to the national police force, and closely collaborates with all other agencies involved in CIIP [7]. CERT-Hungary is an accredited member of all main CERT forums, and acts as a National Contact Point for incident-handling and CIIP-related issues.

[3]Information provided by the Hungarian experts involved.

Furthermore, CERT-Hungary offers also some free services for the public, in particular warnings about emerging threats and new vulnerabilities, and provides chargeable services for private companies, e.g., intrusion detection, security audits, or malware analysis. Finally, CERT-Hungary coordinates a SCADA working group, which is organized jointly by government agencies and the operators of SCADA networks.[3]

***4.1.2 Hun-CERT.*** Hun-CERT [16] is operated by the Computer and Automation Research Institute of the Hungarian Academy of Sciences (MTA SZAKI) [17]. It is sponsored by the Council of Hungarian Internet Service Providers (ISZT) [18] and mainly serves the interests of the members of the council. However, it is the intention of Hun-CERT to disseminate information on network security information among the general public.

Hun-CERT deals with all kinds of computer security incidents affecting Hungarian internet service providers. It supports system administrators in tackling these incidents. The level of support given varies according to the type and severity of the incident, the available resources of Hun-CERT, and the size of the affected community).

***4.1.3 NIIF-CERT.*** The NIIF-CSIRT (Computer Security Incidents Response Team of the National Information Infrastructure Development Program) [19] helps the members of the academic networks (NIIF and HUNGARNET) to handle all kinds of security incidents. The NIIF-CSIRT also disseminates important security-related information and warnings to its members.

### 4.2 Hungarian Financial Services ISAC

In 2007, with the coordination of CERT-Hungary, the Hungarian Financial Services ISAC (Information Sharing and Analysis Center) was formed, involving law enforcement, the Hungarian banking association, the Hungarian Financial Regulatory Authority, and individual banks, including the biggest commercial banks. The cooperation between the parties resulted in several exercises, an incident handling directory, and cooperation on a recommendation about IT security in online banking.[3]

### 4.3 Awareness Raising Programs

The www.biztonsagosinternet.hu project ("biztonsagos" means "safe") was launched by CERT-Hungary in May 2006 in order to provide a website for the general public with information on IT security in an easy understandable manner. The project is an adaptation of the German awareness-raising-program BSI für Bürger,[4] where the structure of the German model was adopted, and the texts were fitted to the Hungarian circumstances. The website gives advice for internet usage in general, and for e-shopping and e-banking in particular; it provides information on spam, viruses, and other threats to information security, and demonstrates how users can protect their privacy (with a special focus on child protection). Other awareness-raising programs include www.internethotline.hu and www.baratsagosinternet.hu. Both initiatives came into being as part of the Safer Internet Program—the first operating as an internet hotline for reporting harmful and illegal content, the other being the awareness node of Hungary.

[4]Cf. Country Survey Germany (in this volume).

The "e-Inclusion, be part of it!" [20] campaign was launched in December 2007. It aims to urge European governments and associations to give disabled people access to the advantages that the internet and information and communication technologies provide. The EU has issued three official calls since 2006 urging European governments to promote the advantages and digital opportunities of ICT for senior citizens, ill or disabled people, women (including those on maternity leave), minorities, or people living in rural areas of Hungary. Not only is Hungary's effort scant as far as the issue of inclusion in the information society is concerned. The majority of the Hungarian population are not aware of the advantages of the internet. The EU aims to change this situation by reducing the ratio of 'digital analphabetism' by half by 2010.

The Forum of Hungarian IT Organizations for Information Society (Inforum), together with other associations and firms, has announced plans to join the EU's initiative and is in the process of launching the e-Inclusion Year 2008, Hungary movement.

## 5 LAW AND LEGISLATION

### 5.1 Penal Code

The Hungarian Penal Code includes several sections that are of relevance with regard to CIIP.[5] Particularly important are Articles 300/C and 300/E.

*Article 300/C.* Criminal Conduct for Breaching Computer Systems and Computer Data: This article states that any person who gains unauthorized entry to a computer system shall be punished by imprisonment or community service. The punishment shall be more severe if the person alters, damages, or deletes data without permission, and particularly if the act is committed for financial gain.

*Article 300/E.* Compromising or Defrauding the Integrity of the Computer Protection System of Device: This article prohibits the creation, obtaining, and distribution of software, passwords, entry codes, or other data that can be used to gain access to a computer system or network illegally.

### 5.2 Act on Protection of Personal Data and Disclosure of Data of Public Interest

Enacted in 1992, the Personal Data Protection Act (Act LXIII, Article 10) [22] sets rules and safeguards regarding the processing of personal data by public and private bodies. Its application is controlled by the Parliamentary Commissioner for Data Protection and Freedom of Information.

### 5.3 Act on Electronic Commerce and Information Society Services

Adopted in 2001, this act implements an EU directive on electronic commerce. In doing so, it not only integrates the EU directive, but also makes use of the regulatory solutions included in the German (TDDSG, Mediendienststaatsvertrag) and US (Digital Millenium Copyright Act) legislation, especially in the sections relating to the liability of Information Service Providers (ISPs) and the notice-and-takedown procedure. The act governs the legal relationships of individuals, legal persons, and organizations for the

[5]For an overview on the cybercrime legislation of Hungary, see: [21].

purposes of e-commerce, in cases where the service is provided for or from the territory of Hungary [22].

### 5.4 Act on Electronic Signature

The Act on Electronic Signature [23] was adopted on 29 May 2001 and entered into force on 1 September 2001. It provides for legal recognition of electronic signatures (e-signatures) and electronic documents. Electronic documents and e-signatures are presumed to be admissible evidence in court and may not be challenged successfully based on the mere fact of their electronic form. An electronic document signed with an e-signature is deemed to be in compliance with a statutory requirement for a handwritten signature on a paper document. However, the act excludes family-related documents (e.g., marriage certificates and divorce decrees), and those documents must continue to be in paper form to have legal validity. Also, consumers are not obliged to accept the electronic format; if a consumer objects, a business firm must use paper documents. Hungarian government departments may elect to issue or accept electronic documents. Although all types of e-signatures are recognized, the digital signature enjoys most-favored status because it utilizes cryptographic methods resulting in a heightened degree of reliability and security.

### 5.5 Further Regulations with Regard to CIIP and Information Security

In addition to the acts mentioned above, there are several further acts and decrees referring to CIIP and information security to some extent:

- Act no. CXII of 1996 on financial institutions and enterprises has a separate section in §3B on the security requirements of IT systems within financial institutions and enterprises;
- Act no. LXXXV of 1998 on the establishment of the National Security Supervision Office (NSSO): The NSSO is to provide advice on security for personal, physical, document and information, and industrial purposes. The office is also in compliance with the security measures promulgated within NATO, with regard to classified information;
- Government Decree 180/2003 on the rules of procedures of NSSO. Chapter IV regulates the detailed procedures of electronic security supervision;
- Ministerial Decrees 24/2004 and 27/2004 of the Ministry of Informatics and Communications on the National Alert Service in the Postal and Communications Sector and the Designated Service Providers: Ministerial Decree 24/2004 obliges service providers to co-operate in the National Alert Service (NAS) of the Postal and Communication Sector. Decree 27/2004 sets the rules for the organization and operation of the NAS and gives a thorough list of definitions for CIIP (e.g., critical infrastructure, network security);
- Government Decree 84/2007 on the security measures of the Central Electronic Service System and adjoining systems: This decree states that the same security measures have to apply to all systems of the Central Electronic Service System (CESS), which include the government backbone, the government portal, the client portal, and all the services available through these gateways. The decree lists the

uniform requirements of IT security for the CESS and includes the IT catastrophe recovery plan. The Prime Minister's Office is the operator of the Central Electronic Service System.[2]

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Bence Birkás and Ferenc Suba of CERT, Lajos Muha of Dennis Gabor College, Barbara Locher of the Ministry of Economics and Transport, Peter Csokany of the National Communication Authority, and Csaba Sandor of the Electronic Government Center, who validated the content of this chapter.

## REFERENCES

1. Commission of the European Communities (2005). "Green Paper on a European Program for Critical Infrastructure Protection", Brussels.
2. Ministry of Foreign Affairs of the Republic of Hungary. (2007). The National Security Strategy of the Republic of Hungary, Chapter II.1.6: Challenges of the Information Society, Budapest. http://www.mfa.gov.hu/kum/en/bal/foreign_policy/security_policy/national_sec_strategy_of_hun.htm "The National Security Strategy of the Republic of Hungary", Chapter II.1.6.
3. Government of Hungary. "The National Security Strategy of the Republic of Hungary", Chapter III.3.7.
4. Detreköi Á. (2006). "Information Society in Hungary". http://www.agile2006.hu/papers/detrekoi_agile_welcome.pdf.
5. http://www.niif.hu/en, 2008.
6. http://www.commoncriteriaportal.org/, 2008.
7. Suba F. and Drencsán J. (2005). "Hungary's National NIS Projects". In *ENISA Quarterly no. 12*, ENISA (European Network and Information Security Agency), Heraklion, pp. 16ff.
8. http://www.gkm.gov.hu, 2008.
9. http://www.meh.hu/english, 2008.
10. http://www.ekk.gov.hu, 2008.
11. http://www.honvedelem.hu, 2008.
12. http://irm.gov.hu/?lang=en, 2008.
13. http://en.nhit.hu/start, 2008.
14. http://www.neti.hu/pta/en/index, 2008.
15. http://www.cert-hungary.hu, 2008.
16. http://www.cert.hu/index.php?option=com_content&task=view&id=16&Itemid=36, 2008.
17. http://www.sztaki.hu/?en, 2008.
18. http://www.iszt.hu/iszt/English/, 2008.
19. http://www.niif.hu/en/csirt, 2008.
20. http://einclusion.hu, 2008.
21. Council of Europe. "Project on Cybercrime, Cybercrime Legislation—Country Profile: Hungary". http://www.coe.int/cybercrime, 2008.
22. European Commission. "EGovernment in Hungary, Legal Framework", p. 10. http://ec.europa.eu/egov, 2008.
23. http://www.epractice.eu/document/3374, 2008.

# INDIA

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

In India, the following sectors are considered critical:

- Banking and Finance,
- Insurance,
- Civil Aviation,
- Telecommunications,
- Atomic Energy,
- Power,
- Ports,
- Railways,
- Space,
- Petroleum and Natural Gas,
- Defense,
- Law Enforcement Agencies.

These 12 critical sectors were identified by the National Task Force on Y2K a few years ago, taking into account the extent of penetration of information technology in these sectors and the impact that a disruption of any of these sectors would have [1].

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

In India, many efforts in the field of CIIP were triggered by the government's goal of making the country a leading knowledge-driven global economy by boosting IT and e-business. In 1998, the prime minister of India announced a drive to make India an IT superpower and one of the largest producers and exporters of software in the world within the next ten years. The government of India has recognized the potential of IT for

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

rapid national development [2]. Therefore, it has established a National Task Force on Information Technology and Software Development [3] and a Department of Information Technology (DIT) within the Ministry of Communications and Information Technology, also dealing with CIIP [4].

### 2.1 National Task Force on Information Technology and Software Development and Information Technology Action Plan

The Indian government has given top priority to developing an appropriate action plan for the country to emerge as a global leader in the field of IT. As a first step, the National Task Force on IT and Software Development [3] was set up by the then Prime Minister Atal Behari Vajpayee on 22 May 1998, under the chairmanship of the deputy chairman of the planning commission. This task force had a mandate to formulate the draft of a National Informatics Policy, including [5]:

- To recommend an appropriate institutional mechanism to implement this policy as a national mission with the participation of the central and state governments, industry, academic institutions, and society at large;
- To prepare a vision statement that will excite and energize the people of India, creating a faith in IT for personal and national growth. The task force will also suggest a strategy for the effective articulation and dissemination of that vision, so as to create an ethos, an ambiance, a mind-set, and a work culture that is consistent with the needs of the emerging knowledge-driven global civilization;
- To prepare a blueprint for the nationwide adoption of information technology, with a network of task forces at all governmental and non-governmental levels.

The IT Task Force submitted its first report in the form of an Information Technology Action Plan to the prime minister on 4 July 1998. The report contained a special section on IT for all by Year 2008, the centerpiece of which is a major national campaign called Operation Knowledge, focusing on spreading IT and IT-based education at all levels.[1]

The establishment of the Task Force is a clear indication that IT is an area where India wants to achieve global pre-eminence. It is hoped that IT, fostered by these government policies, will prove immensely useful in all areas of national economy—especially industry, trade, and services— and will contribute significantly to making India a global economic power.[1]

### 2.2 National e-Governance Plan (NeGP)

The government of India approved the National e-Governance Plan [7] (NeGP) on 18 May 2006. The plan lays the foundation and provides the impetus for long-term growth of e-governance within the country. The plan is intended to create the right government and institutional mechanisms, to set up the core infrastructure and policies, and to make the public administration more responsive to the needs of citizens and businesses.

[1]The IT Action Plan included, among others, the following measures: Ministries and departments to earmark 1-3 per cent of their budget for IT; IT literacy requirement for government/public-sector employment; software and IT to be treated as a priority sector by banks; zero tax on all IT products by 2002; internet access through cable TV; early introduction of IT legislation; networking of all engineering/medical colleges and universities before 2000 [6].

The NeGP has started to realize three important elements of the e-Governance Plan that form the core infrastructure for effective service delivery: Data processing centers, State Wide Area Networks (SWANs), and Common Services Centres (CSCs). In addition, the government announced in 2006 that it would enhance its efforts to bring a number of services online. Subsumed under the label 'E-District', these services are provided at the district level and serve as the primary interface between citizens and the government [8].

### 2.3 Core Group on Standards for e-Governance

Under the NeGP, standards for e-governance are crucial to ensure integration and interoperability of data and electronic applications. The Department of Information Technology (DIT) has therefore constituted a Core Group on Standards for e-Governance [9] to develop an institutional mechanism and processes, and to recommend key areas for standardization. Some of the priority areas for standardization are:

- Technical standards,
- Localization standards,
- Quality and documentation,
- Security standards,
- Metadata and data standards for various application domains.

An apex body has been constituted under the chairmanship of the secretary of the DIT with senior representatives from the government, the National Association of Software and Service Companies (NASSCOM) [10], the Bureau of Indian Standards (BIS), and others with a mandate to approve, deliver notification of, and enforce the standards formulated by various working groups and to ensure that they are in accordance with international practices.

The National Informatics Centre (NIC) [11] publishes whitepapers on all the desired standards, which serve as discussion papers for the working groups that develop the standards.[2] The working groups with representatives of the DIT, associations, industry, academia, and central and state governments, etc., are constituted with the approval of the DIT.

The standards approved by the apex body are released on the web by the Standardization Testing and Quality Certification (STQC) Directorate, an office attached to the DIT. The STQC further ensures conformance and certification (where required) of these standards. The e-Governance Division of the NIC and the STQC function in tandem with the e-Governance Programme Management Unit at DIT.[3]

[2]The National Informatics Centre (NIC) of the Department of Information Technology provides network backbone and e-governance support to the central government, state governments, administrations, districts, and other government bodies. It offers a wide range of ICT services, including a nationwide communication network for decentralized planning, improvement in government services, and greater transparency of national and local governments. The NIC collaborates closely with central and state governments in implementing IT projects.

[3]Information provided by an expert.

## 3 ORGANIZATIONAL OVERVIEW

In the Indian government, the National Information Board (NIB) is at the very top of the national information security structure. Directly linked to the NIB are the National Technology Research Organization (Technical Cybersecurity) and the National Information Security Coordination Cell (NISCC), which is part of the National Security Council Secretariat (NSCS). The NIB has instructed the NSCS to coordinate cyber-security activities across the country. The NISCC provides input for the consideration of the NIB. It works through the Sectoral Cyber Security Officers (SCOs).

Directly below the NIB are the Information Infrastructure Protection Centre (IIPC), followed by state cyber-police stations; and the Computer Emergency Response Team India (CERT-In), followed by state- and sectoral-level CERTs. Various ministerial coordinators of special functions are also situated at this level, as is the Development and Promotional Section of the Ministry of Communications and Information Technology (MOC).

As a public-private partnership initiative, the Indo-US Cyber Security Forum strives to discuss and implement increasing cooperation in high-technology between the two countries.

### 3.1 Public Agencies

***3.1.1 National Information Board (NIB).*** The establishment of the National Information Board (NIB) was recommended by a group of ministers. It consists of 21 members. The national security advisor is the chairman of the board, while the deputy national security adviser serves as its member secretary. The NIB acts as the highest policy formulation body at the national level and periodically reports to the Cabinet Committee on Security of the Government of India, headed by the Prime Minister. The NIB is at the very top of the information security structure [12].

***3.1.2 National Information Security Coordination Cell (NISCC).*** The NIB has charged the National Security Council Secretariat (NSCS) with coordinating cyber-security activities across the country, covering both the public and the private sectors. NISCC provides input to NIB for its consideration. It works through the Sectoral Cyber Security Officers (SCOs). There are 20 such SCOs in various ministries, where the senior officer holds the rank of a joint secretary or director. The NISCC deals with the following topics: CERT functions, research and development, encryption, laws, interception and early warning, cyber-crime, training, and international cooperation. It represents the government in international forums for cyber-security and issues related to large scale cyber-related incidents.[3]

***3.1.3 Ministry of Communications and Information Technology (MOC): Department of Information Technologies (DIT).*** The Department of Information Technologies (DIT) [13], part of the Ministry of Communications and Information Technology (MOC) [14], was established with the purpose of making India a leading IT nation by 2008. Through the DIT organization, the Indian government has undertaken several initiatives and strategies:

- The promotion of the internet and provision of IT infrastructure;
- The development of legislation;

- The support of IT education and development;
- The promotion of standardization, testing, and quality in IT;
- The establishment of an Information Security Technology Development Council (ISTDC);
- The creation of a National Information Security Assurance Framework;
- The establishment of Inter Ministerial Working Groups [15].

The Indian Computer Emergency Response Team (CERT-In) and the Controller of Certifying Authorities (CCA) are also DIT organizations. The Standardisation, Testing, and Quality Certification (STQC) Directorate and the National Informatics Centre (NIC) are also attached offices of the DIT [16].

The DIT has set up the following Inter Ministerial Working Groups on:

- Cyber-Security Education and Research;
- Cyber-Security Assurance and Awareness;
- Encryption Policy and PKI;
- Legislation and Forensics in Cyberspace;
- Critical Infrastructure Protection [17].

***3.1.4 Standardization, Testing and Quality Certification (STQC) Directorate.*** The Standardization, Testing, and Quality Certification (STQC) Directorate is an office attached to the DIT. The STQC provides quality and security assurance services that meet international standards to Indian companies and users. The STQC program has been in place for over three decades, and the STQC has positioned itself as a prime provider of assurance services to both the hardware and the software industry, as well as for users. The recent focus of the DIT on IT security, software testing and certification, and the assignment of a national assurance framework, has further raised the responsibility of the STQC as well as the expectations it must meet [18]. The STQC worked together with the US National Institute of Standards and Technology (NIST) to create a US standard for controls of Information Security, SP-800-53.

***3.1.5 Information Security Technology Development Council (ISTDC).*** The main objective of the Information Security Technology Development Council (ISTDC) is to facilitate, coordinate, and promote technological advancements, and to respond to information security incidents, threats, and attacks at the national level. ISTDC was established for the following functions [19]:

- To evaluate cyber-security project proposals, and to provide recommendations for further processing by DIT;
- To review on-going projects through monitoring committees and recommend any modification in scope, funding, duration, additional input, termination, and transfer of technology;
- To recommend follow-up action on completed projects concerning transfer of technology and the initiation of subsequent phases;
- To form project review and steering groups of projects approved and funded by the DIT.

### 3.2 Public-Private Partnerships

*3.2.1 Indo-US Cyber Security Forum.* In pursuance of the Indo-US Cyberterrorism Initiative announced by Indian Prime Minister Atal Behari Vajpayee and US President George Bush in Washington in November 2001, the first plenary session of the Indo-US Cyber Security Forum was held at the National Security Council Secretariat (NSCS) in India in April 2002. The second plenary meeting was held in Washington, D.C. in November 2004. This meeting resulted in the creation of five working groups on legal issues and law enforcement, research and development, emergency response and watch and warning, defense cooperation, and standardization. In 2005, the NSCS organized five seminars and a workshop with the help of the Confederation of Indian Industry (CII). There has also been some exchange of experts. In 2006, the third Plenary of the Indo-US Cyber Security Forum was held. The Confederation of Indian Industry, in consultation with its US counterpart, decided to set up an India Information Sharing and Analysis Center and an India Anti-Bot Alliance to raise awareness about emerging threats in cyberspace. CERT-In and the US national Cyber Security Division agreed to share expertise in artifact analysis, network traffic analysis, and exchange of information. The research and development group concentrates on hard problems of cyber-security, cyber-forensics, and anti-spam research [20].

The Indo-US Cyber Security Forum is a part of the Indo-US High Technology Group, a public-private partnership between India and the US established to discuss and implement ways and means of increasing cooperation between the two countries in high-technology areas.

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 Indian Computer Emergency Response Team (CERT-In)

The Indian Computer Emergency Response Team (CERT-In) [21] was established in January 2004 by the Department of Information Technologies (DIT) as part of the international CERT community. It has a mandate to respond to computer security incidents reported by the national computer and networking community as well as to create security awareness among Indian IT users. The main CERT is located in New Delhi, with backup in Bangalore. It has reactive as well as proactive functions [22]. CERT-In aims to become India's most trusted agency for responding to computer security incidents. In addition, CERT-In will also assist Indian IT users in implementing proactive measures to reduce the risks of security incidents.

Another five sector-specific CERTs have been set up: three for the army, air force, and navy; one for banking, known as FinCERT; and one for railways, known as RailCERT. It is anticipated that more CERTs will be established for the telecom and the power sectors.

CERT-In recently appointed a panel of IT security auditors, whose tasks will include vulnerability assessment and penetration testing of the computer systems and networks of various organizations of the government, critical infrastructure organizations, and in other sectors of Indian economy [23]. The auditors will assist CERT-In in assessing the information security risks. They will determine the effectiveness of information security controls over information resources and assets that support operations in the auditor organizations at their request [23].

## 5 LAW AND LEGISLATION

In the year 2000, the government of India enacted the Information Technology Act (IT Act) to provide a framework for the legal recognition of electronic commerce in India. The IT Act provides for the establishment of a public-key infrastructure in India and addresses issues of cyber-crime and the admissibility of digital evidence. It achieves this through various provisions and by way of amendments to other statutes, such as the Indian Penal Code 1860, the Indian Evidence Act of 1872, the Bankers' Books Evidence Act of 1891, and the Reserve Bank of India Act of 1934. The amendments relate to the inclusion of electronic records and other such computerized data alongside the traditional forms of documents.

### 5.1 Information Technology Act 2000 (IT Act)

The IT Act comprises 13 chapters, divided into 94 sections. The chapters relevant to the present discussion are: Chapter V (Secure Electronic Records and Secure Digital Signatures), Chapter VII (Digital Signature Certificates), Chapter IX (Penalties and Adjudication), Chapter XI (Offences), and Chapter XII (Network Service Providers Not To Be Liable In Certain Cases).

The IT Act provides a much-needed legal framework for electronic transactions in India. The National Association of Software and Service Companies (NASSCOM), the leading trade body and the chamber of commerce of the IT software and services industry in India, summarizes some of its key progressive features as follows [24]:

- From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. First of all, these provisions have approved e-mail as a valid and legal form of communication in India that can be duly produced and approved in a court of law;
- Companies are now able to carry out electronic commerce using the legal infrastructure provided by the act;
- The act bestows legal validity and sanction on digital signatures;
- The act allows companies to become certifying authorities that may issue digital signature certificates;
- The act allows the government to issue legal notifications on the internet, a first step towards e-governance;
- The act enables companies to file any form, application, or other document with any office, authority, body, or agency owned or controlled by the government in such electronic formats as may be prescribed by the government;
- The IT Act also addresses important issues of security that are critical for the success of electronic transactions. The act includes a legal definition of the concept of secure digital signatures that must undergo a security procedure as stipulated thereunder;
- The act offers companies a statutory remedy in case anyone should break into their computer systems or network and cause damages or copy data. The remedy provided by the act is in the form of monetary damages not exceeding 10 million rupees.

In order to resolve IT-related disputes in a focused and timely manner, the IT Act provides for the constitution of a Cyber Appellate Tribunal, which acts as a forum for

original jurisdiction on issues arising under the IT Act. Appeals from the tribunal can be made to the relevant state high courts.

Section 79 of the IT Act declares that network service providers shall not be liable for any third-party information or data made available by them if they prove that the offense or contravention was committed without their knowledge or that they had exercised all due diligence to prevent the commission of such an offense. This provision is crucial, as it is the only one under which a network service provider can claim a defense under the provisions of the act.

In order to further strengthen the scope and ambit of the IT Act, a committee has been set up comprising several experts in cyber-law and data protection who will review the act and make necessary changes to ensure that the existing lacunae in the law can be filled. These amendments are likely to deal with provisions concerning third-party liability, issues of privacy and data protection security, and the replacement of written signatures with digital signatures, among others.

## 5.2 IT Related Offenses Under the IT Act

Section 43 of the IT Act specifies acts committed without the permission of the owner or person in charge of a computer, computer system, or computer network that may cause damage by destruction, alteration, deletion, addition, modification, or rearranging of any computer resource. The offenses relate specifically to: (a) accessing or securing access to a computer, computer system, or computer network; (b) downloading, extracting, or copying of data or information from such computers, computer systems, or computer networks; (c) introducing or causing the introduction of any virus or computer contaminant; (d) disrupting or causing disruption to computers, computer systems, or computer networks; (e) damaging or causing to be damaged any computer, computer system, or computer network or any programs residing therein; (f) denying or causing denial of access by any person authorized to use the computer system or computer network; (g) assisting a person in contravention of the IT Act; (h) manipulating a computer for financial benefit.

Sections 65 through 74 of the IT Act contain provisions relating to various cyber-crimes.[3]

***5.2.1 Hacking and Tampering with Computer Source Code.*** The popular and notorious offense of hacking is dealt with under Section 66 of the IT Act. Hacking is defined as the act of destroying, altering, deleting, diminishing in value, or injuriously affecting the information residing in a computer resource, by any means. An essential element of this offense is the intention or knowledge on the part of the perpetrator of causing the wrongful loss. This provision is often viewed as a "catch-all" provision because of its broad wording, which could be potentially used to cover any IT crimes that are not covered by any other provision of the IT Act.

Tampering with computer source code has been made an offense under Section 65 of the act. This provision applies to offenders who alter, conceal, or destroy computer source codes.

The maximum punishment for both hacking and tampering with computer source code is three years' imprisonment and/or a fine of up to 200,000 rupees, or both.

***5.2.2 Breach of Confidentiality and Privacy.*** Section 72 of the IT Act deals with the penalty for breach of privacy and confidentiality. It applies to situations where individuals

who have gained access to any electronic record, book, register, information, document, or other material by virtue of powers conferred to them under the IT Act or related legislation make an unauthorized disclosure of the same.

Offenses relating to digital signatures, which include misrepresentation or suppression of material facts from the Digital Signature Certificate and publishing a digital signature for fraudulent purposes, are also covered under this section.

## 5.3 IT-Related Offenses under the Indian Penal Code

The Indian Penal Code of 1860 (IPC) is the statute governing criminal jurisprudence in India. With the enactment of the IT Act, specific provisions of the IPC dealing with offenses relating to documents and paper-based transactions were amended to include crimes conducted using electronic devices.

The amendments made to the IPC refer to the sections dealing with forgery, extortion, criminal breach of trust, criminal intimidation, and fraud.

***5.3.1 Forgery.*** The offense of forgery is covered by Section 463 of the IPC. It is defined as an act of creating false documents or electronic records for the purpose of causing damage or injury to the public or any person, or to commit fraud. A "forged document or electronic record" is defined under Section 470 as a document or electronic record that is false and has been forged either entirely or in part. The general offense of forgery is further classified into a range of individual offenses. These include forgery for the purpose of cheating or defaming another party; making, using, or possessing forged documents; and counterfeiting authentication marks and designs.

***5.3.2 Extortion.*** Such an offense involves one person dishonestly inducing another to deliver any property or valuable security by intentionally putting fear of injury in that person's mind. This offense is dealt with by the IPC under Section 383. When such crimes are committed electronically, they would be included within the purview of this section as well. Web-jacking and threatening e-mails are examples of extortion committed by an electronic medium.

***5.3.3 Criminal Breach of Trust.*** Section 405 of the IPC defines "criminal breach of trust" as any act whereby a person who has been entrusted with property, or with any power over any property, dishonestly misappropriates the property, makes wrongful use of the property, dishonestly disposes of that property, or induces any other person to do so.

***5.3.4 Criminal Intimidation.*** When a person threatens another or someone in whom such other person is interested with injury to their physical well-being, reputation, or property and causes them to commit or desist from actions against their free will in order to avoid the execution of such threats, this constitutes criminal intimidation. When such threats or intimidation occur through e-mails or other electronic means of communication, they are punishable under Section 503 of the Indian Penal Code. Threats of denial-of-service attacks, e-mail bombing, virus attacks, cyber-stalking, etc., can be used to intimidate a person and amount to criminal intimidation.

***5.3.5 Cheating.*** Section 420 of the Indian Penal Code deals with fraud cases. Under the section, whoever cheats and consequently dishonestly induces a person to deliver any property (to any other person), or to alter or destroy the whole or any part of a valuable

security, shall be punished. When fraud is committed with the use of a computer, as in the case of credit card fraud, money-laundering, or e-mail spoofing, it is punishable under the IPC.

### 5.4 Further Issues

***5.4.1 Data Protection.*** The only provision of the IT Act that currently addresses the issues of data protection and confidentiality is Section 72. To address the issue of misuse of personal information and data, India is currently in the process of reviewing the various clauses of the IT Act. In the absence of a specific law on data protection, appropriate principles, safeguards, and liquidated damages for breach would need to be built into a contract between relevant parties to ensure adequate remedies for data protection.

The Indian Contract Act of 1872 (Contract Act) codifies the way one enters into a contract, the execution of a contract, the implementation of its provisions, and the effects of breach of such contract. Contracts are among the best ways for foreign firms to protect their data and intellectual property while subcontracting work to India. The Indian Contract Act provides adequate safeguards to foreign companies, provided that both firms (Indian and foreign) agree to the contract. The companies subcontracting their work to India need to enter an exhaustive Service Level Agreement (SLA) with their vendor that covers various aspects of data security and confidentiality. This will help companies to safeguard against any fraud or misconduct.

***5.4.2 Copyright.*** The Indian Copyright Act of 1957 was amended in 1994–1995 to include penalties for any person who knowingly makes use of an illegal copy of a computer program. Such an act is punishable with a minimum imprisonment of seven days, although a sentence of up to three years can be imposed. The act further provides for fines of 50,000 to 2,000,000 rupees, a jail term up to three years, or both.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Subimal Bhattacharjee of Argus Integrated Systems and Luthra & Luthra, who validated the content of this chapter.

## REFERENCES

1. Vineeta, M. (1999). Critical sectors to be Y2K ready in time: government report. In *India Times*, http://www.apnic.net/mailing-lists/s-asia-it/archive/1999/10/msg00050.html.
2. Government of India. (1998). National task force on information technology and software development. *Information Technology Action Plan, (Preamble)*, http://it-taskforce.nic.in/infplan.htm#aa.
3. http://it-taskforce.nic.in, 2008.
4. http://mit.gov.in, 2008.
5. http://informatics.nic.in/archive/inf98jul/cover.htm, 2008.
6. http://it-taskforce.nic.in/index.html, 2008.
7. http://mit.gov.in/default.aspx?id=836, 2008.
8. Government of India. Ministry of communications and information technology. Department of information technology. (2007). *Annual Report 2006–2007*, p. 4. http://mit.gov.in/download/annualreport2006-07.pdf.

9. http://egov.mit.gov.in, 2008.
10. http://www.nasscom.org, 2008.
11. http://home.nic.in, 2008.
12. Mukesh Saini National Security Council, India, at the Indo-US Cyber Security Forum Washington, DC, 9–10 November 2004.
13. http://www.mit.gov.in, 2008.
14. http://www.moc.gov.in, 2008.
15. http://www.mit.gov.in/default.aspx?id=9, Chandrashekhar, R. (2005). On the national E-Governance plan—approach and key components. *National e Governance Plan—Workshop with States and UTs*. New Delhi. http://www.mit.gov.in/default.aspx?id=115.
16. http://www.mit.gov.in/default.aspx?id=12, 2008.
17. Presentation by Shri R. Chandrashekhar, op. cit.
18. http://www.stqc.nic.in, 2008.
19. http://www.nasscom.org//download/india.pdf, 2008.
20. http://www.indianembassy.org/newsite/press_release/2006/Mar/11.asp, 2008.
21. http://www.cert-in.org.in, 2008.
22. http://www.cert-in.org.in/roles.htm, 2008.
23. http://www.cert-in.org.in/audit-background.htm, 2008.
24. http://www.nasscom.org/artdisplay.asp?cat_id=852, 2008.

# ITALY

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Since information and communication technologies (ICTs) play an important role in a number of critical sectors, the protection of critical information infrastructures is crucial

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

for the well-functioning of the Italian society. In consequence, there are several strategy and policy papers with regard to CIP and CIIP (see the section on Past and Present Initiatives and Policies). These documents define the critical sectors consistently, so that it is possible to specify the sectors that are deemed to be critical, even if there is no official register of the critical infrastructures of Italy:

- Banking and Finance,
- Public Safety and Order,
- (Tele-) Communication,
- Emergency Services,
- Energy Production, Transportation, and Distribution,
- Public Administration,
- Health Care Systems,
- Transportation and Logistics (Air, Rail, Maritime, Surface),
- Water (Drinking Water, Waste Water Management),
- Information Services and the Media,
- Food supply.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

There is no central unit in Italy devoted to defining CIP and CIIP policies and strategies: Various activities are assigned to ministries and public bodies in charge of the different critical sectors, as well as those responsible for public safety and security. In addition, a variety of coordination efforts have been undertaken:

- In order to create an inter-sectoral forum and to improve awareness on CIIP, a Working Group on Critical Information Infrastructure Protection was set up in March 2003 at the Department for Innovation and Technologies of the Presidency of the Council of Ministers. All ministries involved in the management of critical infrastructures are represented in the group, together with many Italian infrastructure operators and owners as well as various research institutes. The working group ended its activities after publishing the Report on Critical Information Infrastructure Protection: The Case of Italy in 2004;
- The Ministry of Communication has established a special working group to analyze the responsibilities and security requirements that CIIP imposes on communication infrastructure operators, and to analyze the dependencies of the latter on other critical infrastructures. This working group has issued the following guidelines with regard to CIIP: The Network Security of Critical Infrastructures (2005); Network Security: From Risk Analysis to Protection Strategies (2005); Guideline on Managing Local Emergencies (2006). With the publication of these guidelines, the working group ended its activities;
- In July 2005, to coordinate activities better and improve the protection of CII with respect to cyber-attacks, the Postal and Communications Police was identified as the unit responsible for law enforcement initiatives in this area;
- In 2006, a new body for the coordination of all ministries and agencies involved in CIP was established. This body, named Tavolo interministeriale di coordinamento

ed indirizzo nel settore della protezione delle infrastrutture critiche (Tavolo PIC)[1] is chaired by the Military Advisor to the President of the Minister's Council. Tavolo PIC is charged with coordinating all activities in the field of CIP and CIIP. It also serves as an international contact point;

- To improve the protection of critical information infrastructure against cyber-threats, the Ministry of the Interior established the National Anti-Cybercrime Center for the Protection of Critical Infrastructures (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, CNAIPIC) in 2008.

### 2.1 Report on Critical Information Infrastructure Protection: The Case of Italy

The Working Group on Critical Information Infrastructure, established as part of the Prime Minister's Office in 2003 to address CIIP, released the report Protezione delle Infrastrutture Critiche Informatizzate—La Realtà Italiana (Critical Information Infrastructures Protection: The Case of Italy) [1] in March 2004, offering a synthesis of its efforts. The document describes many elements of the Italian infrastructure, emphasizes their interdependencies, and suggests CIIP policy strategies. In particular, the Working Group suggests that full responsibility for the correct implementation of a survivability policy should remain with the individual owners and operators of critical infrastructure, while the government should be responsible for the definition of an overall policy to minimize interdependencies and cascading failures.

### 2.2 Guidelines for the Protection of Critical Information Infrastructures

The Institute for Information and Communication Technologies (ISCOM) of the Ministry for Communication has published several guidelines with regard to the security of ICT and the protection of critical information infrastructures. The guidelines are elaborated in close collaboration with various private organizations, most notably with the owners and operators of critical infrastructures. The following two guidelines directly address the security of information in critical infrastructures:

- The guideline The Network Security in Critical Infrastructures [2] highlights the importance of information infrastructures in Italy and identifies and analyzes the vulnerabilities and interdependencies of critical information infrastructures. The document also proposes best practices for the protection of critical infrastructures (e.g., certification of secure services), as well as organizational measures such as the creation of a crisis management group where stakeholders of all the critical infrastructures can be represented.
- The guideline Network Security: from Risk Analysis to Protection Strategies [3] describes the features of the information and communication network and its importance for contemporary society. In particular, the document addresses the topic of risk analysis and risk management with regard to ICT.

Other documents issued by the Ministry of Communication also deal with information security and risk analysis. They encompass analyses on the quality of communication

[1]Interministerial Coordination Platform and Contact Point for the Sector of Critical Infrastructure Protection.

networks; analyses on outsourcing in the field of information security; guidelines for local crisis management; and studies on the certification of secure ICT.[2]

## 3 ORGANIZATIONAL OVERVIEW

The main Italian government bodies dealing with CIIP are the Ministry of the Interior (Postal and Communications Police) and the Ministry of Innovation and Technologies. The Ministry of Communication is also involved in various activities to improve the security of information and communication networks.

In order to improve CIIP at all levels, the public agencies also collaborate closely with the private sector. The most important Public-Private Partnership in the field of CIP is the Association of Italian Experts for Critical Infrastructures (Associazione Italiana Esperti in Infrastrutture Critiche, AIIC) [5], an expert group of practitioners from both the public and the private sectors.

### 3.1 Public Agencies

***3.1.1 Ministry of Communication.*** The Ministry of Communication supervises postal and telecommunications services, acting as a regulator as well as implementing a policy of coordination, supervision, and control [6]. It is involved in the definition of security policies for communication. In 2004, ISCOM established a working group to analyze the different aspects of security in communication networks and the security requirements required in communication networks to guarantee an adequate level of services for critical infrastructures. The working group ended its activities in 2006.[3]

***3.1.2 Permanent Working Group on Network Security and Communications Protection.*** The Ministries of Communication, the Interior, and Justice established the Permanent Working Group on Network Security and Communications Protection in 1998 with a focus on criminal, legal, and economical aspects of communication services, such as the duration for which a provider should store communication data. Within this group, the Internet Subgroup deals with investigative and judicial matters related to the internet.

***3.1.3 Postal and Communications Police.*** In 1992, the Ministry of the Interior issued a directive assigning to the state police specific responsibilities for IT and telecommunications security that are in fact carried out by the Postal and Communications Police. The Postal and Communications Police is a flexible organization with a staff of around 2,000 highly trained officers, and placed at the peak of a structure involving 19 regional departments and 76 territorial sections. The Postal and Communications Police reviews communications regulations, studies new technical investigative strategies to fight computer crime, and coordinates operations and investigations for other offices. This police force also collaborates with other institutions—in particular, with the Ministry of Communication and the Privacy Authority—and with private operators who deal with communications. As the Italian contact point for the G8's computer crime offices,

[2]For an overview on the documents issued by ISCOM, see: [4].
[3]Information provided by an expert.

it is available at all times. This particular organizational aspect guarantees a quick, qualified, and efficient response [7] in the event of a threat or computer attack originating nationally or internationally.

The Postal and Communication Police Service also hosts and manages an emergency center at both the national and regional levels, in order better to deal with computer crimes against critical infrastructure and to conduct preventive monitoring activities on a technical and operational level. The center serves as a focal point for the evaluation of threats, thus providing adequate countermeasures to face such situations.

Article 7 bis of the Law n.155/2005 assigns the task of protecting national information infrastructures against cyber-crime attacks to the Postal and Communication Police Service. In order to perform this task, the aforementioned Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) was established as a special unit of the Postal and Communication Police Service.[4]

***3.1.4 Ministry for Innovation and Technologies (MIT).*** The Ministry for Innovation and Technologies [8] has been delegated to act on behalf of the prime minister in the areas of technological innovation, the development of the Information Society, and related innovations for government, citizens, and businesses. This ministry has particular responsibility for network structures, technologies, and services, the development and use of information and communication technologies, and the fostering of IT and digital awareness and literacy, including through links with international and EU bodies that are active in the sector. The MIT has also been delegated to chair the Committee of Ministers for the Information Society and the Committee of Ministers for Joint Satellite Navigation Initiatives.

The Department for Innovation and Technologies (DIT) is the department of the Presidency of the Council of Ministers that provides support to the minister of innovation and technologies. It serves to coordinate ministerial policies for the development of the Information Society and to promote innovation in public offices and among citizens and businesses [8].

***3.1.5 National Technical Committee for ICT Security in the Public Administration.*** On 16 October 2002, the Ministry for Innovation and Technologies and the Ministry of Communication created the National Technical Committee for ICT Security in the Public Administration. The establishment of this new committee followed from the Directive on ICT Security for the Public Administration, which enacts EU recommendations with the important initial aim of achieving compliance with a set of minimum security standards. The Technical Committee can therefore be seen as the operative arm of the new national IT security policy [8]. It was constituted in July 2002 with support from the Ministry for Innovation and Technologies and the Ministry for Communications [9].

The committee aims to attain a satisfactory security level in information systems and digital communications, in compliance with international standards, in order to guarantee the integrity and reliability of the information. It prepares strategy proposals concerning computer and telecommunications security for the public administration. In particular, it develops:

[4]Information provided by an Italian expert.

- The National Emergency Plan for the Security of Information and Communication Technologies in the Public Administration. The committee annually verifies its state of progress, and proposes corrective measures if required;
- The ICT security national organizational model for the public administration. The committee monitors its level of activation and application.

Furthermore, the committee formulates proposals for regulating certification and security assessment, as well as certification criteria and guidelines for ICT security certification in the public administration, on the basis of national, sectoral, and international norms of reference.

Finally, the committee elaborates guidelines for agreements with the Ministry of Public Administration for training public employees in ICT security. Among other proposals, the group is tasked with establishing the Computer Emergency Response Team (CERT) for the Public Central Administration (CERT-PA, now GovCERT.it, which has also assumed the role of coordinating the CERTs of the other parts of the public administration). It will have a central Early-Warning System operating around the clock.

In March 2004, the National Technical Committee on ICT Security published a preliminary proposal for the National Security Plan and an organizational model. Guidelines were suggested for building an organizational infrastructure to coordinate and support public offices at the national level, and the most urgent areas of action for putting the process on track were identified [8].

***3.1.6 National Center for Informatics in the Public Administration (CNIPA).*** The Authority for IT in the Public Administration (AIPA), founded in 1993, was transformed into the National Center for Informatics in the Public Administration (CNIPA) in 2003 [10]. CNIPA is supervised by the Ministry of Innovation and Technologies, and its head is nominated by the Council of Ministries. It addresses central and local administrations, especially the elements responsible for IT systems in the public administration. The main task of CNIPA is to promote modern information technologies in the Italian public administration, to establish standards and methods, to deal with security issues, and to make recommendations and technical regulations in the field of IT for public administration [10]. CNIPA published a comprehensive guide on the protection of personal data in 2001.

## 3.2 Public-Private Partnerships

***3.2.1 Association of Italian Experts for Critical Infrastructures (AIIC).*** The Association of Italian Experts for Critical Infrastructures [5] is a not-for-profit-organization that aims "to support an interdisciplinary and inter-sectoral culture for the development of strategies, methodologies, and technologies supporting the correct management of Critical Infrastructure during periods of crisis, in case of exceptional events, and during terrorist attacks or natural disasters" [11]. The AIIC comprises public as well as private members.

In order to raise awareness of information security and critical infrastructure protection, the association publishes periodical newsletters on national and international developments in the field of CIIP and provides information on strategies and policies as well as on recent scientific findings on its website.

## 4 EARLY WARNING AND PUBLIC OUTREACH

A variety of Computer Emergency Response Teams (CERTs) is currently active in Italy. They are all devoted to the development of IT security and to supporting organizations in increasing their level of security with respect to cyber-threats.

- *CERT-IT.* The Italian Computer Emergency Response Team was founded in 1994 as a non-profit organization. It is mainly supported by the Department of Informatics and Communications (DICO) at the University of Milan [12]. CERT-IT is a member of the Forum of Incident Response and Security Teams (FIRST). It promotes research and development activities in security systems, provides information about computer security, and has an expert team for handling computer incidents [13];
- *GovCERT.it.* [14] This initiative was planned by the National Technical Committee on Computer and Telecommunications Security to help public administrations to improve their level of ICT security by providing an early-warning service on cyber-threats;
- *GARR-CERT.* [15] The GARR Network Computer Emergency Response Team assists the users of the GARR Network (Gestione Ampliamento Rete Ricerca—the Italian Academic and Research Network) in implementing proactive measures to reduce the risk of computer security incidents and in responding to such incidents when they occur;
- *CERT Difesa.* [16] The CERT of the Ministry of Defense assists its users in protecting ICT networks and disseminates information about ICT security.

The Ministry of the Interior, together with the Postal and Communication Police, is also active in early-warning activities. These agencies continuously monitor cyberspace to discover criminal or malicious behavior in order to provide adequate countermeasures. Moreover, specific protocols have been established to prevent incidents and to manage and share information as well as criminal evidence.

## 5 LAW AND LEGISLATION

Italy has specific laws and ministerial decrees devoted to CIP and CIIP. In the early 1990s, a new law related to computer crimes was introduced (Law 547 of 23 December 1993) that gave more power to investigators in the evidence-collection phase and allowed computer and telecommunication intercepts. Italy was one of the first European countries to adopt such legislation, mainly due to the incidence of new crimes in the areas of computer fraud, forgery, data corruption, computer misuse, unauthorized interceptions of computer communications, and sabotage. The great attention given to such crimes is underscored by the fact that computer intrusions are treated as domestic property violations.

The innovative concept of High-Tech Crime, which had already enjoyed currency in the Italian penal legislation for different types of offenses, was introduced with Law 547. According to Article 420 of the Italian Penal Code (attempt to damage public utilities systems), actual damage or destruction to the systems are not required for such activities to constitute an offense; the mere intention suffices. Such cases will be prosecuted even if the attempt was unsuccessful.

Other relevant laws include:

- Legislative Decree 518, enacted on 29 December 1992 and modified by Law 248 (18 August 2000), a legislative decree against illicit ICT piracy;
- Law 547, enacted on 23 December 1993, a comprehensive and integrated law against ICT crimes;
- Law 675, enacted on 31 December 1996, a law governing personal data protection, integrated by subsequent legislation (DPR 318/1999, Law 325/2000, Legislative Decree 467/2001, and Legislative Decree 196/2003);
- Legislative Decree 374/2001, changed into Law 438/2001, a law devoted to improving law-enforcement instruments and to combating terrorism. Law 374/2001 was transformed into Law 438/2001 after 11 September 2001, so that now, crimes committed in Italy are liable to prosecution even if they are directed against a foreign state or against a multilateral institution.
- Article 7 bis of Law 155/2005 defines the authority of the Postal and Communication Police Service to carry out undercover investigations and preemptive interceptions both for the protection of critical infrastructures and for countering terrorist acts committed by means of new technologies.

### 5.1 Privacy Law

Part of Article 15 of Law 675/96 [17] (the Privacy Law) deals with the organizational issues that the use of IT systems raises. By establishing a duty to store data in a way that minimizes the risk of loss and prevents unauthorized access (including access inconsistent with the reasons given for the original acquisition and processing of such data), Article 15 requires data holders to update their security to keep up with technical advances and changes in the methods of infiltration.

Consequently, not only should the minimum measures established by Presidential Decree 318/99 be strictly implemented and observed, but all appropriate additional measures should also be taken and regularly updated to match technical progress.

A New Privacy Code, which contains specific requirements for the protection of personal data online, has been in force since July 2003 [18].

### 5.2 Italian Penal Code

Penal Code Article 615 ter: Unauthorized Access to Computers or Telecommunication Systems: Any person who enters a computer or telecommunication system protected by security measures without authorization, or remains in it against the expressed or implied will of the authority that has the right to exclude them, shall be sentenced to imprisonment not exceeding three years.

The imprisonment is from one until five years:

1. if the crime is committed by a public official or by an officer of a public service, through abuse of power or in violation of the duties concerning the function or the service, or by a person who practices—even without a license—the profession of a private investigator, or by abusing the authority of a system operator;
2. if, in order to commit the crime, the culprits use violence against assets or people or if they are manifestly armed;

3. if the deed causes the destruction or damage of the system or the partial or total interruption of its operability, or the destruction or damage of the data, information, or programs contained in it.

If the crimes listed in the first and second paragraphs concern computer or telecommunication systems of military importance, or of importance to public order or public security, or civil defense, or any public interest whatsoever, the penalty is one to five years and three to eight years of imprisonment, respectively. In the case provided for in the first paragraph, the crime is only liable to prosecution after an action by the plaintiff; the other cases are prosecuted ex officio.

Penal Code Article 615 quater: Illegal Possession and Diffusion of Access Codes to Computer or Telecommunication Systems:

Whoever, in order to obtain a profit for themselves or for another or to cause damage to others, illegally gets hold of, reproduces, propagates, transmits, or delivers codes, key-words, or other means for accessing a computer or telecommunication system protected by safety measures, or whoever provides information or instructions for the above purpose, will be punished by imprisonment not exceeding one year and a fine.

Penal Code Article 615 quinquies: Diffusion of Programs Intended to Damage or to Disrupt a Computer System:

Whoever propagates, transmits, or delivers a computer program—written by themselves or by another party—with the aim and the effect of damaging a computer or telecommunication system, the data or the programs contained therein or pertinent to it, or achieving the partial or total interruption or an alteration in its working, will be punished by imprisonment not exceeding two years and a fine [19].

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Roberto Setola of Università Campus Bio-Medico and Tommaso Palumbo of the Postal and Communication Police, who validated the content of this chapter.

## REFERENCES

1. Working Group for the Protection of Critical Infomration Infrastructure Protection (2004). *Protezione delle Infrastrutture Critiche Informatizzate—La realtà Italiana*, March.
2. http://www.isticom.it/documenti/news/pub_003_eng.pdf, 2008.
3. http://www.isticom.it/documenti/news/pub_002_eng.pdf, 2008.
4. http://www.isticom.it/index.php?option=com_frontpage&Itemid=1, 2008.
5. http://www.infrastrutturecritiche.it, 2008.
6. http://www.comunicazioni.it/english_version, 2008.
7. http://www.poliziadistato.it/pds/english/specialist.htm, 2008.
8. http://www.innovazione.gov.it, 2008.
9. Minister for Innovation and Technologies (2002). *Government Guidelines for the Development of the Information Society*, (13 February). http://www.innovazione.gov.it/eng/intervento/allegati/docu_base130202.pdf.
10. http://www.cnipa.gov.it, 2008.

11. http://www.infrastrutturecritiche.it/jml/index.php?option=com_frontpage&Itemid=1, 2008.
12. http://security.dsi.unimi.it, 2008.
13. http://idea.sec.dsi.unimi.it/activities.en.html, 2008.
14. http://www.cnipa.gov.it/site/it-it/Attivit%C3%A0/Servizi_per_la_PA/Govcert.it/, 2008.
15. http://www.cert.garr.it/index-en.html, 2008.
16. http://www.difesa.it/SMD/Staff/Reparti/II-reparto/CERT/default.htm, 2008.
17. http://www.innovazione.gov.it/ita/privacy/legge675_96.rtf, 2008.
18. http://www.innovazione.gov.it/eng/egovernment/infrastrutture/sicurezza_privacy.shtml, 2008.
19. http://www.cybercrimelaw.net/laws/countries/italy.html, 2008.

# JAPAN

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

The critical infrastructures of Japan are defined in the Action Plan on Information Security Measures for Critical Infrastructures that was issued by the Information Security Policy Council in 2005: "Critical infrastructures are formed by business entities providing highly irreplaceable services and are essential for people's social lives and economic activities. If an infrastructure's function is suspended, reduced or unavailable, people's social lives and economic activities will be greatly disrupted" [1]. The paper lists the following ten sectors that are deemed to be critical:

- (Tele-) Communication,
- Government and Administrative Services,
- Finance,
- Civil Aviation,

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- Railways,
- Logistics,
- Electricity,
- Gas,
- Medical Services,
- Water.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

The government of Japan, based on the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society of 1998,[1] has been steadily promoting policies contributing to the advancement of information technology and telecommunications in Japan [2].

The Comprehensive Strategy on Information Security, released in 2003 by the Ministry of Economy, Trade, and Industry (METI) was the next step of the policy development process. In this document, ICT-related risks and threats confronting the Japanese society were explicitly considered from a national-security perspective [3].

In 2005, the First National Strategy on Information Security was issued. This is now the most important policy paper and provides the basis for all other guidelines and action plans related to CIIP and information security [4].

### 2.1 The First National Strategy on Information Security

In October 2003, the Information Security Committee of the METI published the Comprehensive Strategy on Information Security [5]. This document was the starting point for the development of a national strategy on information security, because it highlighted the need for a comprehensive approach to bring about and improve a highly reliable Information Society in Japan. Most importantly, the Comprehensive Strategy called for a clear definition of responsibilities within the government and promoted the development of a dedicated organization for information security within the Cabinet Secretariat.

In 2005, the propositions of the Comprehensive Strategy were implemented. A council and an organization were established within the Cabinet Secretariat (the Information Security Policy Council (ISPC) and the National Information Security Center (NISC)), and a new national strategy was elaborated. This strategy, called The First National Strategy on Information Security—Towards the Realization of a Trustworthy Society [6], is a mid- and long-term strategy formulating clear goals for the years 2006–2008. The Information Security Policy Council issued separate implementation plans for each of these three years [7].

In general, the strategy aims to make Japan an advanced nation in the field of information security. Most importantly, the strategy aims to establish a new public-private partnership model to improve information security. Thus, the strategy defines the roles of government, critical infrastructures, businesses, and individuals, and the measures that need to be implemented by these actors:

[1]Decision of the Advanced Information and Telecommunications Society Promotion Headquarters (9 November 1998).

- Central and local governments are required to define best practices for information security and implement these practices in their agencies. By defining and implementing standards for information security, the government shall increase the overall ability to respond to emergencies, including cyber-attacks;
- Critical infrastructures must ensure stable provision of their services. The major step to prevent disruptions of critical infrastructures is the development of so-called Capabilities for Engineering of Protection, Technical Operations, Analyses, and Response (CEPTOAR; for more detail, see the chapter on Organizational Overview) for each major sector. The Action Plan on Information Security Measures for Critical Infrastructures defines the strategy for critical infrastructures in more detail;
- Businesses need to implement information security standards and measures that are promoted by government agencies. Security audits and third-party evaluation systems shall be promoted;
- Individuals: the government aims to raise awareness of information security among users of IT services by improving information security education and by promoting user-friendly services.

The second version of the Comprehensive Strategy is being discussed as of March 2008.[2]

### 2.2 Action Plan on Information Security Measures for Critical Infrastructures

In 2000, the Cabinet Secretariat released a Special Action Plan on Countermeasures to Cyber-Terrorism of Critical Infrastructure [8], which was replaced in December 2005 by the Action Plan on Security Measures for Critical Infrastructures [9], published by the ISPC as an amendment of The First National Strategy on Information Security.

The new plan includes definitions of critical infrastructure elements and threats, safety standards for information security, information-sharing systems in public-private partnerships (PPP), interdependency analyses, and exercises. In particular, the plan emphasizes the importance of PPPs. The plan therefore aims to establish within each critical sector so-called Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response (CEPTOAR, see the chapter on Organizational Overview).

In addition, the Action Plan provides for analyses of interdependencies and cross-sectoral status assessments of the critical infrastructures. For this purpose, various cross-sectoral exercises are projected. Such exercises shall be implemented in every fiscal year, based on concrete threat scenarios corresponding to the assumed threats.

### 2.3 Standards for Information Security Measures for the Central Government Computer Systems

In order to achieve a sector plan for improving the information security level of the whole government, the ISPC has issued the Standards for Information Security Measures for the Central Government Computer Systems. The standards formulated by the ISPC represent the nominal level of information security in government agencies. The NISC inspects and evaluates the actual levels and compares them with the standards. In that way, it is possible to formulate recommendations for each government agency [10].

[2]Information provided by an expert.

## 3 ORGANIZATIONAL OVERVIEW

Within the Japanese government, the Cabinet Secretariat is the main actor in the field of CIIP and information security in general. In 2005, the ISPC and the NISC were established within the Cabinet Secretariat. These two organizations are now the focus of CIIP policies in Japan.

In addition, the METI, the National Police Agency (NPA), and the Ministry of Internal Affairs and Communications (MIC) assist the Cabinet Secretariat and play major roles in the field of CIIP.

As a private-public partnership initiative, the so-called CEPTOAR (Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response) are designed to serve the purpose of information-sharing between government and the private sector.

### 3.1 Public Agencies

***3.1.1 Cabinet Secretariat and IT Strategic Headquarters.*** The IT Strategic Headquarters, which includes all ministers and private-sector experts, was established in July 2000 within the cabinet in order to promote comprehensive measures for making Japan an internationally competitive IT nation. At the same time, the IT Strategy Council, consisting of 20 opinion leaders, was established in order to study the issue strategically and by combining private-public partnerships [11]. In January 2001, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) was launched under the provisions of the Basic Law on the Formation of an Advanced Information and Telecommunications Network Society (IT Basic Law), with the prime minister as its director-general, and including all cabinet members and opinion leaders from the private sector as members, to serve as a new base for joint government and private-sector promotion of IT policies [12].

***3.1.2 Information Security Policy Council (ISPC).*** The ISPC, set up in May 2005, is chaired by the chief cabinet secretary and forms part of the IT Strategic Headquarters with members from various ministries as well as private-sector experts. It plays a central role in developing and reviewing the information security strategies and policies. Thus, the ISPC has the following tasks:

- To develop and review strategies with regard to information security;
- To undertake proactive and retrospective assessments of information security policy, based on the basic strategy;
- To develop safety guidelines for information security that are uniform throughout government;
- To recommend information security policies based on the government-wide safety guidelines.

***3.1.3 The National Information Security Center (NISC).*** The NISC was launched in April 2005 as Japan's central implementing body for IT security issues. It collaborates closely with the ISPC and pursues the following tasks:

- Planning government-wide fundamental strategies for information security policy;
- Promoting comprehensive measures on information security concerning government organizations;
- Supporting these government organizations in an appropriate way when information security incidents occur;
- Strengthening the information security of critical infrastructures;
- Reinforcing information-sharing systems;
- Implementing cross-sector cyberspace exercises;
- Creating an international strategy and promoting relationships with other countries.

***3.1.4 Ministry of Economy, Trade and Industry (METI).*** The METI is responsible for planning and implementing various information policies under the guidance of the IT Strategic Headquarters. In particular, METI deals with e-commerce, e-government, data protection, and research and development related to IT [13]. In order to enhance the IT industry competitiveness in Japan, METI promotes policies that improve information security in companies.

***3.1.5 National Police Agency (NPA).*** The NPA [14] has long been committed to maintaining computer and network security and investigating cyber-crimes. Traditionally, it has done this via its High-Tech Crime Prevention Department. In 1999, a new program was established to help fight high-tech crime. The High-Tech Crime Technology Division (HTCTD) was set up in the Information-Communications Bureau, and a National Police Agency Technology Center was created as the technical heart of the division. In April of 2004, the National Police Agency established the HTCTD in each Prefectural Information-Communications Department in order to enhance the capacity for technological support [15].

Additionally, the National Police Agency is committed to creating a monitoring and emergency response service to prevent and minimize the spread of large scale cyber-related incidents, as well as to arrest so-called cyber-terrorists. One branch of this service consists of mobile technical teams, or Cyber Forces. These technical computer-security teams are stationed throughout Japan, and the Cyber Force Center acts as their command center. It monitors internet security around the clock and collects and analyzes relevant information. It is also equipped with facilities for a wide range of research and development, as well as for personnel education and training.

***3.1.6 Ministry of Internal Affairs and Communications (MIC).*** The MIC [16] is responsible for creating the fundamental national infrastructure of Japan, including information and communications. In order to realize “secure and safe” communications as a social infrastructure, MIC promotes various policies that reinforce information security in the three categories of “Network”, “Terminal System and Equipment”, and “Person”.

The MIC publishes an annual White Paper on Information and Communications in Japan [17]. In each edition, a special chapter deals with privacy protection as well as information security. The aim is to strengthen public-private partnership cooperation to ensure information security. Moreover, the MIC conducts research related to fundamental technologies related to measures against cyber-attacks and other network security issues

and to the protection of personal information in the field of ICT, and carries out measures to upgrade emergency information functions in the telecommunications area.

The 2007 White Paper deals with ways to achieve a ubiquitous network society (u-Japan) by 2010 that allows connection to networks anytime, anywhere, by anyone, and enables an easy exchange of information. The MIC outlined the future of such a society and summarized the necessary policies as the u-Japan Policy, which is based on the four principles "ubiquitous", "universal", "user-oriented", and "unique". Among these, "ubiquitous" (connects everyone and everything) plays the key role [18].

### 3.2 Public-Private Partnerships

***3.2.1 Capabilities for Engineering of Protection, Technical Operation, Analysis, and Response (CEPTOAR).*** Public-private partnerships are an important part of CIIP policies in Japan. The Comprehensive Strategy on Information Security of 2003 already contained suggestions for cooperation between the national government and private enterprises [19]. The First National Strategy on Information Security and the Action Plan on Security Measures for Critical Infrastructures substantiated this requirement. They formulate the need for implementation of CEPTOAR within each critical infrastructure sector.

The latter serve the purpose of information-sharing between the government and the private sector. The CEPTOAR receive information from the Cabinet Secretariat (via the presiding ministries and agencies) and provide this information to their corporate members that operate critical infrastructures [9].

In order to enable information sharing between government agencies and private companies, the NIPC issued a "traffic light" protocol for information sharing: information can be classified as red (not to be disseminated), amber (need-to-know restriction), green (can be shared among all persons concerned), or white (can be made public) [20].

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 National Incident Response Team (NIRT)

The National Incident Response Team (NIRT) has been part of the IT Security Office of the Cabinet Secretariat since April 2002 [21], and is in charge of the first response to cyber-incidents as the Japanese government CERT. Based on the Action Plan for Ensuring e-Government's IT Security (adopted on 10 October 2001 by the IT Security Promotion Committee), NIRT comprises 17 computer security experts from both the government and the private sector and has the following tasks [22]:

- To understand incidents correctly: To collect and analyze the related information or intelligence and make forecasts on possible future damage;
- To develop technical countermeasures for mitigation and recovery, and to prevent reoccurrence: To analyze countermeasures and to organize concrete remedies to be implemented by the ministries and agencies;
- To assist in response: To provide help-desk service for ministries and agencies, as well as response support when required;
- To collect and analyze information or intelligence in order to make predictions and provide effective incident response;

- To supply expertise, knowledge, and information to government organizations;
- To improve the necessary expertise.

### 4.2 Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

JPCERT/CC [23] is an independent non-profit organization acting as a national point of contact for the other Computer Security Incident Response Teams (CSIRTs) in Japan. Since its establishment in 1992, the center has been gathering information on computer incidents and vulnerabilities, issuing security alerts and advisories, and providing incident responses as well as education and training to raise awareness of security issues. JPCERT/CC coordinates with network service providers, security vendors, government agencies, and industry associations, and is a member of the Forum of Incident Response and Security Teams (FIRST; see the survey on FIRST in this volume).

### 4.3 Asia Pacific Computer Incident (Emergency) Response Team (AP-CIRT/APCERT)

The aim of the Asia Pacific Security Incident Response Coordination (AP-CIRT) is to foster close collaborations among the CIRTs (Computer Incident Response Teams) in the region.[3] In February 2003, its name was changed to Asia Pacific Computer Emergency Response Team (APCERT), and it continues to carry out its mission, which is to maintain a trusted contact network of computer security experts to improve the region's awareness and competency in relation to computer security incidents [25].

### 4.4 Telecom Information Sharing and Analysis Center Japan (Telecom-ISAC Japan)

Telecom-ISAC Japan [26] is an independent organization established as Japan's first ISAC (Information Sharing and Analysis Center) in July 2002. Telecom-ISAC Japan works to improve information security by various means such as collecting, analyzing, and sharing incident information, providing timely countermeasures and best practices, and coordinating/collaborating with related organizations, based on mutual cooperation between a wide variety of members in the information and telecommunications industry, such as ISPs, carriers, and manufacturers.

### 4.5 Cyber Force

The Cyber Force, a section within the police, gathers data on the internet around the clock and looks for evidence of cyber-crime. When the Cyber Force detects an unusual phenomenon, it provides critical infrastructure operators with security information to prevent cyber-terrorism and conducts vulnerability tests. Additionally, the Cyber Force will give operators of critical infrastructures advice on how to limit the damage from such an incident and how to recover their services safely, and to find the cause of the incident [27].

[3] See the membership list: [24].

### 4.6 @police

The National Police Agency has a security portal site, @police, whose purpose is to prevent large-scale cyber-related incidents or keep them from spreading by quickly providing information gathered by the police on information security. Moreover, @police makes efforts to increase security awareness among internet users. Therefore, it provides a wealth of diverse content in order to help as many people as possible improve their security. Special online security courses, examples of internet crimes and how to avoid them, quick security checks, and information on security holes are provided for the benefit of private PC users as well as server administrators [28].

### 4.7 Ministry of Economy, Trade and Industry (METI)

METI has responded to security breaches in cooperation with JPCERT/CC and the Information Technology Promotion Agency (IPA) since 1990. Around that time, it also began releasing reports on computer viruses and unauthorized access and started to gather information about damage caused by computer viruses and disseminating it to the public immediately after the incident [29].

## 5 LAW AND LEGISLATION

### 5.1 Unauthorized Computer Access Law 1999

The Unauthorized Computer Access Law No. 128 of 1999 prohibits acts of unauthorized computer access (Article 3) as well as acts that facilitate unauthorized computer access (Article 4).

Article 3 covers acts such as:

- Facilitating a specific use that is restricted by an access control function, by entering via a telecommunications line another person's identification code into a specific computer that controls access;[4]
- Facilitating a specific use that is restricted by an access control function, by entering via a telecommunications line any information (excluding an identification code) or command that can evade the restrictions of that access control function for that specific purpose;
- Facilitating a specific use that is restricted by an access control function, by operating a computer whose specific use is restricted by an access control function installed on another specific computer that is connected, via a telecommunication line, to that specific computer, by entering via a telecommunications line any information or command that can evade the restriction concerned.

Article 4 makes it illegal to provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function, or to the authorized user for that identification code, while indicating

[4]To exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code.

that it is the identification code for a specific computer's specific use, except where such acts are conducted by the access administrator, or with the approval of that access administrator or of the authorized user.

Moreover, the Japanese Penal Code, Article 258, makes it illegal to damage documents or electronic-magnetic records in public or private use [30].

### 5.2 Act on Electronic Signatures and Certification Business 2000

The Act on Electronic Signatures and Certification Business No. 102 of 2000 aims to promote the distribution of information by electromagnetic forms and information processing by ensuring easy use of electronic signatures, and thereby to contribute to the improvement of citizens' quality of life and the sound development of the national economy, by providing the presumption of authentic establishment of electromagnetic records, the accreditation system for designated certification businesses and other necessary matters, with respect to electronic signatures [31].

### 5.3 Basic Law on Formation of an Advanced Information and Telecommunication Network Society 2001

The purpose of the IT Basic Law, which entered into force on 6 January 2001, is to promote measures for forming an advanced information and telecommunications network society where citizens can enjoy the benefits of ICT. Its measures include (Articles 16–24) the formation and expansion of advanced ICT networks; the promotion of fair competition; increasing IT user skills and development of expert human resources; reform of regulations and facilitation of e-commerce through appropriate protection; promotion of e-government and digitalization of administration; assuring security and reliability for networks and the protection of personal data; promotion of creative research and development; and international cooperation [32].

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Mika Shimizu of East-West Centre, Tomoko Makino and Tohru Nakao of the Ministry of Internal Affairs and Communications, and Yoshihiro Sato and Toshihiko Suguri of the National Information Security Center, who validated the content of this chapter.

## REFERENCES

1. Information Security Policy Council *Action Plan on Information Security Measures for Critical Infrastructures*, p. 2. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf, 2008.
2. *Outline of the First Follow-up of the Action Plan of the Basic Guidelines Toward the Promotion of an Advanced Information and Telecommunications Society* (19 May 2000). http://www.kantei.go.jp/foreign/it/2000/0706outline.html.
3. Ministry of Economy, Trade and Industry. New Dimensions of Risks Confronting Society as a Whole. In *Comprehensive Strategy on Information Security: Executive Summary*, Chapter 1.2. (no date). http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf, 2008.

4. *Japanese Government's Efforts to Address Information Security Issues*, http://www.nisc.go.jp/eng/pdf/overview_eng.pdf, 2008.
5. http://www.meti.go.jp/policy/netsecurity/downloadfiles/strategy_summary_English.pdf, 2008.
6. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf, 2008.
7. (a) *Secure Japan 2006: First Step Towards a Trustworthy Society*, (2006). http://www.nisc.go.jp/eng/pdf/sj2006_eng.pdf; (b) *Secure Japan 2007: upgrading of information security measures in order to create an environment in which people can use IT safely and securely*, (2007). http://www.nisc.go.jp/eng/pdf/sj2007_eng.pdf.
8. *Special Action Plan on Countermeasures to Cyber-terrorism of critical infrastructure*, (15 December 2000). provisional translation. http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN009986.pdf; (b) *Special Action Plan on Countermeasures to Cyber-Terrorism of Critical Infrastructure*, (2001). Summary, provisional translation. http://www.kantei.go.jp/foreign/it/security/2001/cyber_terror_sum.html.
9. http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf, 2008.
10. National Information Security Center (NISC) Standards for Information Security Measures for the Central Government Computer Systems. In *Japanese Government's Efforts to Address Information Security Issues–Focusing on the Cabinet Secretariat's Efforts*, Chapter 3.1. http://www.nisc.go.jp/eng/pdf/overview_eng.pdf, p. 23ff, 2008.
11. E-Japan Priority Policy Program http://www.kantei.go.jp/foreign/it/network/priority-all/1.html, 2008.
12. *Basic Law on the Formation of an Advanced Information Telecommunication Network Society*, http://www.kantei.go.jp/foreign/it/network/0626_e.html, 2008.
13. http://www.meti.go.jp/english/policy/index_information_policy.html, 2008.
14. http://www.cyberpolice.go.jp/english/action01_e.html, 2008.
15. http://www.npa.go.jp/english/kokusai/pdf/Poj2007-52.pdf, 2008.
16. http://www.soumu.go.jp/english/index.html, 2008.
17. http://www.soumu.go.jp/joho_tsusin/eng/whitepaper.html, 2008.
18. Ministry of Internal Affairs and Communications, Information and Communications in Japan (2007). *2007 Report on the Current Status of Information and Communications*, http://www.johotsusintokei.soumu.go.jp/whitepaper/eng/WP2007/contents.pdf.
19. Comprehensive Strategy on Information Security (executive summary), op. cit. http://www.meti.go.jp/english/information/downloadfiles/cInfo031216e.pdf, 2008.
20. http://www.nisc.go.jp/eng/pdf/overview_eng.pdf, p. 51, 2008.
21. http://www.nisc.go.jp/en/sisaku/h1310action.html, 2008.
22. http://www.nisc.go.jp/en/shoukai/nirt, 2008.
23. http://www.jpcert.or.jp/english, 2008.
24. http://www.apcert.org/about/structure/members.html, 2008.
25. http://www.apcert.org/about/mission/index.html, 2008.
26. https://www.telecom-isac.jp/index.html. Information provided by an expert, 2008.
27. http://www.cyberpolice.go.jp/english/action02_e.html, 2008.
28. http://www.cyberpolice.go.jp/english, 2008.
29. Hayami, Y. *Realizing a World-Class Highly Reliable Society*, http://www.aavar.org/2004web/AVAR2004/Presentations/ps011.ppt, 2008.
30. http://www.cybercrimelaw.net/laws/countries/japan.html, 2008.
31. http://www.cas.go.jp/jp/seisaku/hourei/data/aescb.pdf, 2008.
32. http://www.kantei.go.jp/foreign/it/it_basiclaw/it_basiclaw.html, 2008.

# REPUBLIC OF KOREA*

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

The critical information and communication infrastructure plays a crucial role in providing public safety and stable services that are essential for everyday life. In Korea, the following sectors are counted among the critical infrastructures that are heavily dependent on information and telecommunication technologies.

- E-Government and National Government Administration,
- National security,
- Emergency/Disaster Recovery Services,
- National Defense,
- Media Service, e.g., Broadcasting Facilities,
- Financial Service,
- Gas and Energy, e.g., Power Plants,
- Transportation, e.g., Subways and Airports,
- Telecommunication [1].

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

Report on the status of the Critical Information Infrastructure (2001)
e-Korea Vision (2006)
Cyber Korea 21 (1999)
Mid- to Long-Term Roadmap for Information Protection (2005)
Basic Strategy for Ubiquitous Information Security (2006)

*The Country Survey of the Republic of Korea 2008 was reviewed by Heung Youl Youm, Professor at the Department of Information Security Engineering of Soonchunhyang University.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

### 2.1 Report on the Status of the Critical Information Infrastructure

In 2001, the Korean Information Security Agency (KISA) published a Report on the Status of the Critical Information Infrastructure. The scope of the research was:

- To provide technical consulting for critical information infrastructure management agencies to perform a risk assessment and establish safeguards;
- To evaluate the security and confidentiality of internet data centers;
- To assign information-security consultants for information infrastructure.

These efforts resulted in a model and guidelines for vulnerability analysis and assessment of critical information infrastructures, including a protection guide and protection measures; a vulnerability analysis and assessment model; a guide to risk computation; asset classification; threat classification; and vulnerability analysis. In addition, technical consulting was provided for the former Ministry of Information and Communication [2] now the Korea Communications Commission.

### 2.2 e-Korea Vision 2006

In April 2002, the Ministry of Information and Communication published its third master plan for Informatization Promotion for the years 2002–2006, called e-Korea Vision 2006 [3], in consultation with the Korean Informatization Promotion Committee [4]. It followed the first master plan of informatization promotion devised in 1996 and the second, called Cyber Korea 21, drawn up in 1999. e-Korea Vision focuses on "Ensuring Safety and Reliability of Cyberspace" to strengthen the security of the critical information infrastructures. Government policies relevant to the vision paper include the following:

- Identifying critical information infrastructures that are important for national security and the economy, systematic analysis of vulnerabilities and preparation for protective plans, and establishment of cooperation between the public and private sectors in order to prevent cyber-attacks and intensify response measures;
- Reinforcement of real-time warning systems to fight against hacking and viruses and strengthening international cooperation, because cyber-terrorism is intrinsically transnational;
- Developing information security technologies and training new information security experts to meet the changing needs of the information security environment;
- Strengthening cooperation between the government and the private sector for a sound and healthy cyberspace;
- Devising plans to establish information ethics that enable a secure cyberspace, and encouraging voluntary regulation of the private sector in terms of online information circulation.

With the designation of major information and communication facilities as critical to the national defense and the economy, the government plans to conduct a systematic analysis of their weaknesses and implement strong security measures to protect these facilities. The government has established an Information Sharing and Analysis Centre (ISAC) for each area of the government and the financial and information sectors. In addition, standards have been developed for information security technologies, together with an evaluation methodology for information security systems [5].

### 2.3 Basic Strategy for Ubiquitous Information Security

The downside of the information revolution is seen in the growing number of cyber-attacks on the internet, infringement of private information, and spam. According to a vision called u-Korea, based on the four principles "ubiquitous" (connects everyone and everything), "universal", "user-oriented", and "unique", the resulting damage would not be limited to individuals, but would affect the whole society and its economy, and even pose a threat to the life and property of its citizens. Therefore, a new framework of information protection is required that takes the new virtual ubiquitous environment into account.

In May 2005, the Ministry of Information and Communication issued a report on the Mid- to Long-Term Roadmap for Information Protection dealing with the security of high-technology infrastructures and the establishment of reliable systems for new IT services. In particular, the report presents a phased roadmap from 2005 to 2008 for the prevention of attacks on the internet, advanced response measures, reinforced protection of privacy, improvement of the legal system regarding information protection, and the training of a specialized force [6].

In December 2006, the Ministry of Information and Communication established the Basic Strategy for Ubiquitous Information Security. The strategy aims to strengthen the global competitiveness of Korean industries; improving the existing legal and regulatory system, and promoting research and development in the field of ICT. It defines four specific policy goals: [7][1]

- *Secure infrastructures.* developing a more efficient incident response system, minimizing threats, protecting critical infrastructures from cyber-attacks;
- *Privacy Protection of users.* privacy protection of location information, protection of biometric and healthcare information, protection of personal information and personally identifiable information;
- *Trusted IT services and devices.* developing authentication and ID management systems, developing techniques for making IT services secure, providing a base for secure electronic transactions;
- *Clean internet environment.* preventing the dissemination of illegal and harmful traffic on the internet, spreading a culture of security, raising users' awareness.

## 3 ORGANIZATIONAL OVERVIEW

In general, all governmental organizations and their subsidiary organizations are in charge of CIIP.

The National Cyber Security Center (NCSC) coordinates the efforts of these departments and agencies. In the field of cyber-crime investigation and prevention, the Internet Crime Investigation Center (ICIC) under the authority of the Supreme Public Prosecutors' Office plays a central role. The Electronics & Telecommunications Research Institute has the leadership in developing technology and providing support to protect critical information infrastructure. The Ministry of Public Administration and Security, the Korea Communications Commission (the former Ministry of Information and Communication), and the Korea Internet Security Center (KISC; KrCERT/CC) within the Korean

[1]Information provided by an expert.

Information Security Agency (KISA) are undertaking efforts to foster a culture of safe internet and telecommunication networks.

In addition, the structure of government organization was changed in February 2008. According to new regime plan, the Ministry of Information and Communication was abolished, and its functions in the area of information security were transferred to several ministries: the Ministry of Public Administration and Security, the Ministry of Knowledge and Economy, and the Korea Communication Commission. Therefore, the Ministry of Public Administration and Security, the Korea Communications Commission, and the Ministry of Knowledge and Economy have begun sharing CIIP-related responsibilities in Korea.

As a public-private partnership, the national Information Security Alliance (NISA) strives to improve information security by fostering information exchange between governmental agencies, enterprises, and research institutes. The Financial Information Security Alliance has members from banks and insurance companies and strives to implement international information protection policies. The Information Security Practice Alliance is an initiative fostering information protection activities in the private sector, and the Korea Information Security Industry Association (KISIA) is an exchange platform for the information security industry.

### 3.1 Public Agencies

***3.1.1 Ministry of Public Administration and Security (MOPAS).*** As a result of the government restructuring, the Ministry of Public Administration and Security (MOPAS), a government department that is responsible for electronic-government and public administration services, began to play a primary role in information security tasks including CIIP-related missions in March 2008. The informatization strategy office, which is part of MOPAS, is responsible for information security matters in the private sector. It pursues the following tasks:

- Establishing an information security policy for private sector;
- Ensuring the protection of users' privacy;
- Dealing with electronic authentication;
- Cultivating a sound internet culture for the public and private sectors [8].

***3.1.2 Korea Communications Commission (KCC).*** As a result of the government restructuring in February 2008, the Korea Communications Commission (KCC), a government department that is responsible for establishing the policy for communications and digital broadcasting, began to play a primary role in tasks of the network security in March 2008. It pursues the following tasks:

- Establishing a network security policy;
- Ensuring the protection of internet users' privacy [9].

***3.1.3 National Cyber Security Center (NCSC).*** The government established the National Cyber Security Center (NCSC) [10] in February 2004. It not only coordinates the efforts of the Korean governmental departments and agencies in charge of CIIP, but is also a platform that brings together the private, public, and military sectors to fight

cyber-threats. This is based on the understanding that cooperation among all sectors is crucial for the effective prevention of cyber-attacks as well as for the minimization of damage. The NCSC operates under the auspices of the National Intelligence Service (NIS) and is the central point of government for identifying, preventing, and responding to cyber-attacks and threats in Korea. NCSC performs the following tasks:

- Overall management of national cyber-security by working out plans and guidelines to improve national cyber-security systems, as well as providing support for strategic committee meetings;
- Publishing national cyber-security manuals, security guidelines, and analysis reports, and collecting, analyzing, and distributing information on cyber-threats;
- Detecting and responding to cyber-threats, issuing warnings and information on cyber-incidents, and developing cyber-security technology;
- Preventing the spread of cyber-attacks, providing support for recovery procedures, and establishing and managing pan-governmental working groups for prompt response measures;
- Promotion of cooperation among international and domestic IT security organizations;
- Education and public relations regarding cyber-security issues.

In addition, NCSC operates early-warning services (see the chapter on Early Warning and Public Outreach) [11].

***3.1.4 Internet Crime Investigation Center (ICIC).*** The Supreme Public Prosecutor's Office and the Seoul District Public Prosecutor's Office have established the Internet Crime Investigation Center (ICIC) [12] to deal more effectively with internet-related crimes. The ICIC monitors crime trends such as hacking, the spread of viruses, fraud in electronic commerce, and infringement of privacy. In doing so, it develops more effective response measures and new investigative methods to crack down on cyber-crimes. Moreover, to maximize its investigation capacity, it maintains close cooperation with international and domestic organizations. The ICIC is operated by a high-tech crime investigation team of the Central Investigation Department and performs the following tasks:

- Intensive and systematic monitoring of cyber-crime trends;
- Collecting reports on cyber-crimes;
- Developing effective investigation methods;
- Improving the legal system in the field of cyber-crime;
- Around-the clock monitoring system to respond to high-tech crime.

***3.1.5 Korea Information Security Agency (KISA).*** The Korea Information Security Agency (KISA) [13], affiliated with the Korea Communications Commission (the former Ministry of Information and Communication), was established in 1996 to create a safe, reliable information environment in Korea by reacting effectively to various acts of electronic infringement and intrusion. KISA is devoted to enhancing the security and reliability of electronic transactions by developing and supplying cryptographic algorithms. In addition, KISA has supported the development of information security in

Korea through evaluations of IT-security products, IT-security education, public awareness campaigns, information security policy, and research and standardization in support of the legislative framework. In January 1998, KISA became a member of the Forum of Incident Response and Security Teams (FIRST; for more information on FIRST, see the FIRST chapter in this volume).

KISA opened the Korea Certification Authority Central in 1999, and the Personal Information & Privacy Protection Center in 2000. In addition, the Korea Information Security Industry Support Center (KISIS) was established under KISA in 2001. The Korea Internet Security Center (KISC, KrCERT/CC) [14] was founded in 2003 (see the chapter on Early Warning and Public Outreach), the Korea Spam Response Center (KSRC) also in 2003, and the Korea IT Security Evaluation Center (KISEC) [15] began its work in 2004.

In accordance with the Information Infrastructure Protection Act and the Act on Promotion of Utilization of Information and Communication Network and Data Protection, which became effective as of July 2001, KISA acquired additional duties such as the analysis and evaluation of the vulnerabilities of the critical information infrastructure, and the certification of information security management systems.

KISA includes an Information Infrastructure Protection Division with a CIIP Planning Team, a Critical Infrastructure Security Management Team, and the Korea Certification Authority Central Team, providing:

- Vulnerability analysis and assessment, including technical consulting and vulnerability analysis for facilities designated as CII;
- Security technology service for CII, including technical consulting for CII management agencies to establish safeguards and help in computer system recovery;
- Certification for information security management systems, including certifying integrated information security management systems, as well as technical and physical safeguards [16].

***3.1.6 Electronics and Telecommunications Research Institute (ETRI).*** The Information Security Research Division, a part of the Electronics and Telecommunications Research Institute (ETRI) [17], is developing advanced technologies in the area of information security for the private sector in Korea and supporting rapid industrialization of those technologies to resolve impediments to the emergence of the Information Society such as malfunctions of the Broadband Convergence Network infrastructure, the exchange of unsound and harmful information, and leaking of personal information, all of which are obstacles to the creation of a knowledge-based society. It aims to establish leadership in information security technology in order to approach the ideal of a secure u-Korea (see the chapter on the Past and Present Initiatives and Policies). This division focuses on four major research areas: Network Security, Ubiquitous Security, Biosecurity, and Security Chipset Technology.

The National Security Research Institute (NSRI), an affiliated research institute of ETRI [18], is managed by the Ministry of Science and Technology [19]. NSRI contributes to the public welfare by developing technology for protecting critical information infrastructures and enables the government to exercise information sovereignty by providing national security technology and policies required to protect the country and public organizations from cyber-attacks. NSRI deals with: [20]

- Developing technology to deal with cyber-terror and cyber-attacks, and for evaluating information protection systems, as well as to ensure the reliability and viability of governmental and military critical information infrastructures;
- Raising awareness of CIIP and giving seminars;
- Analyzing weaknesses in the government, public, and military sectors;
- Supporting Korea's e-Government strategy for information protection;
- Demonstration projects in the area of information protection for governmental organizations.

***3.1.7 Information and Telecommunication Infrastructure Protection Committee.*** The Information and Telecommunication Infrastructure Protection Committee, which is chaired by the viceminister for State Affairs of the Prime Minister's Office [21] and whose members are appointed by the chiefs and chairpersons of central administrative organizations, reviews items related to critical information infrastructures. The chairperson of the Information and Telecommunication Infrastructure Protection Committee can set up the Joint Working Group for Security Incident Response in order to provide emergency measures, technological support, and recovery procedures in the case of a large-scale security incident [22]. This committee was established in accordance with Article 3 of the Critical Information Infrastructure Protection Act. However, the Ministry of Public Administration and Security in May 2008 announced plans to abolish this committee.

### 3.2 Public-Private Partnerships

***3.2.1 National Information Security Alliance (NISA).*** The National Information Security Alliance (NISA) was established in September 2002 to improve information security by facilitating information exchange, presenting policies, and concentrating pan-governmental efforts. The alliance consists of 22 major governmental organizations, such as the Ministry of National Defense, the Ministry of Public Administration and Security, and the Korea Communications Commission, as well as information security officials from 17 public enterprises, communication network providers, the Korea Information Security Industry Association, research institutes, and experts from industry and academia. One main aspect of NISA's work is the executive meeting of chairpersons of the National Information Security Alliance, the Public Enterprise Information Security Alliance, and the Industrial-Educational-Research Information Security Alliance as a way of improving cooperation, while guaranteeing the autonomy of each of these actors within the alliance [23].

***3.2.2 Financial Information Security Alliance.*** The Financial Information Security Alliance was established in October 2002 to protect financial information security systems from cyber-terror and hacking, and to implement changes in international information protection policies such as the Banking Industry Technology Secretariat (BITS). The alliance has 87 members (20 banks, 27 security corporations, 30 insurance companies, and ten non-bank financial institutions). The Financial Information Security Alliance develops information protection standards and policies for the financial sector, as well as assessments and certifications. It also performs research in the field of information security and provides education.[1]

***3.2.3 Information Security Practice Alliance.*** The Information Security Practice Alliance was set up in July 2002 as a way of voluntarily increasing information protection activities in the private sector, in cooperation with various security companies and associations and with the help of the KISA. KISA has introduced a variety of projects in order to promote information protection campaigns with voluntary efforts from the public.[1]

***3.2.4 Korea Information Security Industry Association (KISIA).*** The KISIA was established in July 1998 as a platform for nurturing the information security industry (KISA has more than 150 members). Moreover, KISIA became a corporation in 2004 in accordance with Section 2 of Article 59 of the Act on Telecommunication Network Usage Promotion and Information Protection. It proposes measures to improve the legal system relevant to information security, trains specialized forces in the field, does joint research on innovative technology, analyzes market trends to understand the status of information security industry and to make plans, solves IT problems of the industry, reflects the opinions of members on governmental policies, promptly shares information with related authorities through an integrated system, provides support for participating in information security seminars or expositions, and promotes joint research with governmental or other related organizations [24].

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 National Cyber Security Center (NCSC)

The National Cyber Security Center (NCSC) takes preventive measures against cyber-threats. It also analyzes collected information on IT security, traffic, and capacity, using the service networks of numerous organizations, including government high-speed networks. Moreover, NCSC issues color-coded cyber-threat warnings (“green”, “blue”, “yellow”, “orange”, and “red”). It also distributes various security guidelines and information on worms and viruses, security news, cyber-incidents, and security technology to the private, public, and military sectors.[2] Furthermore, if a cyber-incident takes place, NCSC staff is dispatched to the site to investigate its cause and swiftly restore the system. The NCSC staff also examines the security of systems to prevent similar incidents in advance. Besides, the security center has organized a response team alliance dealing with national cyber-attacks, and is installing an emergency contact system for affected organizations [26].

### 4.2 Korea Internet Security Center (KISC, KrCERT/CC)

The Korean Internet Security Center (KISC, also called the Korea Computer Emergency Response Team Coordination Center, or KrCERT/CC), established in 2003, aims at raising the technical capability for the protection of critical network infrastructure in order to create a safe internet and communication network. KISC develops effective countermeasures against hacking and viruses, such as cyber-attack countermeasure methodology and attack tools. KISC is organized into five major teams:

[2]For example, the NCSC issues the “NCSC Monthly”, which contains information about incidents, cyber-threat trends, response activities, and analysis results [25].

- Incident Analysis Team,
- Response Coordination Team,
- Hacking Response Team,
- Spam Response Team,
- Botnet Response Team,
- Network Monitoring Team.

KISC responds to threats against IT networks and has built cooperation systems with relevant organizations in order to immediately handle incidents. As a member of FIRST, KISC does its utmost to fulfill its duties in cooperation with international organizations. The tasks of KISC (KrCERT/CC) are as follows:

- Technological support to prevent cyber-incidents;
- Analysis of cyber-incidents, analysis of malicious codes and their destructive power, and development of response and recovery measures;
- Analysis of network traffic and the status of the internet, monitoring of vulnerabilities at the national and the international levels;
- Analysis of the latest hacking tools and development of response measures;
- Receiving reports on spam, making improvements to the legal system, and analyzing domestic as well as international trends;
- Reinforcing cooperation with international CERTs;
- Dealing with phishing, activating CERTs, and raising awareness in the private sector [27].

### 4.3 Information Sharing and Analysis Center (ISAC)

In 2001, the first Korean Information Sharing and Analysis Center (ISAC) was established, after regulations were enacted according to Article 16 of the National Information Infrastructure Protection Act. The aim of ISACs is to prevent cyber-attacks on critical information infrastructures by sharing information on incidents with other companies and with the authorities concerned.[3]

In Korea, there are three ISACs, each of them addressing businesses of a different sector:

- The KS-ISAC (Korean Security Information Sharing and Analysis Center) was the first ISAC in Korea. It offers a database on cyber-incidents, vulnerabilities, and patches, shares information with relevant organizations outside the ISAC, and provides information online; [28]
- The KF-ISAC (Korea Financial Information Sharing and Analysis Center) was established in 2002 within the Korean Financial Telecommunication and Clearings Institute (KFTC). It provides various information security services to the participating members, especially customized for the Korean banking industry. The most important services are information security reports; real-time monitoring and warning services; information security checks for core systems; and education and training services [29];

[3]The first ISACs were established in the US (see country survey on the United States in this volume).

- The Korean Telecommunication ISAC was also established in 2002. It aims to provide its members with the opportunity to share proper information on incidents and to exchange experiences and insights. The ISAC gathers and disseminates information obtained from different sources, such as CERTs or other information-security associations [30].

## 5 LAW AND LEGISLATION

### 5.1 Information Security Promotion Systems

Information-security promotion systems in Korea can be divided into national cyber-security systems, e-Government security systems, critical information infrastructure systems, and private information security systems. With respect to the national cyber-security system, the National Cyber Security Management Regulation was issued by a presidential directive on 31 January 2005, which regulates cyber-security organizations such as the National Cyber Security Strategy Council or the National Cyber Security Center. Meanwhile, for e-Government security systems, the Act on Promotion of Electronic Administration for e-Government, enacted on 28 February 2001, regulates matters of information protection as well as e-Government.[1]

### 5.2 Digital Signature Act 1997

The Digital Signature Act was enacted by Korea Parliament on July 1997 and revised on 31 December 2005 [31].[1] The purpose of the Digital Signature Act is to endow electronic documents with an equal level of legal validity as paper documents and to regulate basic matters related to achieving reliability, protect consumer rights, and implement policies, and thus to promote electronic commerce, with a view to creating a legally predictable environment in which the private citizens can make secure transactions in the Information Age. It contains provisions on "definition of digital signature", "licensed certification authority", "public-key certificate", "security and trust for certification service", and "electronic certification policy", etc. Responsibility for implementing this act has resided with the Ministry of Public Administration and Security since March 2008.

### 5.3 Act on Promotion of Utilization of Information and Communication Network and Information Protection 1999

The Act on Promotion of Utilization of Information and Communication Network and Information Protection was enacted on 1999 and revised on December 2007 [32].[1] The purpose of this act is to promote the use of information and communications networks, to protect users' personal information when they are using information and communications services, and to construct an environment within which users can safely use information and communications networks. It consists of many articles governing the utilization of digital documents through relay servers, protection of personal information, protection of juveniles in information and communication networks, securing the safety of information and communications networks, and other issues. Responsibility for implementing this act has been shared by the Ministry of Public Administration and Security, the Korea Communication Commission, and the Ministry of Knowledge and Economy since March 2008.

### 5.4 Act on Private Information Protection of Public Organizations 1994

The Act on Personal Information Protection by Public Organization, enacted in 1994 and revised in 1998, aims to ensure the adequate performance of public duties and to protect the rights and interests of users by protecting personal information processed by computers [33].[1]

### 5.5 Critical Information Infrastructure Protection Act 2001

The ministerial meeting on the prevention of large scale cyber-related incidents in February 2000 decided to pass a law covering comprehensive and systematic information infrastructure protection and countermeasures against so-called cyber-terrorism. The Critical Information Infrastructure Protection Act was enacted in January 2001 and revised in December 2007. It serves as a fundamental law protecting critical information infrastructure from various cyber-incidents. A critical information infrastructure was defined as a public or private network that carries information relevant to national security and safety or information of high financial value. The critical ICT infrastructure can also be defined physically as the whole network or a part of the network that exchanges information of high significance. This law consists of many articles defining the critical information and communication infrastructure, outlining protective measures and responses against cyber incidents, defining the work of the information security consulting agency, and specifying legal responsibilities and penalties. It outlines the government framework for critical information infrastructure protection. It directs the affairs of the Critical Information Infrastructure Protection Committee, the Working Group for Security Incident Response, and other central administrative organizations. Moreover, protection measures, prevention and response, technical support, development of technologies, international cooperation, and penalties for cyber-crimes are addressed [34]. Responsibility for enforcing this act has rested with the Ministry of Public Administration and Security since March 2008.

In addition, the Act on Private Information Protection of Public Organizations, the Act on Promotion of Electronic Administration for e-Government, and the Resident Registration Act in the public sector, as well as the Act on Promotion of Utilization of Information and Communication Network and Information Protection in the private sector deal with private information security systems [35].[1]

### 5.6 e-Commerce Framework

As electronic transactions and commerce across long distances become more common due to the development of ICT networks, a legal framework has been established regarding electronic signatures and their certification, in order to secure the safety and reliability of electronic documents that are drawn up by data processing systems and then transferred, received, or saved. The Digital Signature Act and the e-Commerce Framework Act regulate certification of electronic signatures, and the Act on Promotion of Electronic Administration for e-Government governs the use of digital signatures in the public administration [36].[1]

### 5.7 Protection of Telecommunication Networks and Information Systems

As attacks on telecommunication networks and information systems increase in the public and private sectors, the need for a systematic national-level protection system has

become urgent. The Framework Act on Information Promotion, the Critical Information Infrastructure Protection Act, the Act on the Promotion of Utilization of Information and Communication Network Utilization and Information Protection, the e-Commerce Framework Act, the e-Government Act, the Act on Trade Automation Promotion, the Act on Industrial Infrastructure, and the Freight Distribution Promotion Act have been passed to protect telecommunication networks and information systems [37].

### 5.8 Cyber-Attacks

The following laws and regulations are applied in order to prevent national and social loss arising from hacking, viruses, denial-of-service (DoS) attacks on telecommunication networks as well as other information systems, and theft or forgery of information:

- Article 28 of the Critical Information Infrastructure Protection Act imposes a penalty for attacks on critical information infrastructures;
- Article 62 of the Act on the Promotion of Utilization of Information and Communication Network Utilization and Information Protection outlaws attacks on telecommunication networks and violations of a duty to protect secret information;
- Article 25 of the Act on Trade Automation Promotion, as well as Sections 2 and 4 of Article 54 of the Freight Distribution Promotion Act, may also apply.

In addition, there are provisions in the national criminal legislation dealing with computer crime [37].

## ACKNOWLEDGMENT

We acknowledge the contribution of the expert Heung Youl Youm of Soonchunhyang University, who validated the content of this chapter.

## REFERENCES

1. (a) Chaeho, L. (2002). *Creating Trust in Critical Network Infrastructures: Korean Case Study* (slides), http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.14.pdf; (b) Cf. also Chaeho, L. (2002). Creating trust in critical network infrastructures: Korean case study. *Paper Presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures*. Seoul p. 4, http://www.itu.int/osg/spu/ni/security/docs/cni.05.doc.
2. Korean Information Security Agency (KISA) (2001). *Report on the Status of the Critical Information Infrastructure*, http://www.kisa.or.kr/index.jsp.
3. http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN008975.pdf, 2008.
4. Ministry of Information and Communication. (2002). *e-Korea Vision 2006. The Third Master Plan for Informatization Promotion (2002–2006)*, http://www.nca.or.kr/homepage/ehome/ehome.nsf/0/4f84e7068921413ec9256ce80024c20a/$FILE/e-Korea%20Vision%202006.pdf.
5. http://www.ipc.go.kr/ipceng/policy/vision_ground.jsp?num=1, 2008.
6. http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN027266.pdf, 2008.

7. (a) Heung, Y. Y. (2007). *Countermeasures for Combating Cyber Attacks in Korea*, p. 40, http://www.itsc.org.sg/pdf/6thmtg/Korea-Malaysia-Singapore-S.pdf; (b) MIC. *Basic Plan for ubiquitous Information Security (in Korean).*
8. http://www.mopas.go.kr, 2008.
9. http://www.kcc.go.kr, 2008.
10. http://www.ncsc.go.kr, 2008.
11. http://ncsc.go.kr/eng/files/20080123112558_NCSC_M0801.pdf, 2008.
12. http://www.icic.sppo.go.kr, 2008.
13. http://www.kisa.or.kr/index.jsp, 2008.
14. http://www.certcc.or.kr/english/vision.htm, 2008.
15. http://www.kisa.or.kr/kisae/kisec/jsp/kisec_6010.jsp, 2008.
16. http://www.kisa.or.kr, 2008.
17. http://www.etri.re.kr/eng, 2008.
18. http://www.etri.re.kr/www_05/e_etri, 2008.
19. http://www.most.go.kr, 2008.
20. http://www.nsri.re.kr/kor/index.html, 2008.
21. http://www.opm.go.kr/warp/webapp/content/view?meta_id=english&id=1, 2008.
22. Chaeho, op. cit., p. 4.
23. http://www.nisa.or.kr/link_2.php, 2008.
24. http://www.kisia.or.kr/new, 2008.
25. 25.http://www.ncsc.go.kr/eng, 2008.
26. http://www.ncsc.go.kr/eng, 2008.
27. http://www.certcc.or.kr/english/vision.htm, 2008.
28. http://www.allbusiness.com/company-activities-management/management-benchmarking/6058179-1.html, 2008.
29. http://www.kftc.or.kr/english/business/kf.html, 2008.
30. https://www.isac.or.kr/english/e_intro.swf, 2008.
31. (a) Korean Government. *Digital Signature Act (in Korean)*, http://www.klaw.go.kr/; (b) Heung, Y. Y. (2007). *Countermeasures for Combating Cyber Attacks in Korea*, p. 40, http://www.itsc.org.sg/pdf/6thmtg/Korea-Malaysia-Singapore-S.pdf; (c) MIC, *Basic Plan for Ubiquitous Information Security (in Korean).*
32. (a) Korean Government. *Act on Promotion of Utilization of Information and Communication Network and Information Protection (in Korean)*, http://www.klaw.go.kr/. (b) Heung, Y. Y. (2007). *Countermeasures for Combating Cyber Attacks in Korea*, p. 40, http://www.itsc.org.sg/pdf/6thmtg/Korea-Malaysia-Singapore-S.pdf; (c) MIC, *Basic Plan for Ubiquitous Information Security (in Korean).*
33. Korean Government. *Act on Private Information Protection of Public Organizations (in Korean)*, http://www.klaw.go.kr/.
34. Cha, Y.-S. (2002). *Korea's Approach to Network Security*, http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.21.pdf.
35. Korean Government. Act on Private Information Protection of Public Organizations. *The Act on Promotion of Electronic Administration for e-Government, and the Resident Registration Act in the Public Sector (in Korean)*, http://www.klaw.go.kr/.
36. Korean Government. *The e-Commerce Framework Act (in Korean)*, http://www.klaw.go.kr/.
37. http://www.klaw.go.kr, 2008.

# MALAYSIA

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

In Malaysia, the following sectors are regarded as making up the national critical infrastructure [1]:

- Financial Sector,
- Water and Sewerage,
- Communications and Media,
- Energy,
- Health and Emergency Services,
- Industry,
- Central Government,
- Government Services,
- Transportation,
- Military.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

National IT Agenda (NITA)
National Information Technology Council (NITC) Strategic Agenda
e-Secure Malaysia 2005 International Conference

### 2.1 National IT Agenda (NITA) and NITC Strategic Agenda

Malaysia launched the National IT Agenda (NITA) in 1996 as part of a major strategy to prepare the nation for the challenges of the information age. The agenda contains an outline for a national framework aimed at ensuring a balanced IT development for Malaysia, its infrastructure, and the applications found within. According to NITA, for this

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

effort to succeed, Malaysia requires greater trust and faith in the use of information and communication technology (ICT), which can be fostered through enhanced ICT security [2]. The launch of NITA provided the foundation and framework for the utilization of information and communication technology to transform Malaysia into an information and knowledge society.

Besides NITA, the National Information Technology Council (NITC) (see the chapter on Organizational Overview) formulated the NITC Strategic Agenda, a strategy involving a more participatory governance structure with active partnership between the public, private, and community-interest sectors. The Strategic Agenda includes concepts such as e-Community, e-Public services, and e-Economy. It is based on the assumption that knowledge and information will be the most valuable assets in the new economy [3].

### 2.2 e-Secure Malaysia 2005 International Conference

A major information security event, e-Secure Malaysia 2005, took place in September 2005 in Kuala Lumpur. It consisted of two conferences and an exhibition targeted at security professionals, solution providers, policy makers, corporate decision makers, and government officials. The event was jointly organized by various government agencies such as the Ministry of Science, Technology and Innovation (MOSTI); the Ministry of Energy, Water and Communications (MEWC); the Malaysian Communications and Multimedia Commission (MCMC); the National ICT Security and Emergency Response Centre (NISER); and the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU). The conference focused on the following topics: Computer Emergency Response Teams (CERTs) and incident response; critical infrastructure protection; network and application security; security management and strategy; and knowledge-sharing [4].

## 3 ORGANIZATIONAL OVERVIEW

The Malaysian Communications and Multimedia Commission (MCMC) has a coordinating role. The Malaysian Administrative Modernization and Management Planning Unit (MAMPU) administers security issues in the public sector. The Police Cyber Crime Unit is responsible for investigation and prevention of commercial cyber-crime. The Ministry of Science, Technology and Innovation (MOSTI) holds wide-ranging responsibilities concerning national ICT policy and security, while it is the objective of the Ministry of Energy, Water and Communications (MEWC) to protect the infrastructure.

As a public-private partnership, the Information Sharing Forum (ISF) strives to bring together various ICT stakeholders in order to jointly address Malaysian information and network security issues.

### 3.1 Public Agencies

***3.1.1 Malaysian Communications and Multimedia Commission (MCMC).*** The MCMC [5] is a statutory body established in 1998 in accordance with the national policy objectives set out in the Communications and Multimedia Commission Act[1] and

[1]This act created a new regulatory body, the MCMC. Cf. [6].

in the Communications and Multimedia Act (CMA).[2] The MCMC oversees the new regulatory framework for the converging industries of telecommunications, broadcast, and online activities. This includes the development and enforcement of access codes and standards. The MCMC ensures information security and the integrity and reliability of the network of Malaysia, identified as one of the ten national policy objectives in the CMA. Together with the police, the MCMC has enforcement powers for offences relating to network security in the CMA. In June 2002, MCMC hosted a workshop on Information and Network Security and the Protection of Critical Infrastructure [7]. In response to a proposal by the Malaysian prime minister in 2005, an initiative called IMPACT (an International Multilateral Partnership Against Cyber-Terrorism, set up by the Malaysian government) was recently launched. The first inaugurating IMPACT summit took place in Kuala Lumpur in May 2008 under the auspices of MCMC.

***3.1.2 Malaysian Administrative Modernization and Management Planning Unit (MAMPU).*** Security issues in the public sector are administered by the Malaysian Administrative Modernization and Management Planning Unit (MAMPU) [8]. Within MAMPU, the ICT Security Division also operates as Computer Emergency Response Team (GCERT) for the government [9]. In the field of e-Government, MAMPU developed the ICT Strategic Plan in 2003 to provide citizens and businesses with enhanced access to government information and services. The Public Sector ICT Strategic Plan outlines the guidelines for implementing the public sector's ICT requirements, frameworks, and the core areas to be strengthened [10]. The MAMPU is also the host of the Government ICT Security Command Center, a project designed to monitor cyber-threats to the network system and to public ICT. The aims of this project include the provision of periodic scanning of vulnerabilities and assets, the detection of security breaches, and forecasting and warning of cyber-attacks [11].

The current information security measures provided by MAMPU fall under three categories:

- *Proactive measures.* Providing ICT security documents such as an ICT security policy framework for the public sector; ICT incident reporting mechanisms; and best practices;
- *Recovery measures.* Ensuring the continuous function of critical business in the event of disruption; advice on how to upgrade patches; and warnings of virus attacks;
- *Continuous measures.* Monitoring, enforcement, policy review and improving ICT security management.

***3.1.3 Police Cyber Crime Unit.*** The Royal Malaysia Police has established a Technology Crime Investigation Unit under the Commercial Crime Investigation Division of the Criminal Investigation Department. The investigation officers in this unit investigate and take preventive action against commercial crime involving computers and internet-related

[2]This act set out a new regulatory licensing framework for a convergent communications and multimedia industry. For example, it covers fraudulent use of network facilities or services and interceptions of communications [6]. See the chapter on Law and Legislation.

crimes. The police has also established a forensic computer laboratory to assist officers investigating computer crime [12].

***3.1.4 Ministry of Science, Technology and Innovation (MOSTI).*** Under a recent restructuring, the Ministry of Science, Technology and Innovation (MOSTI) took over responsibility from the former Ministry of Energy, Communication and Multimedia (MECM) for the following areas:

- Formulation and implementation of national policy on ICT;
- Formulation and implementation of national information security policy;
- Encouraging research and development and commercialization of ICT;
- Development and promotion of ICT industries [13].

Following the restructuring, the secretariat of the National Information Technology Council (NITC) (see the chapters on Past and Present Initiative and on Early Warning and Public Outreach) was transferred to MOSTI. The ICT Policy Division within MOSTI was established on 1 March 2005 with five units, namely the Policy and Strategic Unit, the ICT Technology Studies Unit, the Assessment and Monitoring Unit, the ICT Acculturation Unit, and the NITC Secretariat [13].

At an NITC meeting in April 2006, agreement was reached on a Malaysian National Cyber Security Policy (NCSP), and the National ICT Security and Emergency Response Center (NISER) was assigned to carry out the function of the national cyber-security agency. In March 2007, NISER was given additional mandates and renamed CyberSecurity Malaysia. And in August 2007, CyberSecurity Malaysia was officially launched by the prime minister. It has been operating autonomously since then under the heading of the MOSTI [14] (see the chapter on Early Warning and Public Outreach).

***3.1.5 Ministry of Energy, Water and Communications (MEWC).*** The Ministry of Energy, Water and Communications (MEWC) was established in March 2004 and manages the nation's energy, communications (infrastructure), and postal services, as well as water supply. MEWC develops and formulates strategic and innovative policies, a self-regulatory framework, and an effective management system. One of its objectives is to ensure a secure and reliable supply and provision of energy, water, and communications services [15].

### 3.2 Public-Private Partnership

***3.2.1 Information Sharing Forum (ISF).*** The Information Sharing Forum (ISF) was formed in June 2004 by the Malaysian Communications and Multimedia Commission (MCMC). It brings together various Internet Service Providers (ISP) and other agencies—namely, CyberSecurity Malaysia, the ICT Security Division of MAMPU, and the Malaysian Technical Standards Committee—to address Malaysian information and network security issues. Apart from encouraging cooperation between different network owners, operators, and other agencies, this forum enables the sharing of experience and expertise for the benefit of the Malaysian network infrastructure. Moreover, it aims at elaborating guidelines and best practices.The ISF meets every month and is chaired by the MCMC. It also hosts a newsgroup where members interact and debate on issues before each ISF meeting [16].

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 Malaysian Computer Emergency Response Team (MyCERT)

In March 1997, the Malaysian Computer Emergency Response Team (MyCERT) was launched [17]. Over the years, MyCERT has provided assistance to many Malaysians in handling ICT security incidents. During this period, there was an increase in national awareness of ICT—in particular, of the fact that ICT security issues encompass a much broader scope than previously envisaged. Purely technical measures, such as firewalls, are not sufficient for tackling security threats. The government of Malaysia realized that the growing number and variety of ICT applications and devices produced by suppliers lacking fundamental security precautions had created a strong need for a trusted ICT security center to support not only reactive measures, but also proactive measures in ICT security. To this end, MyCERT provides a point of reference for the internet community to deal with computer security incidents and methods of prevention. It strives to reduce the probability of successful attack and lowering the risk of consequential damage. MyCERT has the following functions:

- Providing an expert point of reference on network and security matters;
- Reporting security incidents and facilitating communication to resolve security incidents;
- Disseminating security information, including system vulnerabilities and defense strategies;
- Acting as a repository of security-related information, acquiring patches, tools, and techniques;
- Educating the public with regard to computer security in Malaysia [18].

### 4.2 From the National ICT Security and Emergency Response Center (NISER) to Cyber Security Malaysia

The National ICT Security and Emergency Response Center (NISER) [14] was formed by the National Information and Communication Technology Council (NITC) to address e-Security issues and to act as Malaysia's CERT. NISER evolved from what was originally the Malaysian Computer Emergency Response Team (MyCERT) in March 1997. As mentioned earlier (see the chapter on Organization Overview, section on MOSTI), the transformation process of NISER into CyberSecurity Malaysia, through the adoption of the Malaysian National Cyber Security Policy, started in 2006. It was given additional mandates and officially launched by the prime minister in 2007 [14]. Thus, NISER's role was elevated as it became Cyber Security Malaysia. Today, CyberSecurity Malaysia exists as the national reference and specialist center for cyber-security under the purview of MOSTI. CyberSecurity Malaysia was formed as a one-stop coordination center for all national cyber-security initiatives with the aim to

- Reduce the vulnerability of ICT systems and networks;
- Nurture a culture of cyber-security among users and critical sectors;
- Strengthen Malaysian self-reliance in terms of technology and human resources.

With the advent of CyberSecurity Malaysia, the country has been striving towards overcoming cyber-threats and to build a safer and more secure cyberspace. The services offered by CyberSecurity Malaysia include computer emergency response, digital forensics, security assurance, security management and best practices, and training and outreach [19]. Therefore, CyberSecurity Malaysia offers services to private and public entities such as research in vulnerability detection, intrusion detection, and computer forensic technology. It is also a member of the Forum of Incident Response and Security Teams (FIRST) (see the chapter on FIRST in this volume) and APCERT (the Asia Pacific Computer Emergency Response Team). Through collaboration with other agencies, it provides specialized ICT security services and continuously identifies possible gaps that could be detrimental to national security [20]. CyberSecurity Malaysia fosters mutual co-operation, information-sharing, and expert assistance among the different government agencies involved. The integrative purpose of CyberSecurity Malaysia is to reduce the vulnerability of ICT systems and networks, to nurture a culture of cyber-security amongst users and critical sectors, and to strengthen Malaysian self-reliance in terms of technology and human resources [21].

## 5 LAWS AND LEGISLATION

The Malaysian government has passed a number of laws relating to cyberspace since 1997 to provide a comprehensive legal framework that encompasses the security of information and network integrity and reliability, for the benefit of society at large as well as the business sector in particular.

### 5.1 Computer Crimes Act 1997

Part II, Offences

3 (1) A person shall be guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;
(b) the access he intends to secure is unauthorized; and
(c) he knows at the time when he causes the computer to perform the function that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;
(b) a program or data of any particular kind; or
(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall on conviction be liable to a fine or to imprisonment not exceeding five years or to both [22].

### 5.2 Communications and Multimedia Act (CMA) 1998

An Act to provide for and to regulate the converging communications and multimedia industries, and for incidental matters.

Part 1—Preliminary Section 3.

Objects (1)

The objects of this Act are (a) to promote national policy objectives for the communications and multimedia industry; (b) to establish a licensing and regulatory framework in support of national policy objectives for the communications and multimedia industry; (c) to establish the powers and functions for the Malaysian Communications and Multimedia Commission; and (d) to establish powers and procedures for the administration of this Act.

(2) The national policy objectives for the communications and multimedia industry are—(a) to establish Malaysia as a major global centre and hub for communications and multimedia information and content services; (b) to promote a civil society where information-based services will provide the basis of continuing enhancements to quality of work and life; (c) to grow and nurture local information resources and cultural representation that facilitate the national identity and global diversity; (d) to regulate for the long-term benefit of the end user; (e) to promote a high level of consumer confidence in service delivery from the industry; (f) to ensure an equitable provision of affordable services over ubiquitous national infrastructure; (g) to create a robust applications environment for end users; (h) to facilitate the efficient allocation of resources such as skilled labour, capital, knowledge and national assets; (i) to promote the development of capabilities and skills within Malaysia's convergence industries; and (j) to ensure information security and network reliability and integrity.

(3) Nothing in this Act shall be construed as permitting the censorship of the Internet [23].

## REFERENCES


1. Rahman Bistamam Siru Abdul (MCMC) (2002).Malaysia's approach to network security. *Presentation held at ITU Workshop on "Creating Trust in Critical Network Infrastructures"*. Seoul, May 2002, slide 7, http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf.
2. http://www.cybersecurity.org.my/en/index.html, 2008.
3. http://www.msctc.com.my/idb/B-1.htm, 2008.
4. http://www.cybersecurity.org.my/en/knowledge_bank/news/2005/main/detail/891/index.html, 2008.
5. http://www.mcmc.gov.my, 2008.
6. http://www.mcmc.gov.my/about_us/roles.asp, 2008.
7. *Rahman Malaysia's Approach to Network Security*, op. cit., http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.19.pdf, 2008.
8. http://www.mampu.gov.my, 2008.
9. http://www.mampu.gov.my/perkhidmatan/gcert, 2008.
10. http://www.mampu.gov.my/perkhidmatan/isp, 2008.
11. http://www.mampu.gov.my/perkhidmatan/prisma, 2008.
12. http://mpk.rmp.gov.my/english/Eng_indexMail.htm, 2008.
13. http://www.mosti.gov.my/opencms/opencms/MostePortal/NITC/NITCIntro.html, 2008.

14. http://www.cybersecurity.org.my/en/about_us/history/main/detail/734/index.html, 2008.
15. http://www.ktak.gov.my/template01.asp?contentid=280, 2008.
16. Tho Swee Hoe, Malaysian Communications and Multimedia Commission (2004). Information and network security issues in the communications and multimedia industry. *HackInTheBox Conference*, http://www.packetstormsecurity.org/hitb04/hitb04-toh-swee-hoe.pdf.
17. http://www.mycert.org.my/about.html, 2008.
18. http://www.mycert.org.my, 2008.
19. http://www.cybersecurity.org.my/en/about_us/brief_detail/main/detail/729/index.html, 2008.
20. http://www.cybersecurity.org.my/en/about_us/operational_mode/main/detail/735/index.html, 2008.
21. http://www.cybersecurity.org.my/en/about_us/establishment/main/detail/733/index.html, 2008.
22. http://www.cybercrimelaw.net/laws/countries/malaysia.html, 2008.
23. http://www.mcmc.gov.my/mcmc/the_law/ViewAct.asp?cc=4446055&lg=e&arid=900722, 2008.

# THE NETHERLANDS*

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Using the so-called Quick Scan method[1] and in consultation with the industry and government, it was determined in 2002 that the Netherlands' critical infrastructure comprises 11 sectors and 31 critical products and services [1]. That result was adjusted in the ensuing risk analysis phase. Since April 2004, the list comprises 12 critical sectors and 33

*This chapter was reviewed by Eric Luiijf, TNO Defense, Security and Safety; Williët Brouwer, Programme Manager Critical Infrastructure Protection, Ministry of the Interior; and André Griffioen, Deputy Programme Manager Critical Infrastructure Protection, Ministry of the Interior.
[1]For more information on "Quick Scan", see the chapter on Past and Present Initiatives.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

critical products and services. Infrastructures are deemed critical if they constitute an essential, indispensable service for society, and if their disruption would rapidly bring about a state of emergency or could have adverse societal effects in the longer term. In the Netherlands, critical sectors (and products and services) include the following: [2]

- Drinking Water Supply,
- Energy (Electricity, Natural Gas, and Oil),
- Financial Sector (Financial Services and the Financial Infrastructure, both Public and Private),
- Food (Food Supply and Food Safety),
- Health (Urgent Health Care/Hospitals, Sera and Vaccines, Nuclear Medicine),
- Legal Order (Administration of Justice and Detention, Law Enforcement),
- Public Order and Safety (Maintaining Public Order, Maintaining Public Safety),
- Retaining and Managing Surface Water (Management of Water Quality, Retaining and Managing Water Quantity),
- Telecommunications (Fixed Telecommunication Network Services, Mobile Telecommunication Services, Radio Communication and Navigation, Satellite Communication, Broadcast Services, Internet Access, Postal and Courier Services),
- Public Administration (Diplomatic Communication, Information Provision by the Government, Armed Forces and Defense, Decision-making by Public Administration),
- Transport (Mainport Schiphol, Mainport Rotterdam, Main Highways and Waterways, Rail Transport),
- Chemical and Nuclear Industry (transport, storage, and production/processing).

The Critical Information Infrastructure (CII) of the Netherlands consists mainly of the internal supporting infrastructure of critical sectors like the energy, transport, and financial sectors, and is supported by a set of services delivered by the telecommunications and energy sectors (fixed telecommunication, mobile telecommunication, internet access, electricity).

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

In the Netherlands, CIP/CIIP is perceived increasingly as a crucial issue of national security. Since the end of the 1990s, several efforts have been made to manage CIP/CIIP better. The early initiatives and policies were aimed at information security in general, because there was no clear definition of critical infrastructures. This changed with the Critical Infrastructure Protection Project, which started in 2001 and formulated dedicated policies for CIP and CIIP.

### 2.1 Early Efforts to Protect Information and Communication Infrastructure

***2.1.1 The Digital Delta.*** The publication The Digital Delta of June 1999 offered a framework for a range of specific measures regarding government policy on information and communications technology (ICT) for the next three to five years [3]. This memorandum noted the increasing importance of ensuring the security of information systems

and the communications infrastructure, and of mastering the growing complexities of advanced IT applications [4].

***2.1.2 Defense Whitepaper 2000.*** Likewise, the increasing importance of ICT is also explicitly mentioned in the Dutch Defense Whitepaper 2000: "Given the armed forces' high level of dependence on information and communication technology, it cannot be ruled out that in the future attempts will be made to target the armed forces in precisely this area" [5].

***2.1.3 Infodrome Initiative & BITBREUK.*** In March 2000, the key essay BITBREUK (English version In Bits and Pieces) was published by the government-sponsored think-tank Infodrome to stimulate the discussion on the need to protect CII.[2] The essay offered an initial vulnerability analysis and postulated a number of hypotheses for further discussion and examination by the Dutch authorities in co-operation with the appropriate national public and commercial organizations [6]. In mid-2001, this document was used as a starting point for a so-called 24-hour cabinet session. This was a 24-hour workshop with a selected group of experts that created a manifesto on CI/CII issues (KWINT-manifest) with a set of recommendations for all political parties. These recommendations provided the basis for the KWINT program to improve information security.

***2.1.4 KWINT Report and KWINT Program.*** The report entitled Kwetsbaarheid op Internet—Samen werken aan meer veiligheid en betrouwbaarheid (KWINT),[3] written by Stratix Consulting/TNO[4] for the Ministry of Transport, Public Works, and Water Management (V&W), was completed in 2001. The report concluded that the Dutch internet infrastructure was extremely vulnerable. Final recommendations were made on policy measures with regard to awareness and education, coordination of incidents, protection, and security. The report concluded that the measures should be realized within a public-private partnership framework, while the government should play a facilitating and coordinating role [7].

The findings and recommendations of this report triggered the formation of an interdepartmental working group of members of the Ministries of Economic Affairs, Defence, Finance, the Interior, Justice, and Transport (Telecom and Post Directorate).[5] As a result, the KWINT government memorandum Vulnerability of the Internet was endorsed by the cabinet on 6 July 2001. It includes a set of recommendations for action. The government-wide computer emergency response team, GOVCERT.NL, was established, and a malware-alerting service for Small and Medium Enterprises (SMEs) and the public was set up [8]. Other KWINT tasks were given to the Platform Electronic

[2]Infodrome was a think-tank founded in 1999 and sponsored by the Dutch government that served a threefold objective: (1) to develop an understanding of the social implications of the information revolution (this requires the gathering of empirical, quantitative knowledge and data on IT-related developments, and a systematic analysis thereof), (2) to stimulate social awareness of the importance of having a government policy that meets the requirements of the information society, and (3) to examine the priorities given by parties and interest groups to activities (public or private) undertaken in relation to the information society. This requires an understanding of the political and social value of knowledge, experience, and insights. The Infodrome project ended in 2002.

[3]Vulnerability of the Internet –Working Together for Greater Security and Reliability.

[4]TNO is the Netherlands' Organization for Applied Scientific Research.

[5]The Telecom and Post Directorate (DGTP) became part of the Ministry of Economic Affairs as of 1 January 2003.

Commerce in the Netherlands (ECP.NL), the public-private platform for e-commerce in the Netherlands.

The KWINT Program 2002–2005 was especially targeted towards the protection and safe use of the internet. The 2005 report to the Dutch parliament recognizes the need to address the security of ICT that is used across critical sectors. The dependency and vulnerability of Supervisory, Control, and Data Acquisition (SCADA), for instance, is a cross-sector ICT area that will be analyzed in detail.

***2.1.5 Veilige Elektronische Communicatie (VEC).*** The successor of the KWINT program is called Veilige Elektronische Communicatie (VEC).[6] The program started in January 2006 and will run for at least three years. The program is designed as a public-private partnership under the responsibility of the Ministry of Economic Affairs. It aims to raise general awareness of information security and will implement a pilot project to support SMEs in the fight against cybercrime [9].

## 2.2 The Critical Infrastructure Protection Project

In early 2002, the Dutch government initiated the critical infrastructure protection project Protection of the Dutch Critical Infrastructure,[7] with the objective of developing an integrated set of measures to protect the infrastructure of government and industry, including ICT [10]. The project includes four steps: 1) A quick-scan analysis of the Dutch critical infrastructure to identify products and services vital to the nation, the (inter-) dependencies of these products and services, and underlying essential processes; 2) stimulation of a public-private partnership; 3) threat and vulnerability analysis; and 4) a gap analysis of protection measures.

To identify sectors, products, and services comprising the national critical infrastructure, a Quick-Scan Questionnaire was developed. Dutch government departments used this questionnaire in early 2002 to make an inventory of all products and services that they regarded as vital, including the underlying processes and dependencies. In June 2002, an analysis of the collected information was presented in a working conference with key representatives of both the public and the private sectors. The initial results were augmented and refined in 17 workshops with the vital public and private sectors. In parallel, damage experts evaluated the potential damage impact of loss or disruption of vital products and services [11].[8]

In April 2003, the findings of the Quick Scan, performed in close collaboration with the Netherlands Organization for Applied Scientific Research (TNO), were published by the Ministry of the Interior and Kingdom Relations [12].[8] The following main conclusions were drawn from the Quick Scan results:

[6]Safe Electronic Communications.

[7]Bescherming Vitale Infrastuctuur.

[8]To determine the elements of the national critical infrastructure, the Dutch approach aims to distinguish between products and services vital to the nation and those that are "merely" very important. Under this method, a product or a service is defined as vital if it "provides an essential contribution to society in maintaining a defined minimum quality level of (1) national and international law and order, (2) public safety, (3) economy, (4) public health, (5) ecological environment, or (6) if loss or disruption impacts citizens or the government administration at a national scale." By measuring criticality according to a predefined minimum level of acceptable quality in vital services to society, the approach shifts the problem of defining "vital" or just "very important" elements to the political level. It is the government that must determine the level of damage impact that is acceptable to society.

- The Dutch government and industry now have a clear understanding of the critical products and services that comprise the Netherlands' critical infrastructure, and of their (inter-) dependencies;
- The direct and indirect vitality of critical products and services has been elaborated;
- It became clear that actors responsible for critical products and services only have a limited understanding of other critical products and services that depend on them, and of the extent of this dependence [13].[8]

The next steps concerning the strengthening of the Netherlands' CIP/CIIP included pinpointing the vital nodes for each of the critical services, risk and vulnerability analyses for each critical sector, scenarios to test the effectiveness of CIP/CIIP measures, and an international exchange of CIP/CIIP information and coordination [14].[8] In addition, the CIP project has been established as a regular policy file under the responsibility of the Ministry of the Interior and Kingdom Relations. In 2005, the ministry outlined the Report on Critical Infrastructure Protection for the attention of the Dutch parliament. The report contained a review of the achievements of the CIP Project and defined a new set of actions [15].

- *Intensifying critical infrastructure security policy.* CIP is a collective task, and it is important that all relevant stakeholders pull together to improve the security of national infrastructures. Therefore, a Strategic Board for CIP (Strategisch Overleg Vitale Infrastructuur, SOVI) was created (for more information, see the chapter on Organizational Overview);
- *Analyzing CIP dependency.* Fostering cross-critical sector communication is also the goal of the CIP Dependency project. Critical sectors must be able to get in touch with each other—not only to determine the extent of the crisis, but also to assess its likely duration. The project is underway and will determine whether the affected critical sectors will have to take additional measures in order to guarantee continuity;
- *Improving protection of critical infrastructures against human threats.* Protection against willful disruptions of vital services is a high priority. Such attacks may be conducted by hackers, activists, frustrated employees, ordinary criminals (who are motivated by financial gains), and terrorists. In order to prevent such attacks, cooperation between law enforcement units, the intelligence services, CERTs, and private parties is indispensable. The National Advisory Centre Critical Infrastructures (NAVI) [16] provides a platform for mutual exchange among these organizations;
- *Awareness-raising.* Scenario exercises will be implemented involving distribution plans for CI products/services in the event of scarcity of supply, both at the national and regional levels.

Progress reports on these activities were published in 2006 and 2007 [17].

### 2.3 National Security Strategy and Work Programme 2007–2008

In order to cope with emerging risks, the Dutch cabinet has drawn up a National Security Strategy and Work Programme for the years 2007–2008 [18]. The strategy defines the goals of Dutch security policy, analyzes and assesses threats and risks, and develops methods for strategic planning. The strategy pursues an all-hazard approach and aims to provide for a more coordinated and integrated approach to national security [19].

Accordingly, the strategy will serve as a framework for the future protection policies for critical infrastructures [20]. The document states that there are many potential threats to the country and that each of these threats puts a strain on national security. National security is conceived as being under threat when vital interests of the Dutch state and society are harmed to the extent that society can become destabilized. These vital interests, and examples thereof, include the following: [21]

- *Territorial security.* The threat or occurrence of (terrorist) attacks on Dutch soil;
- *Economic security.* The breakdown of overseas trade or an ICT malfunction;
- *Ecological safety.* An environmental disaster or disruption of the drinking water supply;
- *Physical safety.* A dyke breach or epidemic;
- *Social and political stability.* Tension between various ethnic groups.

In the Netherlands, national security encompasses both breaches of security by intentional human actions (security) and breaches due to disasters, system or process faults, human failure, or natural anomalies such as extreme weather (safety).

The new approach aims at allowing signals of potential threats to be identified at an earlier stage, by systematically linking information streams and cross-referencing developments (e.g., to what extent will energy requirements change if summers become warmer and more air conditioning and refrigerators are needed). The strategy formulates a method of weighing various interests and strives to prioritize among them [21]. Clearly, critical infrastructure protection is intimately linked with the National Security Strategy and planning. One of the capabilities named to be strengthened according to the national risk assessment (part of this programme) is business continuity [22].

In 2008 one of the issues addressed within the National Security Strategy is ICT failure. A project called "ICT-verstoring" was initiated in which relevant private and public parties co-operate in a government-wide analysis and risk assessment of ICT. In this project, short, medium, and long-term ICT threats to the Netherlands are identified and analyzed in terms of their likelihood and potential impact. The insights gained from this process are used to assess whether preventative capabilities and preparation are sufficient to cope with these threats.

## 3 ORGANIZATIONAL OVERVIEW

Responsibility for the Dutch CI and CII lies with various actors and involves public and private sectors as well as several ministries, including the Ministry of the Interior and Kingdom Relations, the Ministry of Economic Affairs, the Ministry of Transport, Public Works, and Water Management, the Ministry of Housing, Spatial Planning, and the Environment, and the Ministry of Health, Welfare and Sport. The General Intelligence and Security Service is also involved in protecting information security in the Netherlands.

Moreover, public-private partnerships play a crucial role in CIP and CIIP in the Netherlands. As mentioned above, the KWINT program and the Critical Infrastructure Protection Project are both based on public-private collaboration. The KWINT program led to a flurry of policy recommendations that are elaborated in further detail in the public-private partnership Platform Electronic Commerce in the Netherlands (ECP.NL). These recommendations refer to awareness-raising, research and development, alarm and incident response, and the integrity of information.

Public-private co-operation within the project Critical Infrastructure Protection Project gained further importance with the official establishment of the Strategic Board for CIP (SOVI). With regard to the protection of critical information infrastructures, the National Continuity Consultation Platform Telecommunication (NCO-T) is of special interest, because it enables public-private collaboration between the government and telecommunication companies on continuity planning and crisis response. Furthermore, the National Advisory Centre Critical Infrastructures is an initiative of the government striving to enhance information exchange on security issues between critical sectors, critical sector enterprises, and government agencies. Finally, the National Infrastructure against Cyber-Crime is a cyber-crime information-sharing model organized as a private-public partnership program.

### 3.1 Public Agencies

***3.1.1 Ministry of the Interior and Kingdom Relations (BZK).*** First of all, the Ministry of the Interior and Kingdom Relations (MoI) is responsible for the general C(I)IP policy, the co-ordination of the national activities across all sectors and responsible ministries, and international policy (e.g., EPCIP) and co-ordination. Additionally, the MoI is responsible for the protection of government information infrastructures (government CIIP), national emergency management, and the CIP aspects of emergency response services. The national emergency management includes the National Crisis Centre (NCC), which is in charge of co-ordination activities at the policy level in case of emergencies and disasters with a nation-wide impact.

***3.1.2 Ministry of Economic Affairs (EZ).*** Some other key C(I)IP areas are the responsibility of the Ministry of Economic Affairs (EZ). EZ is responsible for C(I)IP coordination with the private sector in the areas of energy and telecommunications, including the internet [23]. Other parts of the same ministry are responsible for CIP/CIIP policies regarding the private industry, including SMEs.

***3.1.3 Ministry of Transport, Public Works, and Water Management (V&W).*** The Ministry of Transport, Public Works, and Water Management (V&W) [24] is responsible for the public-private C(I)IP co-ordination for the critical infrastructures related to transport (road, rail, air, harbors, and inland shipping) and water management as well as the biochemical quality of the surface water.

***3.1.4 Ministry of Housing, Spatial Planning, and the Environment (VROM).*** The Ministry of Housing, Spatial Planning, and the Environment (VROM) [25] is responsible for public-private co-ordination of the C(I)IP activities of the chemical and nuclear industries, as well as the potable water infrastructure.

***3.1.5 Ministry of Health, Welfare and Sport (VWS).*** The Ministry of Health, Welfare, and Sport (VWS) [26] is responsible for the public-private coordination of the C(I)IP activities of the health sector.

***3.1.6 General Intelligence and Security Service (AIVD).*** The General Intelligence and Security Service (AIVD) [27] is a division of the Ministry of the Interior and Kingdom Relations and is tasked with protecting the information security and vital sectors of Dutch

society [28]. The AIVDs focus shifts in accordance with social and political changes. One of its tasks is to uncover forms of improper competition, such as economic espionage, that could harm Dutch economic interests. Another task is foreign intelligence. In the interests of national security, it will carry out investigations abroad, though only in the non-military sphere. The AIVD is responsible for analyzing potential and likely threats to the Dutch CI sectors.

### 3.2 Public-Private Partnerships

***3.2.1 Platform Electronic Commerce in the Netherlands (ECP.NL).*** The Platform Electronic Commerce in the Netherlands (ECP.NL) [29] has been tasked by the Ministry of Economic Affairs with setting up a public-private partnership program to implement the action guidelines of the KWINT Memorandum.

The objective of the KWINT program focused on the following aspects: continuity of the internet infrastructure in the Netherlands, viruses, denial-of-service attacks, hacking, transparency of internet services, integrity and confidentiality of information, and misuse by personnel. As the KWINT program expired in 2005, ECP.NL established the Digibewust program (Digital Awareness) [30] in order to improve awareness of information security.

***3.2.2 National Continuity Plan for Telecommunications (NACOTEL) and National Continuity Forum Telecommunications (NCO-T).*** The National Continuity Plan for Telecommunications (NACOTEL) was established in 2001 in order to structure the contingency policy and crisis management in the telecommunications sector. The public-private partnership included BT (IT-services), Enertel, KPN Telecom, Telfort, Orange, T-Mobile, and Vodafone—as well as the Ministry of Economic Affairs. NACOTEL was based on voluntary cooperation. The participants discussed possibilities to strengthen the security of the telecommunication sector. The building of trust was a central goal of the process. However, it became apparent that effective crisis management could not be achieved solely on a voluntary basis of cooperation. During crisis situations, it is possible that individual operators need to implement actions that run contrary to their interests. This analysis led to the decision to make participation in the public-private partnership mandatory for all operators of critical telecommunication services [31]. Therefore, NACOTEL was dissolved in February 2006 and replaced by the National Continuity Consultation Platform Telecommunications (NCO-T) [32].

***3.2.3 Strategic Board for CIP (SOVI).*** The Strategic Board for CIP (Strategisch Overleg Vitale Infrastructuur, SOVI) was established in September 2006 as a dedicated public-private partnership for critical infrastructure protection. All critical sectors are represented in the strategic board, which meets two or three times a year. In 2007, the SOVI initiated a study on the electric power dependency of the various critical sectors and their resilience and ability to cope with longer duration power outages. It investigated issues such as secondary dependencies (e.g., dependency of various sectors on diesel oil for back-up generators) and the way in which these are prioritized amongst the critical sectors. It also studied the question of which related arrangements already exist or have yet to be made.

***3.2.4 Nationaal Adviescentrum Vitale Infrastructuur (NAVI).*** The Dutch Nationaal Adviescentrum Vitale Infrastructuur (National Advisory Centre Critical Infrastructures,

NAVI) [33] was initiated by the Dutch government as part of the CIP action plan discussed above [34]. In 2006, the Dutch parliament agreed to its business plan for 2006–2009 [35]. NAVI has knowledge and expertise about the security of critical infrastructures and aims to exchange these with the critical sectors, critical sector enterprises, and government agencies. It builds upon its links within the government and critical sectors, such as current information provided by the AIVD and the Dutch National Coordinator for Counterterrorism (NCTb) [36].

NAVI offers various services to its constituency such as support for risk analysis as well as security advice. NAVI's modus operandi is derived from the (physical security aspect) of the UK's Centre for the Protection of National Infrastructure (CPNI). It has established sector-specific information exchanges between critical sectors and government functions. NAVI offers various services such as a front office and advisory function for critical infrastructure enterprises, good practices, and an international contact desk (information and good practices exchange with other nations and the EU). NAVI offers products such as risk analyses and risk methodologies, critical sector-specific threat scenarios, security methodologies, and advice.[9]

***3.2.5 Nationale Infrastructuur ter bestrijding van CyberCrime (NICC).*** The National Infrastructure against Cybercrime (NICC) was established in 2006 as a three year program [37]. The NICC infrastructure consists of several components: a contact point, a reporting unit, trend-watching, monitoring and detection, information distribution, education, warning, development, knowledge sharing, surveillance, prevention, termination, and mitigation. The NICC further strengthens this infrastructure by hosting the Cybercrime Information Exchange, where public and private organizations share sensitive information, and by developing and supporting practical projects and trials that both solve concrete problems and generate knowledge about cybercrime.

The Cybercrime Information Exchange information-sharing model is based on the one designed by the UK's Centre for the Protection of National Infrastructure (CPNI). The NICC Information Exchange function can be pictured as following a 'flower' model. The heart of the flower is made up of government bodies, like the police, intelligence services, GOVCERT.NL, and the NICC itself. Critical infrastructure sectors and some other major industrial communities that heavily rely upon ICT can be thought of as being the petals of the flower. The different sectors chair their own petal, decide which parts of the meeting can be attended by the government bodies, and decide which information is sharable outside their sector 'petal'. The confidentiality of their exchanged information is maintained by an agreed set of rules on dissemination that follow the Traffic Light Protocol.

Many of the recognized information infrastructure sectors take part in a 'petal': The financial sector; providers of drinking water, energy, and telecommunication; Schiphol Airport; Rotterdam harbor; large enterprises/multi-nationals; and the rail sector.

One of the 2007 activities was the analysis of the information security posture of the SCADA and other process control systems in the Dutch drinking water sector. As a result, a SCADA security good practices document has been developed [38].

It is expected that the NICC will receive new instructions in a successor program from mid-2009. The information exchanges will either continue under another public-private partnership entity or be merged with the NAVI activities that are oriented more towards physical security.[10]

[9]Information provided by an expert.
[10]Information provided by the country expert.

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 SURFCERT (part of SURFnet)

SURFCERT, formerly known as CERT-NL, is the Computer Emergency Response Team of SURFnet, the internet provider for institutes of higher education and for many research organizations in the Netherlands. SURFCERT handles all computer security incidents involving SURFnet customers, either as victims or as suspects. SURFCERT also disseminates security-related information to SURFnet customers on a structural basis (e.g., by distributing security advisories) as well as on an incidental basis (distributing information during disasters) [39].

## 5 GOVCERT.NL

A computer emergency response team for government departments (CERT-RO) was established in June 2002. In February 2003, it was renamed GOVCERT.NL [40]. It is operated under the responsibility of the Ministry of the Interior and Kingdom Relations (MoI). The GOVCERT.NL team is co-located and co-operates with Waarschuwingsdienst.nl (Alert Service) [41], a website and initiative provided by the Ministry of Economic Affairs/Directorate-General for Energy and Telecom (EZ/DGET). The Waarschuwingsdienst is responsible for issuing alerts and advice memoranda to the public and SMEs about viruses, Trojan codes, and other malicious software. Warnings are disseminated to the public via e-mail, web services, and SMS. The Waarschuwingsdienst was founded in early 2003 and is funded by the Ministry of Economic Affairs.

## 6 LAW AND LEGISLATION

### 6.1 Penal Code

The Penal Code prohibits attacks against (non-ICT) CI (e.g., sabotage and interference with water management systems, electricity, the railway network, etc.).

### 6.2 Computer Crime Laws

The second version of the Dutch computer crime law has been under development since 1999. It was delayed because of the need to adapt it to the European Cybercrime Convention, and several anti-terror measures have been included in this new national law. The Computer Crime Law II was introduced in September 2006, with some articles taking effect from September 2007 onwards [42].

### 6.3 Telecommunications Law

This law states the requirements that must be met by public telecommunication operators regarding the capacity, quality, and other properties of the services offered (e.g., free access to the 112 emergency number), as well as regulations with respect to safety and privacy precautions regarding their network and services.

### 6.4 Criminal Code, Articles 138a and 138b

In summary, Article 138a states that any person who intentionally and unlawfully accesses an automated system for the storage or processing of data, or part of such a system, is guilty of a breach of computer peace and shall be liable to a term of imprisonment not exceeding six months or a related fine [43] if they breach security by technical intervention with the help of false signals or a false key, or by acting in a false capacity.[10]

An unauthorized person penetrating an automated system who copies the contained, processed, or transferred information for their own use or use by a third party may be punished with a maximum of four years imprisonment. The same holds for someone using public telecommunications means for accessing an automated system with the purpose of own gain or gain of a third party or for unauthorized access to an automated system of a third party.

In summary, Article 138b states that whoever deliberately and without authorization disrupts an automated system by sending information to that system shall be punishable with no more than one year's imprisonment.

The penal aspects of disrupting various critical infrastructure services have been described in specific articles of penal law for electric power, railway systems, and water management, and are covered by a cybercrime law article that raises the penalties when the safety or even the lives of people are threatened, or when people are actually injured or die.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Eric Luiijf of TNO Defense, Security and Safety, and Williët Brouwer and André Griffioen of Ministry of the Interior, who validated the content of this chapter.

## REFERENCES

1. Ministry of the Interior and Kingdom Relations. (2003). *Critical Infrastructure Protection in the Netherlands*, http://cipp.gmu.edu/archive/NetherlandsCIreport_0403.pdf.
2. Ministry of the Interior and Kingdom Relations. (2005). *Report on the Netherlands*, Critical Infrastructure Protection, September 2005, p. 72.
3. http://www.gbde.org, 2008.
4. Luiijf, E., and Klaver, M. (2000). *In Bits and Pieces: Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society*, Amsterdam,translation of the Dutch Infodrome essay 'BITBREUK', de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij, p. 5.
5. Ministerie van Defensie. (1999). *Defensienota 2000*, p. 59.
6. Luiijf/Klaver, op. cit.
7. De Bruin, R. (2002). From research to practice: a public-private partnership approach in the netherlands on information infrastructure dependability. *Dependability Development Support Initiative (DDSI) Workshop*. Brussels, 28 February 2002.
8. http://www.waarschuwingsdienst.nl, 2008.

9. (a) http://www.minez.nl/dsc?c=getobject&s=obj&objectid=136886&!dsname=EZInternet&isapidir=/gvisapi/ (in Dutch), 2008; (b) Cf. also: Durinck, M., and Boersma, W. *Public-Private Partnership in Awareness Raising: Internet Safety Awareness in the Netherlands*, http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_public_awareness_raising_in_the_netherland_boersma_durincks.pdf.
10. Ministry of the Interior and Kingdom Relations. (2003). *Critical Infrastructure Protection in the Netherlands*. http://cipp.gmu.edu/archive/NetherlandsCIreport_0403.pdf.
11. Luiijf, E., Burger, H. H., and Klaver, M. H. A. (2003). Critical infrastructure protection in the Netherlands: a quick-scan. In *EICAR Conference Best Paper Proceedings*, U. E. Gattiker, P. Pedersen, and K. Petersen, Eds., EICAR, Denmark.
12. Luiijf, E., Burger, H. H., and Klaver, M. H. A. (2003). Critical infrastructure protection in the Netherlands: a quick-scan. In *EICAR Conference Best Paper Proceedings*, U. E. Gattiker, P. Pedersen, and K. Petersen, Eds., EICAR, Denmark, p. 7.
13. Luiijf, E., Burger, H. H., and Klaver, M. H. A. (2003). Critical infrastructure protection in the Netherlands: a quick-scan. In *EICAR Conference Best Paper Proceedings*, U. E. Gattiker, P. Pedersen, and K. Petersen, Eds., EICAR, Denmark, p. 23.
14. Luiijf, E., Burger, H. H., and Klaver, M. H. A. (2003). Critical infrastructure protection in the Netherlands: a quick-scan. In *EICAR Conference Best Paper Proceedings*, U. E. Gattiker, P. Pedersen, and K. Petersen, Eds., EICAR, Denmark, p. 25.
15. House of Parliament. (2005). (Tweede Kamer) 2005–2006, 26643 No. 75, 16 September 2005, and annex *Rapport ter Bescherming Vitale Infrastructuur*, dated 1 September 2005.
16. http://209.85.135.104/search?q=cache:ghBixn6L-noJ:www.fbiic.gov/reports/neth_2.pdf+%22govcert%22+%22aivd%22&hl=de&ct=clnk&cd=7&gl=ch, 2008.
17. Kamerstuk 2006–2007, 26643, nr. 83, Tweede Kamer and Kamerstuk 2007–2008, 29668, nr. 18, Tweede Kamer.
18. Ministry of the Interior and Kingdom Relations. (2007). *National Security Strategy and Work Programme 2007–2008*, http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/88474/natveiligh.bwdef.pdf.
19. Schoof, D. (2007). *National Security Strategy—The Netherlands*, Presentation, 25 September, http://www.hightechconnections.org/files/HTC_homeland_security_Dick_Schoof.pdf.
20. Ministry of the Interior and Kingdom Relations. (2007). *National Security Strategy and Work Programme 2007–2008* op. cit., p. 18.
21. http://www.minbzk.nl/bzk2006uk/subjects/public-safety/national-security, 2008.
22. http://www.minbzk.nl/onderwerpen/veiligheid/veilige-samenleving/nationale-veiligheid/publicaties/112985/item-112985, 2008.
23. http://www.minez.nl/content.jsp?objectid=140727, 2008.
24. http://www.verkeerenwaterstaat.nl/english, 2008.
25. http://international.vrom.nl/pagina.html?id=5450, 2008.
26. http://www.minvws.nl/en, 2008.
27. Algemene Inlichtingen- en Veiligheidsdienst. https://www.aivd.nl/, 2008.
28. http://www.fas.org/irp/world/netherlands/bvd.htm, 2008.
29. http://www.ecp.nl, 2008.
30. http://www.digibewust.nl, 2008.
31. http://www.minez.nl/dsc?c=getobject&s=obj&objectid=150713&!dsname=EZInternet&isapidir=/gvisapi/, 2008.
32. http://www.ez.nl/content.jsp?objectid=150712&rid=150996, 2008.
33. http://www.navi-online.nl, 2008.

34. House of Parliament. (2005). (Tweede Kamer) 2005–2006, 26643 No. 75, 16 September 2005, and annex *Rapport ter Bescherming Vitale Infrastructuur*, 1 September.
35. House of Parliament (Tweede Kamer) 2006–2007, 26 643, No. 85.
36. http://www.nctb.nl, 2008.
37. http://www.samentegencybercrime.nl/UserFiles/File/Leaflet_NICC.pdf, 2008.
38. Luiijf E. (2008). *SCADA Security Good Practices for the Dutch Drinking Water Sector*, Report TNO∼DV 2008C096.
39. http://cert-nl.surfnet.nl/home-eng.html, 2008.
40. http://www.govcert.nl/render.html?it=41, 2008.
41. http://www.waarschuwingsdienst.nl/render.html?cid=106, 2008.
42. Official publication: Staatsblad 2006, 300 and 301, 13th July 2006.
43. http://www.cybercrimelaw.net/laws/countries/netherlands.html, 2008.

# NEW ZEALAND*

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Critical information infrastructure protection (CIIP) in New Zealand is about the protection of infrastructure necessary to provide critical services. "Critical services are those whose interruption would have a serious adverse effect on New Zealand as a whole or on a large proportion of the population, and which would require immediate reinstatement" [1]. New Zealand's critical sectors comprise the assets and systems required for the maintenance of [1]:

*The Country Survey of New Zealand 2006 was reviewed by Richard Byfield and Mike Harmon, Centre for Critical Infrastructure Protection (CCIP). For this edition, the authors have thoroughly updated the New Zealand country survey by referring to open-source material.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- Emergency Services,
- Energy (including Electricity Generation and Distribution, and the Distribution of Oil and Gas),
- Finance and Banking,
- Governance (including Law and Order and National and Economic Security),
- Telecommunications and the Internet,
- Transport (including Air, Land, and Sea).

The various critical sectors depend on each other. Most systems assume the continuity of power and telecommunications infrastructures and make extensive use of networked information technology in their management and control systems.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

The New Zealand government's Defence Policy Framework is a crucial document illustrating that CIIP is a key objective of the country's overall security policy. The Centre for Critical Infrastructure Protection (CCIP) [2] addresses the cyber-threat aspects of that objective.

### 2.1 CIIP within the Defence Policy Framework

New Zealand's government promotes a comprehensive approach to security and aims to protect and maintain the country's physical, economic, social, and cultural security. In the government's Defence Policy Framework of June 2000, critical infrastructure protection is identified as one of the key objectives: "[ . . . ] to defend New Zealand and to protect its people, land, territorial waters, Exclusive Economic Zone, natural resources and critical infrastructure" [3].

### 2.2 Report on Protecting New Zealand's Infrastructure from Cyber-Threats

New Zealand's State Services Commission's e-Government Unit released the report Protecting New Zealand's Infrastructure from Cyber-Threats [4] on 8 December 2000. The report deals with the protection of New Zealand's critical infrastructure from cyber-crime and other IT-based threats. The report assessed levels of risk due to IT-based threats in finance and banking, transport, electric power, telecommunications and the internet, oil and gas, water, and critical state services that support national safety, security, and income [5]. The report made several recommendations such as [6]:

- The establishment of a New-Zealand-based security-monitoring and incident-handling organization;
- Harmonization of computer-crime legislation with that of other nations (e.g., Australia, the US, Britain, and Canada);
- Adoption of specific IT security standards;
- Establishment of an ongoing cooperation program between owners of critical infrastructure and the government.

### 2.3 Report Towards a Centre for Critical Infrastructure Protection (CCIP)

The Centre for Critical Infrastructure Protection was established in February 2001. The process of the center's development is traceable within the documents addressed below [7]. On 11 June 2001, the report Towards a Centre for Critical Infrastructure Protection (CCIP) was issued by the e-Government Unit [8]. Following the previous National Information Infrastructure Protection (NIIP) report of December 2000, it recommended that the government establish a centre for critical infrastructure protection. The argument was that the dependence of citizens and businesses on various infrastructure services, the vulnerability of IT systems, and the risks and possible damage caused in case of failure were increasing. Therefore, measures had to be taken to ensure that infrastructure operators and government agencies were kept up to date on vulnerability and threat information: "The CCIP is proposed as an insurance measure in that it mitigates, for a low cost, a risk of a large loss" [9].[1]

### 2.4 Manual on Security in the Government Sector

The Interdepartmental Committee on Security issued a comprehensive and detailed manual in 2002 called Security in the Government Sector [10], which took into account the Australian/New Zealand Standard AS/NZS ISO/IEC 17799:2001 Information Technology—Code of Practice for Information Security Management, which deals with possible sources of threats to information and ways to counter them. The manual's security guidelines are mandatory for government departments, ministerial offices, the New Zealand Police, the New Zealand Defence Force, the New Zealand Security Intelligence Service, and the Government Communications Security Bureau (GCSB). In the manual, the government requires that information important to its functions, its official resources, and its classified equipment be adequately safeguarded to protect the public and national interests and to preserve personal privacy.

Furthermore, the manual proposes that overall responsibility for security should rest with a manager, the designated Departmental Security Officer (DSO). That person's duties should include formulating and implementing the general security policy and common minimum standards within the organization, issuing instructions on security, and serving as liaison with the secretary of the Interdepartmental Committee on Security (ICS), the New Zealand Security Intelligence Service (NZSIS), and the GCSB for any special advice [11].

### 2.5 Security Policy and Guidance Website

The security policy and guidance website [12] provides information on the government's activities in the area of information security. This website acts as a focal point for the publication of government information about security standards, procedures, and resources.

### 2.6 Standards New Zealand (SNZ)

Standards New Zealand (SNZ) [13] promotes several standards specific to New Zealand, as well as a host of joint Australian/New Zealand and international standards. AS/NZS ISO/IEC 17799 Information Security Management provides an overview of factors to be considered and included in the protection of information and information systems.

[1]For more information about the CCIP, see the chapter on Organizational Overview.

## 3 ORGANIZATIONAL OVERVIEW

Among the public agencies concerned and involved with CIIP in New Zealand are the Domestic and External Security Group (DESG), the Officials Committee for Domestic and External Security Co-ordination (ODESC), the Interdepartmental Committee on Security (ICS), the Centre for Critical Infrastructure Protection (CCIP), the Government Communications Security Bureau (GCSB), and the e-Government Programme.

As public-private partnerships, the New Zealand Security Association (NZSA) tries to engage representatives of both sectors in a dialog, as does the Computer Society Special Interest Group on Security (NZCS SigSec).

### 3.1 Public Agencies

***3.1.1 The Domestic and External Security Group (DESG).*** The main actor in charge of formulating New Zealand's security policy, including CIIP, is the Domestic and External Security Group (DESG), which co-ordinates central government activities aimed at protecting New Zealand's internal and external security, including intelligence, counter-terrorism preparedness, emergency and crisis management, and defense operations. The DESG director provides timely advice to the prime minister on issues affecting the security of New Zealand, including policy, legislative, operational, and budgetary aspects. DESG is the support secretariat for the Officials Committee for Domestic and External Security Co-ordination [14].

***3.1.2 Officials Committee for Domestic and External Security Co-ordination (ODESC).*** The Officials Committee for Domestic and External Security Co-ordination (ODESC) is chaired by the prime minister and makes high-level policy decisions on security and intelligence matters, including policy oversight in the areas of intelligence and security, terrorism, maritime security, and emergency preparedness. ODESC comprises chief executives from the Ministry of Foreign Affairs and Trade, the Ministry of Defence and the Defence Force, the New Zealand Security Intelligence Service, the Government Communications Security Bureau, the police, the Ministry of Civil Defence and Emergency Management, the Treasury, and others when necessary [14].

***3.1.3 Interdepartmental Committee on Security (ICS).*** The Interdepartmental Committee on Security (ICS) [12] is a sub-committee of the Officials Committee for Domestic and External Security Co-ordination (ODESC). It formulates and coordinates the application of all aspects of security policy and sets common minimum standards of security and protection that all government organizations must follow. In addition, the ICS provides detailed advice on information security matters to government and other organizations or bodies that receive or hold classified information [15].

***3.1.4 Centre for Critical Infrastructure Protection (CCIP).*** The Centre for Critical Infrastructure Protection (CCIP) [2] was established in 2001 to provide advice and support to public and private owners of CI, in order to protect New Zealand's critical infrastructure from cyber-threats.

In the early stages of CCIP planning, the location of the new center was constrained by the need to give private-sector companies the confidence that their sensitive commercial and security information would be adequately safeguarded, as well as by the need to provide a secure environment to provide adequate protection for intelligence information

that the CCIP had to be able to access. It was stated that "Overseas experience shows that the center should not be part of a law-enforcement agency, since this might reasonably focus on the pursuit of offenders, to the detriment of rectifying damage and of confidentiality" [16].

The Government Communications Security Bureau was finally given the responsibility for this effort, based on cost-effectiveness as well as its significant IT security skills and its culture of security [16, 17]. Furthermore, the e-Government Unit acknowledged that the CCIP requires timely access to classified intelligence, among other sources, in order to provide the best chance of a successful threat warning [18].

Hence, the CCIP is located within the Government Communications Security Bureau and has three main tasks [19]:

- To provide a round-the-clock watch and warning advice to owners and operators of critical infrastructure and to the government;
- To investigate and analyze cyber-attacks against critical national infrastructure; and
- To work with national and international critical infrastructure agencies to improve awareness and understanding of cyber-security in New Zealand.

Whereas the CCIP provides coordination, support, and advice on the ways in which information security can be maintained and improved, owners of critical infrastructures in the public and private sectors remain responsible for the security of their own systems [20].

***3.1.5 Government Communications Security Bureau (GCSB).*** In 1977, the Combined Signals Organization was replaced by the current signals intelligence agency, the GCSB, which is a civilian organization. Its chief executive reports directly to the prime minister. The GCSB gives advice and assistance to New Zealand government departments and agencies concerning the security of information-processing systems [21].

One of the GCSB's tasks is to ensure the integrity, availability, and confidentiality of official information through the provision of Information Assurance (IA) services to departments and agencies of the New Zealand government, and to contribute to the protection of the critical infrastructure from IT threats [22]. The New Zealand Security of Information Technology (NZSIT) publications are therefore produced as guidelines for New Zealand government organizations in support of securing and protecting IT systems and associated information and services [23].

***3.1.6 e-Government Programme.*** The e-Government Unit [24] was established in July 2000 within the State Services Commission (a department of the New Zealand Public Service). The responsibilities of the e-Government Unit, as defined by the cabinet, included, first, the development of an overarching e-government strategy; second, to facilitate the uptake of the e-government vision by government agencies; third, to coordinate collaboration in identifying opportunities across government agencies; fourth, the unit is responsible for providing policy advice to the minister of State Services in relation to e-government; and finally, it is in charge of monitoring progress toward achieving the e-government vision [25]. In April 2001, the work of the new unit resulted in the publication by the government of New Zealand's first e-government strategy. The strategy was updated in December 2001, in June 2003, and most recently, in November 2006. The latest version, called Enabling Transformation, reflects changes in the IT environment. The strategy paper covers the following areas [26]:

- It clarifies what the goal of transformation means for service delivery and collaboration;
- It matches the measurement of success to the indicators for the development goals for state services;
- It confirms the key role of collaboration, standards, and interoperability;
- It provides an updated high-level outline of the work undertaken across the government;
- It establishes a new goal for the way in which the government uses technology by 2020.

### 3.2 Public-Private Partnerships

***3.2.1 New Zealand Security Association (NZSA).*** The New Zealand Security Association (NZSA) [27] was formed in 1972. It represents licensed and certificated persons providing services to government departments, state-owned enterprises, businesses, and private users. The NZSA has two member groups: Corporate members, who are individuals or companies engaged in the security industry, and associate members, who are individuals or companies involved or interested in security, although security is not at the core of their business operations. Members of the latter category include government departments, insurance companies, airlines, banks, food distributors, area health boards, oil companies, etc. [28]. Among the NZSA's main objectives are [29]:

- To set minimum operating standards for members, and to develop and approve codes of practice;
- To co-operate with the police, government departments, and other organizations and agencies concerned with the safekeeping of people, property, and information in New Zealand;
- To provide information and advisory services, education, and training.

***3.2.2 Computer Society Special Interest Group on Security (NZCS SigSec).*** The New Zealand Computer Society's Special Interest Group on Security (NZCS SigSec) [30] is a forum for networking with others with an interest in IT security from within and outside government. The group meets quarterly for a presentation and networking [31].

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 AusCERT

AusCERT[2] is the national Computer Emergency Response Team for Australia. It also provides significant support to New Zealand organizations. It is one of the leading CERTs in the Asia/Pacific region; it provides prevention, response, and mitigation strategies for members [32].

AusCERT was founded as a commercial CERT for Australia before the New Zealand Centre for Critical Infrastructure Protection (CCIP) was formed. The CCIP has a working relationship with AusCERT, but also provides an early-warning service and a moderated mailing list through its website. Moreover, CCIP Vulnerability Alerts are posted daily

[2]See also the Country Survey on Australia in this volume.

on the CCIP website and contain a summary of a vulnerability or patch deemed important by its operations center for general public release [33].

Several commercial organizations—including the New Zealand company Co-logic—also provide vulnerability alerts filtered and tailored for their customers [34].

## 5 LAW AND LEGISLATION

### 5.1 Crimes Amendment Act 2003: Crime Involving Computers

The Crimes Amendment Act came into force in October 2003. It includes four new offenses relating to the misuse of computers and computer systems. These offenses are:

- Accessing a computer system for a dishonest purpose (Section 249);
- Damaging or interfering with a computer system (Section 250);
- Making, selling, or distributing or possessing software for committing a crime (Section 251);
- Accessing a computer system without authorization (Section 252).The terms "access" and "computer system" are defined in Section 248.

The first two offenses carry a range of penalties depending on the seriousness of the offense, with a maximum of seven and ten years' imprisonment respectively, while the remaining offenses carry a maximum penalty of two years' imprisonment.

The Section 249 offense involves accessing a computer system directly or indirectly, either to obtain a benefit for oneself or to cause loss to another person, or with intent to do so. The essential element of the crime in either case is dishonesty or deception (which is separately defined in Section 240(2)).

The Section 250 offense involves intentional or reckless destruction, damage, or alteration of a computer system. In the most serious case, if this is done by a person who knows or ought to know that danger to life is likely to result, the section provides a maximum penalty of ten years' imprisonment. In cases where a person damages, deletes, modifies, or otherwise interferes with or impairs any data or software without authorization, or causes a computer system to either fail or deny service to any authorized users, the maximum penalty is seven years' imprisonment.

The key element of the Section 251 "sale, supply, or distribution" offense is that the person must either know that a crime is to be committed, or must promote the software in question as being useful for the commission of a crime, knowing that or being reckless as to whether it will be used for such a purpose. In the case of the "possession" offense, the key element is intention to commit a crime.

In practice, the more significant of these two offenses is likely to be Section 252, which in effect makes computer "hacking" a criminal offense. The offense is simple unauthorized access, whether direct or indirect, to a computer system, knowing that or being reckless as to whether one is unauthorized to access that computer system.

Sections 253 and 254 contain qualified exemptions in respect of the Section 252 offense for the New Zealand Security Intelligence Service and the Government Communications Security Bureau respectively, where those organizations are acting under the authority of (in the case of the NZSIS) an interception warrant or (in the case of the GCSB) a computer access authorization issued under Section 19 of the GCSB Act 2003 [35].

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Mike Harmon and Richard Byfield of the Center for Critical Infrastructure Protection, who validated the content of this chapter.

## REFERENCES

1. E-Government Unit, State Services Commission (2000). *E-Government: Protecting New Zealand's Infrastructure from Cyber Threats*, http://www.ccip.govt.nz/about-ccip/background/niip-report-final.pdf.
2. http://www.ccip.govt.nz, 2008.
3. (a) The New Zealand Ministry of Defence. (2000). *New Zealand Defence Policy*, http://www.defence.govt.nz/defence-policy.html; (b) Goff, P. (2007). Keynote address to the NZ Border Security and Civil Defence Forum. *Protecting New Zealand's Borders—The Government's Approach*, Auckland, http://www.beehive.govt.nz/speech/protecting+new+zealand%E2%80%99s+borders+%E2%80%93+government%E2%80%99s+approach.
4. *E-Government: Protecting New Zealand's Infrastructure From Cyber Threats*, op. cit.
5. Minister of State Services (2001). Media Release on Cyber-Crime. *Government addressing Cyber-Crime and IT-Based Threats*, http://www.ccip.govt.nz/about-ccip/background/mediarelease-cybercrime.pdf.
6. *E-Government: Protecting New Zealand's Infrastructure from Cyber Threats*, op. cit.
7. http://www.ccip.govt.nz/about-ccip/background.html, 2008.
8. E-Government Unit, State Services Commission of New Zealand. *Towards a Centre for Critical Infrastructure Protection*, 11 June 2001. http://www.ccip.govt.nz/about-ccip/background/ccip-final-report.pdf.
9. *Towards a Centre for Critical Infrastructure Protection*, 11 June 2001, p. 5. http://www.ccip.govt.nz/about-ccip/background/ccip-final-report.pdf.
10. Department of the Prime Minister and Cabinet (2002). *Security in the Government Sector*. http://www.security.govt.nz/sigs/index.html.
11. Department of the Prime Minister and Cabinet (2002). *Security in the Government Sector*, Chapter 2. http://www.security.govt.nz/sigs/index.html.
12. http://www.security.govt.nz, 2008.
13. http://www.standards.co.nz/default.htm, 2008.
14. http://www.dpmc.govt.nz/dess/index.htm, 2008.
15. *Security in the Government Sector*, op. cit.
16. Centre for Critical Infrastructure Protection (2001). *Cabinet Paper*, pp. 5,9–11, http://www.ccip.govt.nz/about-ccip/background/mediarelease-cybercrime.pdf.
17. *Towards a Centre for Critical Infrastructure Protection*, op. cit, p. 2.
18. *Towards a Centre for Critical Infrastructure Protection*, op. cit., p. 9.
19. http://www.ccip.govt.nz/about-ccip.html, 2008.
20. Centre for Critical Infrastructure Protection (2001). *Cabinet Paper*, http://www.ccip.govt.nz/about-ccip/background/cabinetpaper-ccip.pdf.
21. Domestic and External Security Group (2000). *Securing our Nation's Safety: How New Zealand manages its security and intelligence agencies*, http://www.dpmc.govt.nz/dpmc/publications/securingoursafety/index.html.
22. http://www.gcsb.govt.nz/functions/index.html, 2008.
23. http://www.gcsb.govt.nz/publications/nzsit/index.html, 2008.

24. http://www.e.govt.nz, 2008.
25. http://www.e.govt.nz/resources/research/public-sector-2004/public-sector-27-04.pdf, 2008.
26. http://www.e.govt.nz/about-egovt/strategy, 2008.
27. http://www.security.org.nz, 2008.
28. http://www.security.org.nz/Accredited_Members.php, 2008.
29. http://www.security.org.nz/education.php, 2008.
30. http://www.nzcs.org.nz/SITE_Default/special_interest_groups/SITE_Information_Systems_SIG/default.asp, 2008.
31. http://www.kaonsecurity.co.nz/TFCC_demo/Sigs_manual/chapter2.html, 2008.
32. http://www.auscert.org.au, 2008.
33. http://www.ccip.govt.nz/vulnerability-alerts.html, 2008.
34. http://www.cologic.co.nz/aboutus.html, 2008.
35. http://www.cybercrimelaw.net/laws/countries/new_zealand.html, 2008.

# NORWAY*

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

In April 2006, the Commission for the Protection of Critical Infrastructures in Norway submitted a report to the Ministry of Justice and the Police that defined the critical infrastructures of Norway as follows: "Critical infrastructures are those constructions and systems that are essential in order to uphold society's critical functions, which in

*The country survey of Norway was reviewed by Stein Henriksen, Norwegian National Security Authority; Håkon Styri, Norwegian Post and Telecommunications Authority; Einar Oftedal, Norwegian National Security Authority; and Lene Bogen Kaland, Norwegian National Security Authority and National Information Security Coordination Council.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

time safeguard society's basic needs and the feeling of safety and security in the general public" [1].

Based on this definition, the commission identified the critical sectors, distinguishing between critical infrastructures and critical societal functions. A societal function is critical when it is indispensable for covering society's basic needs. These "critical societal functions" are themselves dependent on different infrastructures, some of which are deemed to be critical. The criticality of infrastructures is assessed according to three criteria: dependency (a high degree of dependency on other infrastructures implies criticality), alternatives (few or no alternatives imply criticality), and tight coupling (a high degree of linkages to other infrastructures implies criticality).

Using these criteria, the commission identified the following critical infrastructures:

- Electrical Power,
- Electronic Communication,
- Water Supply and Sewage,
- Transport,
- Oil and Gas,
- Satellite-based Infrastructure [2].

These critical infrastructures provide the basis for the following critical societal functions:

- Banking and Finance,
- Food Supply,
- Health Services, Social Services, and Social Security,
- Police Services,
- Emergency and Rescue Services,
- Crisis Management,
- Parliament and Government,
- Judiciary,
- Defense,
- Environment Surveillance,
- Waste Treatment [2].

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

Over the past few years, and as a result of technological developments, there has been an increased focus on CIIP. CIIP has been regarded as a security issue in Norway since the end of the 1990s. In fact, CIIP was placed on the political agenda by the government commission on "A Vulnerable Society". Moreover, US policy has been an important trigger in putting CIIP on the political agenda in Norway as a political, security, and economic issue.[1]

[1]Information provided by an expert.

### 2.1 Policy Statements

In 1998, the State Secretary Committee for ICT [3] formed a subcommittee with a mandate to report on the status of ICT vulnerability efforts in Norway. Furthermore, the importance of CIIP is also stressed by the Defense Review 2000 and the Defense Policy Commission 2000.[1] In the aftermath of attacks in the US on 11 September 2001, the government considered it necessary to increase national safety and security, particularly within civil defense, in the Police Security Service, and in emergency planning within the health sector [4].

### 2.2 Report A Vulnerable Society

The governmental commission on A Vulnerable Society was established by royal decree on 3 September 1999. It was active from 1999 until 2000. The findings gave important input to the national planning process.[1] The commission's task was to study vulnerabilities in society with a broad perspective. The mandate was to assess the strengths and weaknesses of current emergency planning, to assess priorities and tasks, and to facilitate increased awareness, knowledge, and debate about vulnerabilities.

The government commission identified several focus areas. One of these was CI [5]. In its green paper A Vulnerable Society [6], the commission placed great emphasis on the significance of ICT for the vulnerability of society in general. The commission, in what was probably its most controversial proposal, recommended that responsibility for safety, security, and emergency planning should be concentrated in a single ministry [6]. Furthermore, a strategy based on the following pillars was proposed [6]:

- Partnership between the public and private sectors;
- Promotion of information exchange,
- Establishment of an early-warning capacity,
- Harmonization and adjustments of laws and regulations,
- Public responsibility for CIP.

### 2.3 ICT Vulnerability Project

The ICT Vulnerability Project was an interdepartmental group commissioned by the Ministry of Trade and Industry in 1999. The project collaborated with the government commission on A Vulnerable Society, and the two groups coordinated their findings on ICT vulnerabilities [7]. In the ICT Vulnerability Project, each sector authority evaluated the risks linked to specific functions in that sector. A common feature of these evaluations is that each individual sector operation is dependent on its own ICT user systems as well as on the public telecommunications services. Therefore, robust access to telecommunications seems to be very important to most sectors. The telecommunications services are dependent on ICT. This project resulted in the publication of the National Strategy for Information Security in 2003.

### 2.4 Safety and Security of Society

On 5 April 2002, the Ministry of Justice and the Police presented its 17$^{th}$ report on the Safety and Security of Society to the Norwegian Storting (parliament). The report

is a comprehensive statement of the government's proposals regarding the reduction of vulnerabilities in modern society and measures to increase safety and security in the future. It states that when assessing the vulnerability of society, it is important to "consider the consequences of lapses in CI, such as a lapse in the distribution of power or a lapse in telecommunication" [8]. The recommendations laid the basis for new government measures, including most importantly the formation of the new Directorate for Civil Protection and Emergency Planning (DSB) in 2003 [9].

### 2.5 National Guidelines to Strengthen Information Security, 2007–2010

The Norwegian government published a national strategy for securing ICT systems in Norway in June 2003 [10].[2] The strategy involved all aspects of ICT security, ranging from security for individuals, businesses, and the daily activities of the government to the security of IT-dependent critical infrastructure. As a result of the recommendations of the strategy, the NorCERT, NorSIS, and KIS organizations were established (for more information on these organizations, see below in the chapters on Organizational Overview and Early Warning and Public Outreach). In 2007, this was supplanted by the National Guidelines to Strengthen Information Security, 2007–2010.

These guidelines state three overriding targets for the work in the field of information security:

- Resilient and secure critical infrastructures and support systems for critical societal functions;
- A good security culture guiding the development and use of information systems and sharing of electronic information;
- High competence and a focus on research about information security.

Based on these three targets and on present security challenges, 11 objectives have been identified that will form the basis of concrete measures by the National Information Security Coordination Council (KIS):

- Increased protection of ICT infrastructures critical to society;
- Review of legislation for information security;
- Categorization of information and information systems;
- Implementing risk and vulnerability analyses;
- Awareness-raising and sharing of knowledge;
- Rapid and coordinated warning and incident management;
- Promoting use of standards and certifications;
- Increasing focus on R&D, education, and development of competencies in the area of information security;
- Establishing a coordinated scheme for identity management;
- Coordinating and developing Norwegian international participation;
- Continued development of the National Information Security Coordination Council [10].[2]

[2]This strategy proposed several initiatives for improving security based on the "OECD Guidelines for the Security of Information Systems and Networks".

### 2.6 Report on the Protection of Critical Infrastructures and Critical Societal Functions in Norway

This report was issued in April 2006 by the Commission for the Protection of Critical Infrastructure for the attention of the Ministry of Justice and Police and represents the most recent analysis of CIP and CIIP in Norway. It is a comprehensive assessment on how critical infrastructures and critical societal function are protected in Norway and analyzes the impact of recent evolvements (emergence of new threats, shifts in the ownership of infrastructures, reorganizations within the government) on CIP and CIIP.

As mentioned above, the report starts by defining critical sectors and critical societal functions and clarifies the concepts of threats, risks, vulnerabilities, prevention, etc. Furthermore, it provides an overview on the situation in all critical sectors and functions [11].

The report also contains various recommendations to improve the protection of critical infrastructures. The commission highlights the importance of coordinating the various CIIP efforts and recommends that the Ministry of Justice and Police assume leadership with regard to this task [12].

### 2.7 An Information Society for All

The report "An Information Society for All" was issued in December 2006 by the Ministry of Government Administration and Reform. The purpose of the report is to show the state of affairs in the ICT sector, and to invite debate on challenges and the way ahead. Chapter 9, dealing with ICT security, describes a number of security measures necessary to achieve secure ICT infrastructures. The report also clarifies responsibilities among several ministries—both in relation to preventive security work and responsibilities during a crisis [13].

## 3 ORGANIZATIONAL OVERVIEW

In Norway, the ministry or authority that has responsibility for an area during peacetime or non-crisis times also has responsibility during times of crisis and war. This system also applies to CIIP. The coordinating authority on the civilian side is the Ministry of Justice and Police. The overall authority for ICT security is the Ministry of Government Administration and Reform, which took over this task from the Ministry of Trade and Industry, while the Ministry of Defense is responsible on the military side. The Ministry of Transport and Communications has responsibility for the communication sector in Norway, including all related security issues. The directorates and authorities that are responsible for handling the various aspects of CIIP on behalf of the ministries are answerable to the respective ministries [14].

In order to promote public-private partnerships, the National Information Security Coordination Council (KIS) cooperates with the private sector.

### 3.1 Public Agencies

***3.1.1 Directorate for Civil Protection and Emergency Planning (DSB).*** The Directorate for Civil Protection and Emergency Planning (DSB) was established on 1 September 2003, replacing the former Directorate for Civil Defense and Emergency Planning and the Directorate for Fire and Electrical Safety. The DSB is subordinate to the Ministry

of Justice and Police, and its main task is to serve as a center of resources and expertise for emergency contingency planning. The DSB is a point of contact between the central authorities and regional commissioners during disasters occurring in peacetime.

To ensure adequate preparedness measures in the community, the DSB devotes considerable efforts to ensure that all Norwegian municipalities carry out risk and vulnerability analyses. The DSB works to ensure that activities involving preparedness responsibilities lead to the implementation of internal control systems to ensure the quality of emergency planning at local government level. The DSB also supervises the planning efforts in the ministries and offices of the regional commissioners. In the context of CIIP, the DSB coordinates and carries out research on vulnerabilities and the protection of critical assets in cooperation with other actors [9].

***3.1.2 Norwegian National Security Authority (NSM).*** The Norwegian National Security Authority (NSM) [15] was established on 1 January 2003 and coordinates preventive IT-security measures. It controls the level of security, e.g., of central and local public administration, and monitors private suppliers of goods and services to the public when the products or services concerned are security-sensitive. The NSM also develops technical and administrative security measures and issues threat evaluations and vulnerability reports. The Ministry of Defense funds and administers the NSM. Moreover,

- The NSM hosts SERTIT [16], the public Certification Authority for IT Security in Norway.
- The NSM operates NorCERT (see chapter on Early Warning and Public Outreach).

***3.1.3 Norwegian Post and Telecommunications Authority (NPT).*** The Norwegian Post and Telecommunications Authority (NPT) [17] is an autonomous administrative agency under the Norwegian Ministry of Transport and Communications, with monitoring and regulatory responsibilities for the postal and electronic communications markets in Norway. The NPT is responsible for contingency planning regarding the public electronic communications infrastructure.

***3.1.4 The National Information Security Coordination Council (KIS).*** The National Information Security Coordination Council (KIS) was established in May 2004 [18]. It is chaired by the Ministry of Government Administration and Reform and consists of representatives from six ministries, the Prime Minister's Office, and ten different directorates. KIS has no authority to make decisions, but provides a platform for discussions and advises ministries and government agencies in topics related to ICT security, national security (interests), critical information infrastructure, common standards, working methods for ICT security, risks, and vulnerabilities.

KIS will have a central role in the implementation of the national guidelines to strengthen information security by [18]:

- Keeping track of the implementation of measures in different areas of responsibility;
- Identifying cross-sectoral challenges in information assurance that have to be followed up;
- Pushing for the implementation of measures of a cross-sectoral nature.

The KIS will be in close dialog with the private sector, local government, and others that may be impacted by the guidelines during the implementation of measures.

### 3.2 Public-Private Partnerships

In reaction to the report A Vulnerable Society, public-private initiatives have been established to enhance early-warning capabilities, e.g., NorCERT and NorSIS. In addition, there are sectoral co-operation bodies within sectors such as electric power, finance, oil, and telecommunications. KIS co-operates with the private sector in the further development of the guidelines. Representatives of the private sector are invited to participate in working groups when required.

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 NorCERT

The Norwegian Computer Emergency Response Team (NorCERT) was formally established in January 2006 as an operational department of the NSM and is the national CERT for Norway. NorCERT consists of two integrated sections [19]:

- The Warning System for Digital Infrastructure (VDI) was established in 2000 by the government. VDI intended to enable security professionals to chart the extent of the threat to vulnerable information infrastructure through the use of a national monitoring system to collect data on emerging threats. Since 2006, VDI has been an integrated part of NorCERT.
- The Incident Handling Section is responsible for incident handling and coordination, including vulnerability handling and artifact handling.
- Together, these two sections manage the Operation Center, where they maintain an up-to-date view of current cyber-threats and day-to-day operational matters.

Apart from early warning and incident-handling, NorCERT also serves as a point of contact for similar organizations abroad and shares information with other response teams regarding emerging threats.

### 4.2 UNINETT CERT

The Computer Emergency Response Team of the UNINETT (the academic research network) [20] was already formed in 1995. Its constituency consists of the Norwegian state universities, colleges, and research and development institutions. The team was created to contribute to better internet security for UNINETT member institutions, and to serve as a focal point for security issues regarding UNINETT member institutions [21]. The basic duty of UNINETT CERT is to provide assistance on handling and investigating incidents involving one or more members of the constituency, but it also collaborates with NorCERT to improve overall information security [21].

### 4.3 Norwegian Center for Information Security (NorSIS)

The aim of the Norwegian Center for Information Security (NorSIS) is to improve the overall level of information security in Norway. Its primary target groups are SMEs and the public authorities. NorSIS engages in the following activities:

- Making the public aware of the importance of information security by means of training and information;

- Compiling guidelines and tutorials for users;
- Establishing an overall awareness towards information security.

The NorSIS has its own web page [22] offering news, advice, and guidance. In addition, the NorSIS helps to disseminate information during serious incidents.

### 4.4 Norwegian Post and Telecommunications Authority

The Norwegian Post and Telecommunications Authority (NPT) has responsibility for contingency planning related to the public telecommunications infrastructure. Its area of responsibility includes the following tasks:

- Considering investment in measures designed to increase the robustness of the telecom networks;
- Conducting inspections to see that the required measures are implemented;
- Creating awareness, improving expertise, and offering guidance to operators, users and other players (courses, seminars, company visits, establishment of forums of expertise, etc.);
- Arranging joint exercises and developing cooperation between the operators of telecom networks.

Electronic communications providers who provide essential electronic communications services to users who have socially critical functions must notify the NPT of significant operational and technical problems that could reduce or have reduced the quality of services.

The establishment of the nettvett.no portal [23] in April 2005 is one example of the NPT's instructional undertakings within the security area. This portal provides information about the secure use of the internet.

## 5 LAW AND LEGISLATION

There are a number of regulations concerning information assurance and critical infrastructures, distributing responsibility onto several bodies. The most pertinent and overriding regulations concerning CIIP in Norway are:

- *The Security Act.* [24] This act applies to the protection of objects and information from incidents threatening security.
- *The Electronic Communications Act.* [25] This act applies to activity connected to the transmission of electronic communications and the associated infrastructure, services, equipment, and installations.
- *Personal Data Act.* [26] This act applies to the processing of personal data wholly or partly by automatic means, and other processing of personal data that is part of or intended to form part of a personal data filing system.

In addition to these, there are sector-specific regulations. Most Norwegian public and private bodies are subject to relevant regulations issues by various authorities. The national guidelines to strengthen information security will, inter alia, focus on making regulations about information assurance more consistent and user-friendly.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Stein Henriksen of the Norwegian National Security Authority, Håkon Styri of the Norwegian Post and Telecommunications Authority, Einar Oftedal of the Norwegian National Security Authority, and Lene Bogen Kaland of the Norwegian National Security Authority and National Information Security Coordination Council, who validated the content of this chapter.

## REFERENCES

1. Commission for the Protection of Critical Infrastructures (2006). *Protection of Critical Infrastructures and Critical Societal Functions in Norway*, Report NOU, 2006:6, April, English summary, p. 4. http://www.regjeringen.no/upload/JD/Vedlegg/Norwegian_CIP_Commision_-_Report_NOU_2006_No_6_English_summary.pdf.
2. Commission for the Protection of Critical Infrastructures (2006). *Protection of Critical Infrastructures and Critical Societal Functions in Norway*, Report NOU, 2006:6, April, English summary, p. 5. http://www.regjeringen.no/upload/JD/Vedlegg/Norwegian_CIP_Commision_-_Report_NOU_2006_No_6_English_summary.pdf.
3. *Statssekretærutvalget for IT–SSIT*.
4. Report No. 17 to the Storting (2000–2001).
5. Hovden, J. Public policy and administration in a vulnerable society: regulatory reforms initiated by a Norwegian commission. *J. Risk Res*. **7**(6), 629–641.
6. http://www.regjeringen.no/Rpub/NOU/20002000/024/PDFA/NOU200020000024000 DDDPDFA.pdf (in Norwegian), 2008.
7. Dependability Development Support Initiative (DDSI). (2002). *European Dependability Policy Environments*, Country Report Norway, (April 2002 version).
8. Ministry of Justice and the Police. Report No. 17 to the Storting (2000–2001). (2002). *Statement on Safety and Security of Society*. http://www.regjeringen.no/en/dep/jd/Documents-and-publications/Reports/Reports/2002/Statement-on-Safety-and-Security-of-Soci.html?id=420173.
9. http://www.dsb.no/forside.asp, 2008.
10. The Norwegian Government. (2003). *National Strategy for Information Security: Challenges, Priorities and Measures*, http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf/viewHtml/index/$FILE/Norway_Nat%20strat%20info%20security.pdf.
11. *Protection of Critical Infrastructures and Critical Societal Functions in Norway*, op. cit, p. 13ff.
12. Commission for the Protection of Critical Infrastructures (2006). *Protection of Critical Infrastructures and Critical Societal Functions in Norway*, Report NOU, 2006:6, April, English summary, p. 7. http://www.regjeringen.no/upload/JD/Vedlegg/Norwegian_CIP_Commision_-_Report_NOU_2006_No_6_English_summary.pdf.
13. Norwegian Ministry of Government Administration and Reform. (2007). Report No. 17 (2006–2007) to the Storting. *An Information Society for All*. http://www.regjeringen.no/en/dep/fad/Documents/Government-propositions-and-reports-/Reports-to-the-Storting-white-papers/2006–2007/Report-No-17-2006–2007-to-the-Storting.html?id=441497/.
14. The Office of the Auditor General. (2005). *The Office of the Auditor General's Investigation into the Authorities' Work to Secure IT Infrastructure*. http://www.riksrevisjonen.no/NR/rdonlyres/2E806C9B-CB55-4F65-9BBA-09D23E3D6044/0/Eng_Doc_3_4_2005_2006.pdf.
15. http://www.nsm.stat.no, 2008.

16. http://sertit.no/article/1, 2008.
17. http://www.npt.no, 2008.
18. http://www.kis.stat.no, 2008.
19. http://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet–NorCERT/NorCERT/English/, 2008.
20. http://forskningsnett.uninett.no/index.en.html, 2008.
21. http://cert.uninett.no/policy.html, 2008.
22. http://www.norsis.no, 2008.
23. http.//www.nettvett.no, 2008.
24. http://ww.nsm.stat.no/, 2008.
25. http://www.npt.no/portal/page/portal/PG_NPT_NO_EN/PAG_NPT_EN_HOME/PAG_PUBLICATIONS/PAG_REGULATIONS/, 2008.
26. http://www.datatilsynet.no/templates/Page_194.aspx/, 2008.

# POLAND*

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

According to expert opinion, Poland perceives those physical and cyber-based systems as critical infrastructures that are essential to the minimum required operations of the economy and the government. They include the following sectors:

- Telecommunications,
- Energy,

*The Country Survey of Poland was reviewed by Tomasz Prz1da, Polish Internal Security Agency, Micha3 M3otek, Polish Ministry of Interior and Administration, and Miros3aw Maj and Krzysztof Silicki, NASK/CERT Polska, Poland.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- Banking and Finance,
- Transportation,
- Chemical Industry,
- Water and Sewage Systems,
- Private and governmental emergency services [1].

In the same expert document, information and communications systems are more specifically defined as key assets within the overall realm of critical infrastructures. Therefore, among other things, it is recommended that the control systems be enhanced and prioritization plans be developed for ensuring cybersecurity.

## 2 INITIATIVES AND POLICY

It was officially acknowledged in Poland in 2000 that access to information has become increasingly significant for the economy and social life, and therefore the Polish government seeks to use means of communication to support the economy and to improve the public standard of living. These government activities were in response to the Polish parliament's resolution of 14 July 2000 on building the foundation of an Information Society in Poland, which underlines that modern technologies, services and applications of telecommunication, communication, and multimedia services may be a catalyst for economic growth, increase the competitiveness of the economy, create jobs, foster the development of the democratic state and its regions, assist in education and health care, and improve access to cultural goods [2]. As a consequence of this acknowledgement, several initiatives have been launched. On the one hand, these initiatives mainly fall into two categories—the development of the Polish Information Society (ePolska) and the application of elements of the Information Society to the public administration (e-government). On the other hand, issues related to the protection and security of information and its infrastructure are addressed exclusively within a single research and development organization, the Polish data networks operator and Research and Academic Computer Network (NASK). The latter are addressed in the early warning and public outreach section of this chapter.

## 3 ePOLAND

In reaction to the above-mentioned parliamentary resolution on building the foundations for a Polish Information Society, the Council of Ministers adopted two relevant documents in 2001: A strategic publications called Aims and Directions of the Information Society Development in Poland and a paper on practical aspects called Action Plan for the Information Society Development in Poland for the years 2001–2006—ePoland [3]. The strategic document had been prepared by the State Committee for Scientific Research in cooperation with the then Ministry of Telecommunications. It set out the following priorities: [4]

- Universal access to information;
- Information technology education;

- Changes in employment structure;
- Law and offences in the information and communications field;
- Electronic documents and commerce;
- Public procurement;
- Information technology implementation in the administration;
- Information and communication technology market development;
- Science and culture.

The Action Plan ePoland, oriented more towards practical applications, followed the European action plan eEurope—an Information Society for All that was issued by the European Commission in May 2000 [5]. The ePoland program [6] deals with a number of issues connected with the implementation of the Information Society, taking into consideration developments and realities in Poland. An absolute precondition for realizing the aims enshrined in the program is broadband, universal, affordable, and safe access to new electronic communication networks. In practical terms, ePoland comprises the following aims: Preparing society for rapid technological changes in the social and economic sphere due to the emergence of the Information Society, education of adults in the area of information technologies, and the promotion of professions connected with the application of these technologies. It foresees the adaptation of the legislative framework to the standards of rapid technological progress and the information age. Moreover, the ePoland action plan is to be compatible with the requirements of the electronic economy. This could be achieved by introducing legal regulation on electronic signatures, electronic transactions means, legal protection of databases, providing universal access to information technology, and electronic commerce. An additional advantage for the development of the Information Society in Poland is identified in the implementation of an electronic procedure in public procurement, facilitating online access to public administration, enhancing the participation of small- and medium-sized enterprises in e-commerce, and the elaboration of models for digital media in Poland.

In 2003, the ePolska action plan was updated in preparation for its adoption on 13 January 2004 by the Council of Ministers. Called ePoland—The Strategy on the Development of the Information Society in Poland for the years 2004–2006, it identifies information technology as a key challenge for Poland and specifies three priorities in order to achieve the goal of becoming a competitive knowledge-based economy and improving the quality of life of citizens: [7]

- Common access to electronic content and services;
- The development of valuable content and services accessible via the internet;
- The ability to use them.

The official projection of the prospects of the Information Society in Poland in the middle range perspective is contained in the document entitled The Proposed Direction of the Information Society Development to the year 2020, which was issued in late 2004. The document focuses on the prioritization of various aspects of public life in the context of Information Society development, and on the problem of ICT infrastructure as a factor shaping the overall framework of development opportunities [8].

### 3.1 E-government

The second pillar of Polish Information Society policies concerns the government's use of ICT and accessibility of government services. One of the government's most important programs for integration of information technology is the summary plan for communications technology development and its application in government administration, drawn up by the Ministry of the Interior and Administration [9]. In July 2003, the government accepted a draft bill on the "informatization of the public administration". The bill creates a legal framework for the monitoring and coordination of the various informatization projects of the public administration and specifically aims at the following: [10]

- To ensure compatibility of public IT systems and registries;
- To establish a legal framework for the development of e-government in Poland;
- To attain budgetary savings thanks to better coordinated spending on IT projects and to shift a number of public services to electronic platforms;
- To enhance the efficiency of the public administration and increase the quality of its services.

The bill empowered what was then the Ministry of Scientific Research and Information Technology (now the Ministry of Science and Higher Education) to audit all public IT systems for their appropriateness and viability and to establish mandatory standards for the exchange of documents and information between various public institutions. Moreover, the bill opens a way for citizens to deliver various public documents electronically.

Common access to e-government services is conditional on providing all citizens with internet access, or at least establishing a network of public internet access points. These projects have not been finished yet. In March 2005, the then Ministry of Science and Information Technology published a statement on "the comparative position of Poland in basic categories of e-government services". Among various services delivered by the public administration via internet, two basic categories can be pointed out based on the target group of the specific service: government to citizen (G2C)—with its reverse (C2G) services—and the second one, government to business (G2B) and reverse (B2G) services. Poland ranks low in the overall European comparison [11].

### 3.2 National Foresight Program

The Polish National Foresight Program was initiated in early 2003 by the then Ministry of Science and Information Technology. It is conceived as a method of building a vision for the medium- and long-term development of scientific and technical policy, its directions, and priorities, and is being implemented at the initiative of the Ministry of Science and Higher Education. An initiatory group of high-ranking experts was responsible for the definition of the foresight areas. The program's scope of realization covers three research areas: sustainable development, security, and information and telecommunications technologies. The latter area is to be coordinated by the Polish Ministry of Science and Higher Education [11] and centers on five major issues:

- Access to information;
- ICT and the society;

- ICT and education;
- e-Business;
- New media.

The foresight program is organized and managed by a coordination consortium, the conceptual work is done by different expert panels, and partnership institutions give scientific and analytical support [12].

## 4 ORGANIZATIONAL OVERVIEW

Within the Polish government, two ministries have responsibilities that impinge upon the country's information infrastructures and their protection—the Ministry of Science and Higher Education and the Ministry of the Interior. As a public-private partnership, the Polish Competence Center for eGov and eEdu [13] strives to provide a platform to bring together the public sector and the IT companies.

### 4.1 Public Agencies

In January 1991, the Parliament of the Republic of Poland passed an act creating the State Committee for Scientific Research (KBN). This governmental body was responsible for the science and technology policy of the state. Following the Council of Ministers' regulation of 18 March 2003, the Committee for Scientific Research was integrated into the newly founded Ministry of Science and Information Society Technologies. For the first time in the history of the Republic of Poland, a governmental body responsible for the country's information technology was created. After the parliamentary elections in 2005, the Ministry of Education and Science was established through the merger of the Ministry of National Education and Sport and the Ministry of Science and Information Technology. In mid-2006, the next reorganization resulted in the creation of the Ministry of Science and Higher Education [14].

***4.1.1 Ministry of Science and Higher Education.*** The main player and the coordinating body for science and technology policies is the Ministry of Science and Higher Education, which is involved in all policies relating to information infrastructures and their protection. Until November 2005, it was called the Ministry of Science and Information Technology. Its responsibilities relating to critical information infrastructures include:

- IT infrastructure, networks, and systems of the public administration;
- The establishment of IT standards for the public administration;
- Supervision and support of IT projects in public, central, and local administrations;
- Education and vocational training in Information Technology standards;
- The development of an Information Society in Poland;
- International cooperation within the IT sector and participation in EU programs [15].

The establishment of this ministry (and of its immediate predecessor) created a single coordinating institution for all state policies on informatization, it advises other ministries and institutions on informatization strategies, and it ensures the compatibility of national public IT systems and the economic viability of new informatization projects. Moreover,

the national foresight program Poland 2020 is also located under the auspices of the Ministry of Science and Higher Education.

***4.1.2 Ministry of the Interior and Administration.*** The Ministry of the Interior and Administration is crucial insofar as it is responsible for the national IT infrastructure, the national teleinformation system, and the national information administrative systems. These responsibilities are handled by the Department of Information Technology Development on the one hand, and through the Department of Teleinformational Infrastructure on the other hand. Both these departments are located at the Undersecretariat of State [16]. The latter is mainly in charge of maintenance of IT systems of the ministry, with particular attention given to security and availability of all processed data. Moreover, its responsibilities include[1]

- Supervision of the teleinformation networks used by government entities for accessing the state registries, planning, developing, and coordination of all IT networks of the ministry;
- Acting as an administrator of the government communication systems, including radio communications and also isolated systems;
- Fulfillment of tasks regarding the Polish Local Domain of the TESTA network and communication center of all the units of the ministry, including supervision and coordination in regard to isolated TESTA SIS/VIS networks;
- Supervision and maintenance of the Public Key Infrastructure (PKI) of the ministry as well as coordination of all tasks regarding digital signatures;
- Building and implementation of a special communication infrastructure for all public security and rescue forces;
- Maintaining continuity of all infrastructure considered essential for the state teleinformation systems and government communication;
- Prevent internal and external threats through securing the above-mentioned infrastructures.

Overall, the Ministry of the Interior and Administration is responsible for digitizing the public administration, developing the Information Society, and protecting it from exploitation of its vulnerabilities.

## 4.2 Public-Private Partnerships

***4.2.1 The Polish Competence Center for eGov and eEdu.*** The Polish Competence Center for eGovernment and eEducation was founded in February 2005 by four partners, including the Fraunhofer Institute for Open Communications FOKUS (Berlin), the Poznan Supercomputing and Networking Center (Poznan), the Foundation for Economic Education (Warsaw), and Witold Sartorius, the designated head and CEO of the center. It is currently run by the Foundation for Economic Education as a consortium and plans to become an incorporated not-for-profit company in Poland. The competence center aims at being an independent and trustworthy platform to bring the public sector, as a potential qualified customer, together with the IT companies to initialize successful and innovative IT projects with additional and significant cost saving and revenues for the partners.

[1]Information provided by an expert.

Therefore, the center supports and coaches partners and public sector clients during the whole process of preparing, organizing, and financing eGov and eEdu projects and brings them to the final implementation stage.

This includes tasks related to technology, organization and re-organization, as well as financial engineering in bigger and smaller projects. The center acquires, checks, tests, shows, and promotes modern IT and software solutions for the public sector and education. It has close links with Polish government bodies at both the ministerial and local levels. Moreover, the center also addresses projects in support of small and medium enterprises. The center's activities are driven by the belief that the strategic planning and realization of cost-effective IT solutions is the key to success for the Polish administration and public sector. Therefore, it aims at bringing the respective relationships to the next level by creating public-private institutional partnerships focused on the promotion of internet business solutions for the local governments. To this end, the competence center cooperates with a variety of programs and initiatives such as, among others, ePolska, the Cisco networking Academy Program, and the Polish education portal Interkl@sa [17].

## 5 EARLY WARNING AND PUBLIC OUTREACH

As mentioned earlier, the concerns of information infrastructure protection in Poland are mainly addressed by one particular organization—the Polish data networks operator NASK.

### 5.1 NASK Polska

NASK connected Poland to the internet in 1991. Since 1993, it has been a research and development organization and the leading Polish data networks operator. It offers telecommunications and data solutions to business, administration, and academic customers. Its service packages comprise broadband internet access, corporate networks, data transmission, collocation and hosting, videoconferencing, and network security services. NASK also carries out scientific and research activities in cooperation with the faculty of electronics and information technology at the Warsaw University of Technology—in particular, its cooperation with the Institute of Control and Computation Engineering led to the establishment of a biometric laboratory—and it is a member of many international organizations and associations including the Forum of Incident Response and Security Teams (FIRST) (see the survey on FIRST in this volume), the Council of European Top Level Domain Registries (CENTR), the Trans-European Research and Education Networking Association (TERENA), and the European IP Networks (Réseaux IP Européens, RIPE). Moreover, NASK is the Polish national registry of internet names in the.pl domain. The Polish Computer Security Response Team (CERT Polska), a part of the NASK organization, is very much engaged in information infrastructure protection and security issues [18].

### 5.2 CERT Polska

The Polish Computer Emergency and Response Team that is now called CERT Polska was formerly known as CERT NASK and was established in March 1996 by the NASK director. Its goals include:

- To provide a single trusted point of contact in Poland for the community of NASK customers and other networks in Poland to deal with network security incidents and their prevention;
- To respond to security incidents in networks connected to NASK and networks connected to other Polish providers reporting security incidents;
- To provide security information and warning of possible attacks in cooperation with other incident response teams all over the world.

The CERT Polska team registers all requests, alerts, and incoming and outgoing information and provides statistical data and reports on registered incidents. It also provides help for sites that have security problems, and supplies current information about security problems and solutions for dealing with them [19]. CERT Polska itself points out that the creation and maintenance of a computer security and incident response team benefits the government in many respects. Four of its areas of activities in particular contribute to critical infrastructure protection: Early warning and alerting, centralized security management, security response, and auditing [20]. CERT Polska signed a cooperation agreement on IT security with the Information Security Department of the Polish Internal Security Agency in July 2004 [21]. It also organizes a highly respected annual conference under the auspices of NASK. The SECURE conference series, organized since 1997, brings together company and IT managers; specialists in information system, network, and database security; and telecommunications and data network users who are interested in security issues. Co-sponsored by ISSE (Information Security Solutions Europe), ENISA (European Network and Information Security Agency) and the Polish Ministry of the Interior and Administration, SECURE is Europe's largest conference on data communications safety [22].

### 5.3 CERT GOV PL

On 1 February 2008, the Internal Security Agency established the government's computer incident response team (CERT GOV PL). Its goals include ensuring and developing the ability of public administration units to defend themselves against cyber-threats, in particular against attacks on the infrastructure consisting of IT systems and networks, the disruption or destruction of which might to a large extent threaten the life and health of people, national heritage, and the environment, or result in considerable financial losses and disrupt the operation of the state.

The goals of the CERT GOV PL include [23]:

- Creating a policy concerning cyber-defense;
- Coordination of the information workflow among the above-mentioned entities with reference to cyber-threats;
- Detection and recognition of, and response to cyber-threats;
- International cooperation concerning cyber defense;
- Playing an oversight role in relation to all national institutions, organizations, and units within governmental departments concerning cyber-defense;

The main objectives of the CERT GOV PL are:

- Collecting information concerning the current security status and threats to the critical IT infrastructure;
- Responding to IT security incidents, in particular the ones concerning the national critical IT infrastructure;
- Post-incident computer forensics;
- Establishing the policy for defense of the cyberspace of the Republic of Poland;
- Training sessions and raising awareness of the topic;
- Consulting and advising with reference to cyber-security.

### 5.4 ARAKIS-Gov

In 2004, ARAKIS-gov, a distributed internet-based early-warning system developed and maintained by CERT Polska (NASK) in cooperation with the Information Security Department of the Polish Internal Security Agency, was accepted as the most important system for ensuring the protection of the Polish critical information infrastructure. The goal formulated for this project is to create a real early-warning system that can detect a new threat, analyze the exploit, and create a description of a new attack.[1] Therefore, data from various sources, such as firewalls, darknets, honeypots, and anti-virus systems are correlated in order to detect emerging threats against the Polish network (also, notably, against governmental institutions), to detect new attack patterns, to monitor differences between attacks observed in Poland and in other countries, to gather statistical data, and to aid in general incident-handling activities. ARAKIS also provides a public dashboard showing a snapshot of network activity observed by the system. In the form of a polar chart, the alerts as generated by the ARAKIS system over the last 24 hours are plotted [24].

### 5.5 PIONIER-CERT

This incident response service entity is responsible for incident-handling in an academic network environment. The main purpose of this initiative is to establish a single point of contact for all security incidents occurring in the constituency of PIONIER, which consists exclusively of Polish academic research institutions [25]. In order to assist system administrators in handling the technical and organizational aspects of incidents, the overall process of incident response is divided into three main stages: incident triage, incident co-ordination, and incident resolution. The incident resolution is performed in a very limited range, and is in fact limited to special cases with a potential significant impact on PIONIER's constituency. The actual range of activities in such cases may cover removing vulnerability, restoring a system that has been compromised, or providing direct technical support while collecting evidence where criminal prosecution or other disciplinary actions are being considered [26].

## 6 LAW AND LEGISLATION

Relevant legislation as concerns the protection of data and information in Poland consists of Articles 267 to 269 of the penal code. These three articles regulate the respective crimes of

- Unauthorized access to information (267);
- Destruction, alteration, deletion, or damaging of information (268);
- Destruction, alteration, deletion, or damaging of information with particular significance for national defense, transport safety, the operations of the government, or other state authority or local governments (269).

These crimes are defined as being of increasing gravity, and the punishments range from two, three, to eight years respectively [27].

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Tomasz Przda of the Polish Internal Security Agency, Michał Młotek of the Polish Ministry of Interior and Administration, and Krzysztof Silicki and Mirosław Maj of NASK/CERT Polska, who validated the content of this chapter.

## REFERENCES

1. Mieczyslaw, B., and Slawomir, P. (2005). Critical infrastructure protection: actions to be implemented shortly. In *ECN European CIIP Newsletter*, August/September 2005, Vol. 1, No. 2, p. 21ff, http://www.irriis.org/ecn/European%20CIIP%20Newsletter%20No%202.pdf.
2. https://www.oecd.org/dataoecd/9/38/1952799.pdf, 2008.
3. Elbzbieta Stefanczyk. *Polish Libraries in the Information Society*. http://www.svkbb.sk/colloquium/zbornik/data/stefanczyk.pps, 2008.
4. https://www.oecd.org/dataoecd/9/38/1952799.pdf, 2008.
5. http://merlin.obs.coe.int/show_iris_link.php?iris_link=2000-6:5&id=392, 2008.
6. Europäische Audiovisuelle Informationsstelle. http://merlin.obs.coe.int/iris/2001/10/article33.de.html, 2008.
7. http://www.itu.int/wsis/stocktaking/scripts/documents.asp?project=1103559107&lang=en, 2008.
8. Skulimowski, A. M. J. (2006). *The Information Society in Poland: Recent Developments and Future Perspectives*, http://www.scholze-simmel.at/starbus/r_d_ws1/poland.pdf, 2008.
9. https://www.oecd.org/dataoecd/9/38/1952799.pdf, 2008.
10. Marcin, P. (2004). Information society in Poland. A prospective analysis. Transformation, integration and globalization economic research. *Leon Kozminski Academy of Entrepreneurship and Management*. January 2004, Warsaw, http://www.tiger.edu.pl/onas/piatkowski/Information_Society_in_Poland_A_Prospective_Analysis.pdf.
11. Skulimowski, A. M. J., *The Information Society in Poland: Recent Developments and Future Perspectives*. http://www.scholze-simmel.at/starbus/r_d_ws1/poland.pdf, 2008.
12. http://www.foresight.polska2020.pl/mis/en, 2008.
13. http://www.egov.edu.pl, 2008.
14. http://www.eracareers-poland.gov.pl/page.html?kid=549:4620, 2008.
15. Skulimowski A. M., op. cit.
16. http://www.mswia.gov.pl/portal/en/3/63, 2008.
17. http://egov.edu.pl/?id=2&lang=2, 2008.

18. http://www.nask.pl/run/n/home, 2008.
19. http://www.cert.pl/index3.html?id=24, 2008.
20. Przemek, J. "All you wanted to know about CSIRTs but were afraid to ask". http://www.ceenet.org/workshops/lectures2005/Przemek_Jaroszewski/Ohrid_Day1.pdf, 2008.
21. Miros3aw, M. (2005). *CERT Polska and CIIP in Poland*, http://www.terena.org/activities/tf-csirt/meeting15/ciip-maj.pdf.
22. http://www.nask.pl/newsID/id/431, 2008.
23. Przemek J., op. cit.
24. http://arakis.cert.pl/en/index.html, 2008.
25. A precise list of PIONIER's constituency can be found on the website. http://arakis.cert.pl/en, 2008.
26. http://cert.pionier.gov.pl, 2008.
27. http://www.cybercrimelaw.net/laws/countries/poland.html, 2008.

# RUSSIA

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

During the last few years, Russia has made significant progress in improving its information infrastructure. The national security and economic welfare of the Russian Federation depends to a substantial degree on ensuring information security, a dependence that will increase in future with technological progress.

The information security is determined by the protection of national interests in the information field. The content of those interests can be inferred from the Information Security Doctrine of the Russian Federation and include the state's guarantee of human rights in the information field, IT support of the state policy of the Russian Federation, development of a domestic information industry, and the protection of information and of

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

information and communication systems in the various areas of public life. The critical sectors subject to critical information infrastructure protection are the following:[1]

- Economy,
- Domestic and Foreign Policy,
- Science and Technology,
- State Information and Communication Systems,
- Defense,
- Justice,
- Disaster Response.

The Information Security Doctrine of the Russian Federation reflects the G8 Okinawa Charter of the Global Information Society [1], which was prepared in the year 2000. However, in the Russian Information Security Doctrine, the specific social and economic circumstances and long-term reforms of the Russian Federation as well as its experience with terrorist attacks were taken into consideration.[1] In Russia, information assurance includes not only (technical) information security, but also the safeguarding of state secrets.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

In 2008, the president of the Russian Federation approved two documents, including Strategy for the Development of Information Society in Russia and Measures for Ensuring the Information Security of the Russian Federation in the Field of Information and Communication Systems use for International Information Exchange.

Earlier, the Russian government had approved the federal program The Development of United Information Environment for Education (2001–2005) (2001), the Concept for the Use of Information Technologies in the Federal State Organizations (2004), a federal program entitled Electronic Russia (2002–2010) (2005), and a federal program entitled National Technological Basics 2007–2011 (2007).[1]

### 2.1 Information Security Doctrine of the Russian Federation

The Information Security Doctrine [2] of the Russian Federation, adopted on 9 September 2000, is an extension of the National Security Concept [3] (approved by the President on 10 January 2000) intended to strengthen state policy regarding information security. Its aim is to help formulate legal, methodological, technical, and organizational provisions for information security in Russia and to assist the development of specific programs for this purpose. The doctrine defines the context of the nation's interests in the information sphere and assesses information threats to citizens, society, and the state. The doctrine is very comprehensive in scope and ranges over many policy areas, from data protection, personal privacy, copyright, and computer misuse (hacking) to state secrets, access to information, and the functioning of the media [4].

Russian information security is defined in the doctrine as "the state of protection of its national interests in the information sphere defined by the totality of balanced interests of

[1]Information provided by an expert.

the individual, society, and the state." Russia views both public opinion and the national information systems as integral parts of its concept of information security [5]. Moreover, the Russian government considers the uncontrolled spread of foreign media in Russia to be a threat to Russian information security and, as a result, intends to "strengthen" the Russian media [6].[2,3]

The doctrine is legally based on Russian federal laws on security, state secrets, the protection of information, and participation in international information exchange. The document is divided into four major chapters, covering 11 sections. The four main chapters are:

- *Information security.* This chapter defines the Russian Federation's national interests in the information sphere, referring to constitutional rights, to IT support for state policy, to the development of the information industry, and to the security of information against unauthorized access. Moreover, internal and external sources of threats to Russia's information security are identified. The doctrine acknowledges frankly that just like private monopolies and organized crime, government policy and legislation can also pose a threat. Aggressive foreign corporations and international terrorists are mentioned as major foreign threats. In the domestic arena, the critical state of the national industry as well as the under-development of the legal framework can constitute a barrier to full exploitation of information technology, particularly where e-commerce is concerned. Finally, the chapter discusses the state of information security in the Russian Federation and objectives for amending it. The deteriorating safety of data constituting state secrets is identified as a major problem;
- *Methods of ensuring information security.* This chapter covers legal, organizational-technical, and economic methods for information security. Moreover, it describes a number of features of information security in various spheres, such as the economy, domestic policy, foreign policy, science and technology, information and telecommunication systems, defense, law enforcement, and emergency situations. Finally, it mentions international cooperation in the field of information security such as banning information warfare, supporting information exchanges, coordinating law enforcement activities, and preventing unsanctioned access to confidential information;
- *The main provisions of the state policy for ensuring information security, and priority measures for implementing it.* This chapter lays out—at a high level of abstraction—the policy of the government, ranging from observing the constitution to supporting the development of new technologies. The chapter suggests provisions for information security, such as developing guidelines for federal institutions. In addition, the document mentions priority measures for implementing the rule of law, an increase in the efficiency of state leadership, programs providing access to information archives, educational measures, and a system for harmonizing standards in the field of computerization and information security are mentioned;

[2]This aspect of Putin's doctrine has been criticized by journalists, who fear restrictions on freedom of opinion and speech.

[3]The Information Security Doctrine claims to protect the interests of the individual, society, and the state in the information sphere. In fact, however, the main focus lies on the government's and society's interests in this field, and the document stresses the possible external threats to information security coming from abroad. Among these, the document mentions the dominance of certain states in the information sphere, foreign policy issues in the economic, military, and intelligence fields, and the exclusion of Russia from the information market by other states.

- *Organizational basis of ensuring information security.* This chapter describes the functions of the system of information security, as well as the organizational elements and actors of Russia's information security system, including the president, the Federation Council of the Federal Assembly, the State Duma of the Federal Assembly, the government of the Russian Federation, the Security Council, and other federal executive authorities, presidential commissions, judiciary institutions, public associations, and citizens.

An area of obvious emphasis is the creation of a legal base for information security. The laws on the Constitution of the Russian Federation, State Secrecy, Information, Computerization, and Information Protection, Participation in International Information Exchange, and Essentials of Legislation of the Russian Federation on the Archive Collection of the Russian Federation and Archives are specifically mentioned. Legal instruments constitute one of three approaches to information security mentioned in the doctrine—the other two being organizational-technical and economic measures. Furthermore, the document stresses the threat of attacks against Russia's information infrastructure and the threat of foreign governments using information warfare techniques against Russia. In addition, special attention is given to the development of telecommunication systems, the integrity of information resources, space-based reconnaissance, and electronic-warfare facilities [7].

## 2.2 Electronic Russia

The idea of Electronic Russia [8] appeared in early 2001, when the Ministry of Economic Development and Trade was elaborating a strategic development plan for Russia up to the year 2010. The program is based on the notion that in order to reduce the country's economic lag, it is necessary to develop the hi-tech sector, where it would be possible to reach a higher productivity level than in the raw-materials sector. None of this would be possible without computers and powerful ICT [9].[4]

Involving various ministries[5] and coordinated by the Ministry of Telecommunications and Informatization (which became the Ministry of Information Technologies and Communication in 2004), Electronic Russia 2002–2010 is the core IT program that will lay the groundwork for a more efficient economy and public administration through mass implementation of information and telecommunications technology [10]. It is also designed to facilitate by technological means the advancement of civil institutions by

[4]All cities in Russia with populations over 30,000 should soon be connected to the country's "fiber-optic backbone", although the connections to individual homes and offices can still be relatively primitive. Many thousands of villages in Russia still do not have a single telephone line, so it will be many years before some of the more sparsely populated areas can hope to have a fully operational telecommunications infrastructure. Many options are under consideration to provide this infrastructure, including satellite delivery. The Electronic Russia plan seeks to deliver an increasing number of government services online, and to alleviate some of the heavy bureaucratic burden on Russia's citizens and businesses. It will then be possible to perform tasks such as tax filing and business registration online. The country's vast geographic area and the financial difficulties of the education system have encouraged Russian planners to seek creative solutions to the provision of education throughout the country. The delivery of a wide range of distance-learning packages via the internet is seen as a potentially effective solution to this problem, which the Electronic Russia plan seeks to explore.

[5]Ministry of Economic Development and Trade, Ministry of Education, Ministry of Industry, Science and Technologies, Aviation and Space Agency, Federal Agency of Government Communications and Information with the President, Agency on Systems Management.

securing the right of citizens to unrestricted information access, and by expanding IT training opportunities for specialists and qualified users [11].

Electronic Russia has a nine-year planning horizon and addresses four key areas:

- Regulatory environment and institutional framework;
- Internet infrastructure;
- e-Government;
- e-Education.

The main objective of Electronic Russia is to increase the efficiency of the economy, to improve management in the public sector, and to enhance self-government by applying information and communication technologies. In order to reach this goal, the following tasks are addressed:

- To create effective legislation governing ICT;
- To ensure open communication and interaction between the state bodies, agencies, and companies by applying state-of-the-art ICT technologies;
- To create conditions for more extensive and more effective use of ICT in the economic and social spheres;
- To provide up-to-date computer training for professionals;
- To create incentives for the development of an independent press and media by employing ICT in their professional activities;
- To develop the infrastructure of telecommunication networks, as well as access to electronic libraries, archives, databases of scientific and technical information for citizens, state-owned organizations, and educational institutions;
- To support the establishment of e-commerce for state procurement and other commercial activities of the state [12].

In 2006, the government of the Russian Federation modified some of the aims and tasks of this program. The main aim of the Electronic Russia program has initially been restricted to increasing the quality of the public administration through implementation of information and telecommunications technology in government bodies, in order to increase the skills of the state employees in their use of IT and the quality of the state's services for citizens. Now Electronic Russia has a four-year planning horizon and addresses mainly e-Government issues.

The main objective of Electronic Russia is to increase the efficiency of management in the public sector by applying information and communication technologies. In order to reach this goal, the following tasks are addressed:

- Formulating standards and proposals related to the use of information and communication technologies in state governance;
- Providing for effective interaction between different bodies through information and communication technologies and integration of the state information systems;
- Providing for effective interaction between the state authorities, citizens, and organizations through information and communication technologies;
- Application of the information systems to control the activities of state authorities;

- Creation of software and technical solutions to support the activities of state authorities;
- Monitoring the program's implementation.

One of the regional branches of the Electronic Russia Program is the city program Electronic Moscow [13]. This program, announced on 24 December 2002, aims to strengthen Moscow's role as the information industry center of Russia. The program is based on the city's powerful telecommunication infrastructure—the Moscow Fiber Optic Network. The issues addressed by e-Moscow include the creation of a normative and legal basis for the information society; a more efficient city management, based on e-Government; developing the urban economy and overcoming information inequality within the city; building an interoperability framework; and integrating all existing ICT projects of the municipal authorities [14].

### 2.3 International Cooperation

International cooperation is an important component of the Russian Federation's efforts in the field of ensuring information security. Russia's international cooperation in ensuring information security has two distinctive features: International competition for technological and information resources and for dominance in the markets has increased, and the world's leading economies have achieved a growing technological lead that allows them to build up their potential for information warfare. Russia views this development with concern, as it could lead to a new arms race in the information sphere and raises the threat of foreign intelligence services penetrating Russia through technical means, such as a global information infrastructure. Therefore, the main areas of the Russian Federation's international cooperation in the field of information security are: [15]

- Banning the development, proliferation, and application of instruments of information warfare;
- Ensuring the security of international information exchange, including the security of information being transmitted via national telecommunications channels;
- Coordinating the activities of law-enforcement bodies worldwide for preventing computer crime;
- Preventing unauthorized access to confidential information in international banks, telecommunications networks, and information support systems that are indispensable for maintaining global trade; and sharing information with international law-enforcement organizations fighting transnational organized crime, international terrorism, the spread of narcotics and psychotropic substances, the illegal trade in arms and fissile materials, and human trafficking;
- Active participation of Russia in all international organizations active in the field of information security, including standardization and certification.

In accordance with UN General Assembly Resolution No. 58/32 of 8 December 2003, a group of government experts on international information security was organized, chaired by a Russian representative [16]. The group of government experts includes representatives of 15 countries.[6] Furthermore, the Russian government has special

[6]United Kingdom, China, Russia, France, Belarus, Brazil, Germany, India, Jordan, Malaysia, Mali, Mexico, South Korea, and South Africa.

partnerships with the state members of the Shanghai Cooperation Organization (SCO)[7] and with the state members of the Collective Security Treaty Organization (CSTO)[8] in the sphere of information security.

## 3 ORGANIZATIONAL OVERVIEW

The main organizations responsible for information security in Russia are the Security Council of the Russian Federation, the Federal Security Service of the Russian Federation (FSB), the Federal Guard Service of the Russian Federation, the Federal Technical and Export Control Service, and the Ministry of Information Technologies and Communications.

As far as public-private partnerships are concerned, the Russian Association of Networks and Services (RANS) strives to contribute to the development of norms for the implementation and use of secure IT, while PRIOR, as a national public initiative, aims at uniting public, private, and non-profit organizations directed at developing the Russian Information Society.

### 3.1 Public Agencies

***3.1.1 Security Council of the Russian Federation.*** The Security Council of the Russian Federation [17] is appointed by the president in accordance with the constitution and the Federal Law on Security. It is responsible for ascertaining Russia's national interests related to information and defines information resources that must be defended. The Security Council defines conceptual approaches to national security [3]. It drafts policy proposals on defending the vital interests of individuals, society, and the state against internal or external threats. The Security Council also coordinates the elaboration of a strategy for the Russian Federation's information security, and helps the president to carry out his constitutional duties in defending human and civil rights, as well as Russia's sovereignty, independence, and territorial integrity [18].

***3.1.2 Federal Security Service of the Russian Federation (FSB).*** According to its statute, the FSB [19] is a federal agency of the executive branch of government with a mandate to safeguard the security of the Russian Federation. This includes defending and protecting the state borders of the Russian Federation, as well as its internal waterways, territorial waters, exclusive economic zone, and continental shelf and their natural resources, and safeguarding the information security and the main areas of activity of agencies of the Federal Security Service, as defined in the laws of the Russian Federation [20].[9]

As far as technical support is concerned, the FSB has its own research institute specializing in information technologies. It carries out technical information assessments, particularly regarding criminal cases [20]. It is also responsible for tracking cases of cyber-terrorism [21]. The FSB Computer and Information Security Directorate

[7]In addition to Russia, these include: China, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.
[8]In addition to Russia, these include: Armenia, Belarus, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan.
[9]Text of the "Statute on the Federal Security Service of the Russian Federation and Structure of the Federal Security Service Agencies". Approved by presidential edict no. 960 of 11 August 2003, signed by V. Putin, President of Russian Federation.

(Directorate-R) was established in October 1998. The Directorate's main tasks are counterintelligence and the fight against cyber-crime. Since undergoing a minor reform in September 2004, the FSB has a changed structure. The Computer and Information Security Directorate is part of its counterintelligence service [22].

Among the fundamental objectives of the FSB in the field of information security are the planning and implementation of state and scientific-technical policy in the sphere of information security; the organization of support for the cryptographic and technical engineering security of information and telecommunications systems; and protecting state secrets as well as systems of encrypted, classified, and other special types of communications in the Russian Federation and in its institutions abroad. Another function is to certify equipment for the protection of information, telecommunications systems, and networks, as well as technical devices for the detection of electronic surveillance in buildings and technical equipment, in accordance with federal law. Moreover, it certifies special technical equipment for the covert collection of information and technical equipment to safeguard the security and (or) protection of information, and defines the basic guidelines of the activity of the agencies of the Federal Security Service in these areas. Finally, it regulates the development, production, sale, use, export, and import of encryption (cryptographic) equipment, telecommunications systems, and networks protected by encryption systems [23].

***3.1.3 Federal Guard Service of the Russian Federation.*** According to its statute, the Federal Guard Service of the Russian Federation is a federal body of the executive branch of government with a public mandate to shape state politics and legal regulations, as well as to conduct monitoring and surveillance to ensure the safety of the president of the Russian Federation, the chairman of the government of the Russian Federation, and other important public figures. An additional structure—the Special Communication and Information Service—was added in August 2004 as a result of the administration reform of the Federal Guard Service of the Russian Federation [24].

Until 2004, the Federal Agency for Government Communications and Information (FAPSI) [25] was the main responsible body for information security. FAPSI was abolished in 2003 and its functions distributed between the Federal Security Service (FSB) and the Federal Guard Service of the Russian Federation. FAPSI was responsible for ensuring the security of communications [26]; the cryptographic and technical security of encrypted communications; intelligence-gathering activities; and providing information to higher bodies of authority. The agency also fought domestic criminals, foreign intelligence services, and engaged in other forms of information warfare; and it monitored information security in the financial sector. FAPSI was a strategic asset and oversaw information security on this level for the Russian Federation. It developed the technological basis not only for the country's administrative system, but also for the command-and-control system of the armed forces [27].

***3.1.4 Federal Technical and Export Control Service.*** The Federal Technical and Export Control Service was formed in August 2004.[10] The Federal Technical and Export Control Service's activities are guided by the president of the Russian Federation and come under the jurisdiction of the Ministry of Defense. The Federal Technical and Export Control Service is an executive body dealing with the following issues:

[10]Edict no. 314" of the president of the Russian Federation of 9 March 2004 on the System and Structure of Federal Executive Bodies.

- Ensuring information security in ICT systems that are important for the state's and society's security;
- Countering foreign technical espionage on the territory of the Russian Federation;
- Ensuring the protection of the state's classified information and other data by restricting access and preventing technical leaks and unauthorized access;
- Export control.

***3.1.5 Ministry of Information Technologies and Communications.*** The Ministry of Information Technologies and Communications is a branch of the federal government that implements state policy and oversight in the telecommunications sector. Among many other tasks, the ministry, together with other parts of the federal government, takes measures aimed at the restoration of the information and communication networks of the Russian Federation in emergency situations. It develops and implements a scientific-technical strategy for information security. The ministry also coordinates efforts to develop the national IT infrastructure [28].

## 3.2 Public-Private Partnerships

For many years, information security problems in Russia were only studied and addressed in a timely fashion for the protection of state secrets in military, governmental, or other state-related automated systems. Thus, over time, a situation developed in which very specific commercial-sector problems went unresolved because of the absence of such a sector [29]. At present, the development of commercial IT security products in the Russian market is prospering, yet it is sometimes limited by financial restrictions and the shortage of IT specialists.

Genuine public-private co-operation in the field of information security remains rather limited when compared to efforts in other countries. This is a result of the fact that for many (especially small and medium-sized) businesses in Russia, information assurance is not the most pressing problem. But both sides—private and public—are currently changing their stance, making more cooperation a much likelier prospect [30].

***3.2.1 Russian Association of Networks and Services (RANS).*** The Russian Association of Networks and Services (RANS) [31] is a public and governmental organization. RANS is developing norms and legal documents for the implementation and use of secure IT. The establishment of RANS was initiated by the Ministry for Information Technologies and Communications of the Russian Federation in 1994. At present, RANS has 122 members from all over Russia including universities, scientific institutions, ministries, legal and insurance companies, operators, ISPs, vendors, and users. RANS has several committees and workgroups on main topics covering the internet, security and privacy, wireless communications, education and training, and IP telephony. One of its working groups monitors standards.

The main activities of RANS are: [32]

- Assisting the development of the internet in Russia;
- Establishing a predictable, informative, non-contradictory, and clear legal environment for internet activities;
- Creating and realizing projects and programs aimed at the development of networks, systems of data transmission, telematic services, and information safety;

- Integration and coordination of the interests of users, producers, and operators of information and telecommunication systems;
- Integration of Russian information and telecommunication systems into the European and global infrastructure;
- Organization of conferences and exhibitions; publishing activities, and professional development.

In the sphere of information security, the program of RANS covers: [33][11]

- The creation and development of the PKI and information security concept in Russia;
- The preparation of a draft law on electronic digital signatures;
- The preparation of proposals in co-operation with the Ministry for Internal Affairs for the prevention of illegal activities in the telecommunication networks;
- Creating a hierarchical PKI Infrastructure, managed by the Federal Cryptographic Body.

***3.2.2 PRIOR.*** PRIOR [34] is a national public initiative that unites public, private, and non-profit organizations. Through its activities, this initiative aims to supplement the existing state and non-governmental programs and projects directed at developing an Information Society and a knowledge economy in Russia. PRIOR recognizes the importance of participating in the major development programs, including those of the state. These include the Federal Program Electronic Russia for the Years 2002–2010, the municipal program Electronic Moscow, the program Electronic Saint Petersburg, and others.

PRIOR's major project is creating the Russia Development Gateway [34], which is envisioned as an environment for partner interaction and collaboration to reach common goals as well as a means of integrating expert knowledge in the development field. It is an unprecedented coalition of equal partners instead of the traditional Russian hierarchical system.

PRIOR is a volunteer association of organizations and individuals who have pooled their efforts and resources in order to provide mutual informational, technological, consulting, financial, organizational, and other types of support to reach common goals. These goals include e-Governance, e-Business, the networked society, distance learning, digital libraries, and strengthening international, national, and local projects and initiatives through effective dissemination of best practice knowledge and experience.

Among others, PRIOR's aims are: [34]

- To assist in developing the legal base of the Information Society, the infrastructure of information processing, and communications channels;
- To serve as an effective national system for applying innovations;
- To educate and train qualified knowledge workers;
- To provide relevant local information content and services;
- To establish a unified methodological and terminological base regarding the Information Society and the knowledge economy;

[11]Other major projects are in the fields of telecommunications, e-business, and education and training.

- To give Russian users access to best-practice solutions and know-how and to assist in the implementation of partnership-based programs and projects aimed at development through ICT.

## 4 EARLY WARNING AND PUBLIC OUTREACH

The Russian Information Security Doctrine mentions the development of some early-warning mechanisms: "In these specific conditions, information security is ensured, among other things, by developing an effective system of monitoring critical objects whose malfunction may give rise to emergency situations and prediction of emergency situations" [35].

### 4.1 Russian Computer Emergency Response Team (RU-CERT)

The Russian Computer Emergency Response Team (RU-CERT) [36] was founded in 1998 and is maintained by the Russian Institute for Public Networks (RIPN) [37]. RU-CERT is part of the RBNet Network Operation Center (NOC) [38]. RBNet was established to provide internet services for science and high school communities in Russia. RBNet is a project funded by the Russian government under the responsibility of the RIPN.

RU-CERT provides computer-incident prevention and response services for RBNET users. The initial goal of the RU-CERT project was the coordination of efforts in the Greater Moscow area in their fight against hackers, primarily "script kiddies" who used stolen dial-up passwords and caused considerable material damage. However, it quickly became clear that service providers prefer to solve all problems independently and hide the results of their anti-hacker efforts from the public. It was subsequently decided to change the scope of its activity and to create an organization like the US CERT for Russia.

### 4.2 Governmental Scientific Support

One of the important factors determining the state outreach policy in the field of the ensuring information security is scientific support. The coordination of the activities of Russian scientific organizations in this field has been entrusted on the Institute Information Security Issues (IISI) [39] of the Moscow State University and the Academy of Cryptography of the Russian Federation (which deals with technical aspects of such problems).

## 5 LAW AND LEGISLATION

The legal framework for information security in Russia includes three main parts: the legal insurance of information security, the legal insurance of the security of information infrastructure and the legal insurance of the legal status of the information security's subjects.

The legal framework for information security is based on the Law of the Russian Federation on Mass Media, the Federal Law on Advertising, the Federal Law on Countering Extremist Activity, the Federal Law on Political Parties, the Code of Administrative

Offences of the Russian Federation. It is also governed by a number of other legal acts such as the Law of the Russian Federation On State Secrets [40], the Basic Principles of the Legislation of the Russian Federation on the Archive Fund of the Russian Federation and Archives [41], and the Federal Laws On Information, Informatization and Information Protection [42], which focus mainly on the use of information resources, information access rights, and information protection in the sense of preventing unauthorized access to documented information that may cause damage to government bodies or any other holder of information resources. Moreover, the Law of the Russian Federation on Legal Protection of Computer Programs and Databases [43] protects the content of computer programs and databases.

The legal framework for the security of information infrastructure is based on the Federal Law on Communications [44], which also covers communication network management in emergencies [45]. A number of other laws [46] have been adopted, and work has begun on implementing them and preparing draft laws regulating social relations in the information sphere [15]. The government hopes that the new federal Electronic Digital Signature (EDS) Law [47] will serve as a tool for regulating the field of information security. The law provides for recognizing the EDS as being legally equivalent to a physical personal signature. Specifically, the EDS Law protects the rights of persons who use EDS in their electronic data exchange. As part of enforcing this law, the government has been working to put into place a network of EDS authentication centers that will help enforce the law and derive regulations. The new Russian Law on Technical Regulation [48] also offers a new definition of the concept of security [49]. It states that "security is a condition in which intolerable risk of harm is absent". Furthermore, Article 7 of this law states that "technical regulations taking into account the degree of risk of harm establish minimum necessary requirements for ensuring, among others, electrical security."[12]

The legal provision on the status of the subjects of information security is based on the Constitution of the Russian Federation, the Criminal Code of the Russian Federation, the Law of the Russian Federation on Mass Media, and other legal acts that consolidate norms ensuring the rights of citizens, organizations, and state bodies in their information-related activities.

### 5.1 Russian Criminal Code 1996/2004

The number of cyber-attacks against enterprises, organizations, and citizens is growing at a stable pace. According to information from the Main Administration for Special Technical Measures of the Russian Ministry of Internal Affairs, the number of computer-related crimes committed in Russia has increased by almost 150 per cent over the previous years [50].

The Russian Criminal Code of 1996 (revised in 2004) provides for the punishment of the following crimes related to breaches of computer security: [51] Unlawful access to lawfully protected computer information; development of computer programs or introduction of changes into existing computer programs that are known to lead to unsanctioned destruction, blocking, modification, or copying of information; disruption of the operation of the computer, the computer system, or its networks, and likewise the use or

[12]Interestingly, before 2003, documents issued by Russian state organizations on information security did not include the word "risk".

dissemination of such programs or discs containing such programs; and violation of the rules of use of a computer, computer system, or network by a person having access to this computer, computer system, or network.

The Criminal Code of the Russian Federation now includes articles establishing penalties for types of crimes that had not been defined previously. Chapter 28 of the code, Crimes in the Computer Information Sphere, consists of three articles outlining the penalties for unlawful access to computer information (Article 272); for the creation, use, and dissemination of malicious computer programs (Article 273); and for violations of rules for the operation of computers, computer systems, and networks (Article 274) [52].

## ACKNOWLEDGMENT

We acknowledge the contribution of the expert, Anatoly Streltsov of Lomonosov Moscow State University, who validated the content of this chapter.

## REFERENCES

1. G8 Information Center. (2008)*Okinawa Charter on Global Information Society*, Okinawa, (22 July 2000), http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm.
2. Putin. V. (2000). Russian Federation. *Doctrine of the Information Security of the Russian Federation*, No. Pr-1895. http://www.medialaw.ru/e_pages/laws/project/d2-4.htm.
3. http://www.kremlin.ru/eng/articles/institut04.shtml, 2008.
4. Leigh, I. (no date). *Information Security Doctrine of the Russian Federation*, http://www.isn.ethz.ch/news/dossier/ssg/pubs/books/FluriSulakshin/05A_LEIGH.pdf.
5. Timothy, L. T. (2001). *Information Security Thinking: A Comparison of U.S., Russian and Chinese Concepts*, http://fmso.leavenworth.army.mil/documents/infosecu.htm, 2008.
6. (a) Albats, Y. (2000). Information security doctrine redux. In *The Moscow Times*, Maxine Maters, Moscow. http://internal.moscowtimes.ru/doc/about/index.html; (b) GeoPowers (2000). *Sicherheitskonzept Russland: Wunschdenken?* http://www.geopowers.com/Machte/Russland/russland.html, 2008.
7. Timothy, L. T. (2001). op. cit.
8. Federal Target Program. (2002). *Electronic Russia (years 2002–2010)*, approved by the government of the Russian Federation (Decree No. 65 of 28 January 2002). http://old.developmentgateway.org/download/182707/erussia_final_en_jr28-02.doc, 2008.
9. Hohlov, Y. Institute of the Information Society (2005). *E-Russia Program for 2002–2010*, State of the Art October 2005, http://www.tedbr.com/apresentacoes/e-Brasil/e-russia_and_e-moscow_programs_2005-10-14.pdf, and http://www.e-rus.ru, 2008.
10. http://www.uni-koblenz.de/~kgt/PM/SemB/Russland.ppt, 2008.
11. http://www.bisnis.doc.gov/bisnis/bisdoc/011001E-Russia.htm, 2008.
12. Federal Target Program. (2002). *Electronic Russia*, op. cit., p. 3f.
13. http://mgd.iis.ru, 2008.
14. (a) Filippov S. (2004). *Policy for ICT Adoption in Moscow, Electronic Moscow Programme*, http://i-policy.typepad.com/informationpolicy/2004/09/policy_for_ict_.html; (b) Hohlov, Y. Institute of the Information Society (2005). *e-Moscow Program for 2003–2007*, State of the Art October 2005, http://www.tedbr.com/apresentacoes/e-Brasil/e-russia_and_e-moscow_programs_2005-10-14.pdf, 2008.

15. http://www.medialaw.ru/e-index.html, 2008.
16. Kremer, A. (2004). *Cyber security in Russia*. Presentation held at ITU-T Cybersecurity Symposium, Florianopolis, Brazil, 4th October 2004, http://www.itu.int/ITU-T/worksem/cybersecurity/presentations/CsecS2-p2-kremer.ppt, 2008.
17. http://www.scrf.gov.ru, 2008.
18. http://www.fas.org/irp/world/russia/docs/edict_1024.htm, 2008.
19. http://www.fsb.ru, 2008.
20. http://www.fas.org/irp/world/russia/fsb/statute.html, 2008.
21. http://www.russia-gateway.ru/content/NEWS/NewsItem_2376921.jsp, 2008.
22. http://www.agentura.ru/english/dosie/fsb/structure; http://www.agentura.ru/english/press/about/jointprojects/mn/fsbreform, 2008.
23. Putin. V. (2003). Russian Federation. *Statute on the Federal Security Service of the Russian Federation*, op. cit.
24. Decree of the President of the Russian Federation No. 1013 of 7 August 2004. *Issues of the Federal Guard Service of the Russian Federation* (2005). (with Amendments and Additions of 28 December 2004, 22 March and 1/6 October 2005). http://egarant.park.ru/rubric.jsp?urn=2622189142 (registration required), 2008.
25. http://www.agentura.ru/english/dosie/brit/fapsi, 2008.
26. http://www.shaneland.co.uk/ewar/docs/dissertationsources/russiansource1.pdf, 2008.
27. http://www.fas.org/irp/world/russia/fapsi/index.html, 2008.
28. http://english.minsvyaz.ru/site.shtml?id=17&page=1, 2008.
29. Mikhail, B. Ignatyev, op. cit.
30. http://www.iis.ru/projects, 2008.
31. http://www.rans.ru/eng, 2008.
32. http://www.rans.ru/eng/directions, 2008.
33. http://www.rans.ru/eng/programs.
34. http://prior.russia-gateway.ru/en.
35. *Doctrine of the Information Security of the Russian Federation*, op. cit.
36. http://www.cert.ru/index_eng.html.
37. http://www.ripn.net:8080/en/index.html.
38. http://www.rbnet.ru/en/about_en.shtml.
39. http://www.iisi.msu.ru/GeneralEng.html.
40. http://www.medialaw.ru/laws/russian_laws/txt/8.htm.
41. http://www.rusarchives.ru/lows/zakon.shtml.
42. http://medialaw.ru/e_pages/laws/project/d2-4.htm.
43. http://www.russoft.org/docs/?doc=131.
44. http://www.medialaw.ru/e_pages/laws/russian/comm_eng/comm_1.html.
45. Council of Federation. (2003.) *Federal Law on Communications*, Adopted by the State Duma on June 18, 2003, Chapter 10, Articles 65–67 http://www.medialaw.ru/e_pages/laws/russian/communications.htm.
46. Further information: http://www.fas.org/irp/world/russia/docs/arf_p2.htm.
47. http://www.bakernet.com/NR/rdonlyres/996F168D-3FED-4EDB-B725-4E5E42B03E2F/28188/RussianElectronicDigitalSignatureLaw.pdf; and http://www.akdi.ru/gd/proekt/086086GD.SHTM.
48. http://www.cababstractsplus.org/google/abstract.asp?AcNo=20043101434, and http://www.aprok.ru/tecreg/chronicle.php.

49. http://books.nap.edu/openbook.php?record_id=10968&page=107.
50. http://www.mvdinform.ru/; Source: http://www.nap.edu/catalog.php?record_id=10968.
51. Further information: http://www.crime-research.org/analytics/Liability_for_computer_crime_in_Russia.
52. http://books.nap.edu/openbook.php?isbn=0309089719&page=102.

# SINGAPORE

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

New security threats that have emerged in the post-11 September 2001 era emphasized the need for closer cooperation between the military and homefront agencies in Singapore. Immediately after the attacks in the US in 2001, the homefront agencies undertook a review of the vulnerabilities and strengths of Singapore's national critical infrastructures from the following sectors:

- Banking and Finance,
- Information- and Telecommunications,
- Energy,
- Water,
- Transportation,
- Health [1].

Since 2002, the critical infrastructures of these six sectors have been reviewed and assessed, and remedial plans were implemented. However, infrastructure protection policies in Singapore are not limited to these sectors, but have been expanded to the following sectors:

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- Food supply,
- Aviation Security,
- Maritime Security.[1]

Even though these sectors have been at the focus of the most recent efforts to prevent terrorism, they do not represent the totality of Singapore's critical infrastructure. Other sectors may well be included in future protection efforts.

## 2 INITIATIVES AND POLICY

Singapore adopted the internet comparatively early. According to the Network Readiness Index by the World Economic Forum, Singapore was the most network-ready country in 2004–2005 [3]. In spring 2005, the Singaporean government presented a comprehensive "Infocomm Security Masterplan" for the years 2005–2007 that is part of the country's national security strategy to address cyber-security and cyber-terrorism [4].

### 2.1 National Emergency System (NEST)

Since the mid-1980s, Singapore has planned and developed its homefront preparedness efforts along the lines of a total defense concept. The Ministry of Home Affairs (MHA) has brought various ministries and emergency authorities together to integrate homeland preparedness plans. Since 2001, the MHA has boosted its efforts and developed a robust National Emergency System (NEST) for national security, while the Singapore Armed Forces are in charge of external defense. NEST is a comprehensive system encompassing civil security, civil defense, the provision of essential services, and the smooth operation of the economy during an emergency. It also ensures the provision of essential services and commodities such as water, power, health services, telecommunications, food, and fuel to the public [5].

### 2.2 National Critical Infrastructures Assurance (NCIA) Program

As announced in 2002 [6], the Singapore government has set up a National Critical Infrastructure Assurance (NCIA) project to carry out an in-depth assessment of the vulnerabilities of the nation's critical national infrastructures and of necessary measures to reduce these vulnerabilities. The project involves consultation and partnership between the government agencies and the private sector. The National Infocomm Security Committee (NISC) supports the NCIA program.

### 2.3 The Fight Against Terror—Singapore's National Security Strategy

In August 2004, the government's National Security Coordination Centre released a document entitled The Fight Against Terror—Singapore's National Security Strategy [7], according to which security standards in crucial areas such as aviation security, maritime security, land transport security, border control, and critical infrastructure protection have been raised in Singapore [8]. In response to terrorist attacks in the US

[1] Cf. [2].

and based on the recommendations of the National Critical Infrastructure Assurance Committee, Singapore has initiated several measures to protect its physical critical infrastructure and key installations, including prominent public places, power stations, and transportation and water supply networks [9].

### 2.4 Infocomm Security Masterplan

In response to cyber-threats such as hacking, virus attacks, and cyber-terrorism, the deputy prime minister announced the three-year Infocomm Security Masterplan (2005–2008) in February 2005. He said that as Singapore's economy would continue to rely heavily on ICT, securing the information and communication environment would be critical. The government would thus set aside S$38 million (about US$23 million) over the next three years to build capabilities in managing cyber-threats and enhancing the security of cyberspace.

The master plan was developed through a multi-agency effort led by the Infocomm Development Authority of Singapore (IDA) under the guidance of the National Infocomm Security Committee (NISC), and is the result of extensive private and public collaboration. Companies and government agencies provided feedback and input through surveys and focus group discussions [10]. It was discovered that businesses have difficulty formulating and complying with IT security policies and best practices, as they lack the necessary professionals and experience.

The Infocomm Security Masterplan has two main aims:

- To maintain a secure IT environment for the government, businesses, and individuals. This involves raising awareness of risks, cyber-threats, and appropriate security measures among internet users and businesses. Two planned key projects to secure these three sectors are the National Authentication Infrastructure, which will develop reliable and robust authentication means to curb identity theft and promote more secure e-services, and the Business Continuity Readiness Assessment Framework. They will measure the effectiveness of government agencies' business continuity plans;
- To defend Singapore's critical infrastructure from cyber-attacks. The master plan also outlines strategies to develop national capabilities, to enhance security technology research and development, and to improve the resilience of critical information infrastructure.

Finally, a Common Criteria Certification Scheme and a set of international standards on security are planned [11].

The Infocomm Security Masterplan 2005–2008 will be replaced by a new five-year master plan in 2008. The new plan will build on existing efforts and will perpetuate the collaborative approach to ensure information security in Singapore [12].

## 3 ORGANIZATIONAL OVERVIEW

The Infocomm Development Authority of Singapore (IDA) is the chief technology office of the Singapore government covering planning, policy formulation, regulation, and cooperation with the private sector in the field of ICT. The National Infocomm Security

Committee (NISC) and the Technology Crime Division (TCD) within the Singapore Police Forces also play important roles in the field of CIIP.

In addition, the government of Singapore has recognized the importance of public-private partnerships to secure critical information infrastructures. In his speech on the occasion on the launch of the Infocomm Security Masterplan, Peter Ho, the then chairman of the National Infocomm Security Committee, emphasized the need for collaboration: "The cyber-threat landscape is constantly changing. No single organization can deal with these changes alone. Instead, collaboration among infrastructure owners, operators and government must take place. This is because separately, each of us sees only a small part of the picture and may not comprehend the full scale of malicious activities involved" [13].

Accordingly, Singapore has implemented different initiatives to foster public-private collaboration in the field of information security. The second part of this section lists the most important among them with regard to the protection of critical information infrastructure.

### 3.1 Public Agencies

***3.1.1 Infocomm Development Authority of Singapore (IDA).*** IDA is a statutory board of the Singapore government that was formed in 1999 as the result of a merger between the National Computer Board (NCB) and the Telecommunications Authority of Singapore (TAS). The aim was to have a single agency for integrated planning, policy formulation, regulation, and industry development of the ICT sector.[2] IDA operates under the Ministry of Information, Communications, and the Arts (MICA).

Among IDA's main responsibilities are fostering a competitive IT industry in Singapore, preparing residents for living and working in the "New Economy", supporting the delivery of citizen-centric e-Government services, and building and operating the government's IT infrastructure [14]. IDA sets ICT standards and regulations and supports the private sector in implementing security measures.

IDA's Infocomm Security Division (iSec) plays a central role in establishing and implementing a solid IT security infrastructure for Singapore's national ICT infrastructures. iSec monitors the implementation of ICT security measures and practices for the whole public sector. Moreover, iSec conducts awareness-raising programs for the public and the private sector as well as individuals. For instance, in 2001, IDA initiated a year-long public-awareness campaign that aimed to educate users from the public and private sectors as well as the general public about safe computing practices [15].

***3.1.2 National Infocomm Security Committee (NISC).*** The National Infocomm Security Committee (NISC) was set up to formulate policies and strategic direction for cybersecurity at the national level. With members from various government agencies, it is a platform for the government to institutionalize considered policies and mandate strategic initiatives in IT security. It comprises representatives from the Ministry of Home Affairs, the Ministry of Defence; the Ministry of Information, Communication and the Arts; the Ministry of Finance; the DSO National Labs; and the Defence Science and Technology Agency (DSTA). IDA serves as the secretariat for this committee [16].

[2]Among other entities, IDA supports the Information Technology Standards Committee (ITSC), the National Trusts Council (NTC)—an industry-led council to build confidence in e-Commerce, and the Public Key Infrastructure (PKI) Forum Singapore.

***3.1.3 Technology Crime Division (TCD) within the Singapore Police Force.*** Within the Singapore Police Force (SPF), the Criminal Investigation Department (CID) is the primary investigation agency in Singapore for all criminal matters [17]. The Technology Crime Division (TCD) is part of the CID. TCD provides specialized investigative and forensic services in addition to training the entire police force in investigating high-tech crime. Its scope of operation goes beyond computer crime and includes traditional crimes committed with the use of technology, such as encrypted mobile devices, the internet, and even wireless platforms. In order to prepare the nation for crimes of the future, the approach adopted by TCD is also to build capabilities through research, alliance-building, and education [18].

### 3.2 Public Private Partnership

***3.2.1 Critical Infocomm Infrastructure Surety Assessment (CII-SA).*** The Critical Infocomm Infrastructure Surety Assessment project was established in 2006 to assess the security readiness of Singapore's critical information and communications infrastructure. The project is led by the IDA, and provides a platform for owners and operators of CII to work together and ascertain the adequacy of their protection measures [19].

***3.2.2 Information Technology Standards Committee (ITSC).*** Volunteer members from the industry, supported by the Productivity and Standards Board (PSB) and IDA, established the industry-led Information Technology Standards Committee (ITSC) [20] in 1990. It is a neutral platform for interested industry and government parties to convene to agree on technical standards. To this end, the ITSC organizes workshops and seminars on various topics.

***3.2.3 Governmentware Seminar.*** The annual Governmentware IT Security seminar series began in 1991. The seminars are organized by the IT Command of the Internal Security Department (ISD) of the Ministry of Home Affairs (MHA). Since 2002, the Institute of Public Administration and Management (IPAM) of the Civil Service College has been the MHA's organizing partner. The lectures are also open to an audience from outside the public sector. The first seminar, organized by ISD for civil service participants, was held in the wake of urgent concerns about virus attacks against the PCs of government users. The Governmentware seminars alert participants to the latest security threats posed by emerging technology and advanced hacking techniques. Private-sector IT security industry experts are invited to participate and share their knowledge [21].

## 4 EARLY-WARNING APPROACHES

### 4.1 Singapore Computer Emergency Response Team (SingCERT)

The Singapore Computer Emergency Response Team (SingCERT) [22] is responsible for the detection, resolution, and prevention of security-related incidents on the internet. SingCERT also issues advisories and alerts about incidents. It maintains a website and a hotline for reporting and dissemination of advisories. SingCERT was initially established in October 1997 as a program of IDA, in collaboration with the Centre for Internet Research at the National University of Singapore (NUS).

SingCERT provides the following services:

- Broadcasting alerts, advisories, and security patches;

- Promoting security awareness through security courses, seminars, and workshops;
- Collaborate with vendors or other CERTs to find solutions to security incidents.

SingCERT is also a founding member of the Asia Pacific Security Incident Response Coordination Working Group (APSIRC-WG). The APSIRC-WG is staffed by volunteers from the national Incident Response Teams (IRTs) of Japan, Korea, and Singapore and aims to promote collaboration with other international IRTs and security groupings, such as the Forum of Incident Response and Security Teams (FIRST). Furthermore, APSIRC-WG provides assistance to countries in the region that would like to establish their own IRTs [22].

### 4.2 National Cyberthreat Monitoring Centre (NCMC)

Under the Infocomm Security Masterplan, the National Cyberthreat Monitoring Centre (NCMC) as a national resource to safeguard Singapore's cybersecurity and to provide focused tracking of cyber-threats. Besides the round-the-clock monitoring of critical networks, the centre will provide regular in-depth analysis of cyber-threats by incorporating information from all available sources. The NCMC will provide latest trends in cyber-threats, allowing the authorities to better respond to, and even preempt future attacks [23].

## 5 LAW AND LEGISLATIVE ACTION

### 5.1 Computer Misuse Act 1993/1998

The Computer Misuse Act (CMA) was first enacted in 1993 and first amended in 1998. It is aimed at protecting computers, computer programs, and information stored in computers from unauthorized access, modification, use, or interception. The CMA also applies to any person, irrespective of physical location, who hacks into computers located in Singapore, and to any person in Singapore who hacks into computers outside Singapore.

The 1998 amendments also address newer forms of cyber-crime (such as Trojan horses, password trafficking, or denial-of-service attacks). The amended CMA also provides enhanced penalties for computer crimes proportionate to the potential and actual harm caused. The amendment gives the police the legal authority to gain access to computer material, including encrypted material [24].

### 5.2 Computer Misuse (Amendment) Act 2003

The amendment to the Computer Misuse Act in 2003 allows the minister to authorize any person or organization to take necessary measures to prevent or counter any threat to a computer system that can affect the national security, essential services, defense, or foreign relations of Singapore. This is part of the government's efforts to establish a robust defense against cyber-attacks.

As in many other countries, Singapore's essential and critical services such as water, electricity, gas, telecommunications, and transportation are increasingly dependent on computer networks and information systems. Terrorists and criminals can exploit this dependence. Any attack on the critical infrastructure and essential services will severely disrupt the economy and threaten the national security.

Furthermore, with an increasingly computer-literate population and widespread availability of user-friendly hacker tools, more people around the world now have the necessary skills to carry out cyber-attacks. Hackers and computer viruses can flood network connections, steal or tamper with information, and disrupt essential services.

Section 15A of the Computer Misuse Act allows the minister to authorize any person or organization to take necessary measures to prevent or counter any threat that may endanger the national security, essential services, defense, or foreign relations of Singapore. The new Section 15A would be invoked to deal with situations of an outright cyber-attack, or in cases where specific intelligence has been received of an imminent cyber-attack against Singapore's critical infrastructure.

The powers given to the minister under Section 15A may not be used indiscriminately. The measures are aimed at preventing or countering any threat to a computer or computer service, or to any class of computers or computer services. The powers would be invoked only to avert threats that may endanger national security and essential services, such as any service directly related to the communications infrastructure, the banking and finance sectors, and the defense and foreign relations of Singapore. The powers under the new Section 15A would not be invoked to prevent or investigate a criminal offence that does not threaten the national security or essential services. Singapore's security agencies will also be required to satisfy the minister that the cyber-threats are imminent before the powers provided by Section 15A can be invoked [25].

### 5.3 Electronic Transactions Act 1998

The Electronic Transactions Act (ETA) was enacted in 1998 to provide a legal infrastructure for electronic signatures and electronic records, and to ensure predictability and certainty for electronic contracts. The ETA establishes the supporting legal infrastructure for the Public Key Infrastructure (PKI). The ETA addresses the following issues:

- Commercial code for electronic commerce transactions;
- Use of electronic applications and licenses for the public sector;
- Liability of service providers;
- Provision for a PKI.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts of the Ministry of Home Affairs who validated the content of this chapter.

## REFERENCES

1. Kee, H. P. (2002). *Speech by Senior Minister of State for Law and Home Affairs at the Monoc Seminar*, 22 March 2002. Ministry of Home Affairs, Singapore, http://app3.mha.gov.sg/news_details.aspx?nid=876.

2. National Security Coordination Centre. (2004). *"The Fight Against Terror—Singapore's National Security Strategy"*. National Security Coordination Centre, pp. 47–51. http://app-stg.nscc.gov.sg/data/25fight-terror.pdf.
3. Costa, V. D. (2005). Singapore's internet policy. *Workshop on Internet Governance at the National Level*, 19 July 2005, Singapore. http://www.wgig.org/docs/Singapore%20Internet%20Policy%2019%20Jul%2005.ppt.
4. Yang, L. B. (2005). Keynote Address. *17th Annual FIRST Conference*, Singapore. http://www.mica.gov.sg/pressroom/press_050629.html.
5. Kee, H. P., op. cit.
6. Infocomm Development Authority of Singapore. (2002). *Asia-Pacific Conference on Cybercrime and Information Security*, 11–13 November 2002, Seoul, p. 15. http://www.unescap.org/icstd/cybercrime%20meeting/Presentations/Session%203%20-%20country%20and%20org.%20reports/Singapore/Singapore%20written%20report.doc.
7. *The Fight Against Terror*, op. cit.
8. National Security Coordination Centre. (2004). *The Fight Against Terror—Singapore's National Security Strategy*. National Security Coordination Centre, p. 12. http://app-stg.nscc.gov.sg/data/25fight-terror.pdf.
9. Acharya, A. (2004). *Defending Singapore's Vital Infrastructure Against Terrorism*. IDSS Commentaries. http://se1.isn.ch/serviceengine/FileContent?serviceID=PublishingHouse&fileid=1A3BA5E1-F1AA-226F-7CEC-C0096894A6ED&lng=en.
10. Ho P. (2005). Singapore's Strategy in Securing Cyberspace, *Keynote Address at the Infocomm Security Seminar 2005*, Singapore. http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21.
11. IDA (2005). Singapore Gears Up for Cyber Security. *Three-year Infocomm Security Masterplan Unveiled,* 22 February 2005, Singapore. http://www.ida.gov.sg/News%20and%20Events/20050712110643.aspx?getPagetype=20.
12. http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx, 2008.
13. Ho P. Singapore's Strategy in Securing Cyberspace, op. cit.
14. http://www.ida.gov.sg/About%20us/20060406102431.aspx, 2008.
15. *Asia-Pacific Conference on Cybercrime and Information Security*, op. cit.
16. IDA. Singapore Gears Up for Cyber Security, op. cit.
17. http://www.spf.gov.sg, 2008.
18. Leong C. (2008). Security Initiatives in the Computerisation of the Singapore Government. http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/13-Homeland-Security-Singapore_R2GVIV_0Z5RDZ-i34K-pR.htm.
19. iGov.Sg. *2006 Report on Singapore e-Government*, iGov.Sg, Singapore, p. 22. http://www.igov.gov.sg/NR/rdonlyres/0D5EE595-4D44-4B02-948C-07FB18239313/0/2006ReportonSporeeGov.pdf.
20. http://www.itsc.org.sg, 2008.
21. http://www.governmentware07.com/home.htm, 2008.
22. http://www.singcert.org.sg, 2008.
23. Yang, L. B. Keynote Address, op. cit.
24. http://www2.mha.gov.sg/mha/ibrowse.jsp?type=3&root=0&parent=0&cat=8, 2008.
25. http://www.mha.gov.sg/basic_content.aspx?pageid=52, 2008.

# SPAIN

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

For a long time, Spain's critical sectors had not been exhaustively defined by the Spanish government. On 7 May 2007, the State Security Secretariat approved the so-called National Plan for the Protection of the Critical Infrastructures (Plan Nacional de Protección de las Infraestructuras Críticas). This plan defines the critical infrastructures as "those installations, networks, services, physical equipment, and information technologies whose interruption or destruction would have a grave impact on the health, security, or economic wellbeing of the citizens or on the efficient functioning of the state institutions and of the public administration".[1] Moreover, the plan includes a list of 12 strategically critical sectors. These are:[2]

- Chemical Industry,
- Nuclear Industry,
- Investigative installations,
- Centers of Power,
- Space,
- Energy sector,
- Telecommunications,
- Transportation,
- Water supply,
- Alimentation,
- Financial Sector,
- Public Health.

[1]Information provided by an expert. Translation by the author.
[2]Information provided by an expert.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

On 12 June 2007, Congress in a plenary session unanimously urged the government to put together a catalog with an exhaustive list of the national critical infrastructures within six months [1]. This classified catalog was elaborated and now contains 3,500 critical installations all over Spain [2]. Moreover, the catalogue is designated to become the basis of information for the European Program for Critical Infrastructure Protection (EPCIP) and will be constantly updated.

The Department of the Interior's General Directorate for Infrastructures and Security Equipment (Dirección General de Infraestructuras y Material de la Seguridad) is tasked, among other responsibilities, with securing the information and communications systems and data systems [3].

## 2 PAST AND PRESENT INITIATIVES AND POLICY

The main Spanish initiatives and policies in the area of information infrastructure and security occur along a two-pronged strand and focus on the opportunities and positive challenges created by the current developments in information and communications technologies.

### 2.1 Information Society Action Plan

In 1999, the Spanish government launched a strategic initiative for the development of the Information Society corresponding to the insight that Spanish society and the country's economy as a whole would benefit from the capacity to adopt the Information Society's technological innovations and to exploit the opportunities thus created.

The very first step of this initiative was the adoption of INFO XXI: La Sociedad de la Inform@ción para todos[3] in January 2000, a project that aims at building the Information Society of Spain. It consists of several structured programs and action steps to help stimulate the development of the Information Society in Spain. The first Action Plan INFO XXI (2000–2003) intends to establish the coordination of public administration initiatives by achieving three major objectives [5]:

- To stimulate the telecommunications and information technologies sector and complete the liberalization process within this sector by fostering competition;
- To enhance e-Government;
- To foster inclusive access to the Information Society.

In July 2003, the successor plan for the further development of the Information Society, called España.es, was adopted by the Spanish government to replace the INFO XXI plan. Covering the two-year period of 2004–2005, it is partly based on the recommendations of an expert commission on the Information Society and pursues two main objectives: to stimulate Information Society services in the population and to improve the infrastructure, contents, and services. The three strategic axes of the new action plan are as follows [6]:

- To foster the availability of contents and services that are most likely to stimulate demand;

[3]This document is accessible in its entirety [4].

- To improve the accessibility of Information Society services in the broadest sense, by offering public access points and developing training and communication;
- To connect small and medium-sized enterprises to enable them to fully take advantage of the benefits of e-Business.

To deliver on these objectives, the plan comprises six areas of action divided into two categories: vertical actions targeting specific segments of society such as the public sector (administración.es), education (educación.es), or small and medium-sized enterprises (pyme.es), and horizontal actions covering the whole population, accessibility and inclusion (navega.es), contents (contenidos.es), and communication and marketing (comunicación.es) [7].

In November 2005, the Spanish cabinet adopted the latest successor plan, the so-called Plan Avanza, which forms part of a broader program, Ingenido2010. The latter is aimed at giving new impetus to research and development investment in Spain. Plan Avanza focuses in particular on the investments needed for the ongoing development of the Information Society [8]. Plan Avanza has three major domains of activity including digital citizenship, small and medium-sized enterprises, and local entities. The element of information and communications security within all three domains is the jointly maintained anti-virus early-warning center (Centro de Alerta Temprana sobre Virus y Seguridad Informática) [9].

### 2.2 E-Government Action Plan

Jointly launched in 2003 by the Ministries of Science and Technology and of Public Administration, the Spanish e-Government action plan initially had the objective to enhance the drive towards electronic public services with a "short sharp shock". Therefore, a bunch of measures was implemented organized around the following four strategic areas [10]:

- Facilitating access to electronic services for all citizens (with the introduction of the electronic ID card, and the development of public access points to the internet);
- Developing interactive and transactional services that meet users' needs in terms of need, accessibility, and sophistication (starting with the improvement of the central e-government portal administracion.es);
- Enabling data and information interchange between administrations, both at the central level and with regional and local administrations;
- Supporting the internal change and re-engineering efforts of public administrations (coordination of developments, technical assistance, and reorganization of supporting structures).

In October 2004, this plan was updated to become the Public Administration Technological Modernization Plan 2004–2007 aiming to "connect administrations and connect people" while reducing bureaucracy, simplifying procedures, and eliminating unjustified delays [11]. Therefore, an electronic system for the secure interchange of data between administrations was to be put in place. In January 2006, the national e-Government initiatives were once again updated to boost the transition of the country's national public administration into cyberspace by offering a full range of on-line services

to Spanish citizens. A new new key element of the latest plan, called MODERNIZA, is a wide-ranging law on e-Government (see the chapter on Law and Legislation). MODERNIZA covers the period from 2006 to 2008 and consists of 16 measures to be implemented with the aim of achieving a huge step towards e-Government in Spain. The new law, for example, establishes citizens' electronic access to all public administration services and their right to submit electronic documents and signatures for official purposes. Other measures in the action plan repeated earlier calls for the distribution of electronic ID cards, the online availability of 800 new administrative forms, the conversion of 100 services to cyberspace, and a progressive introduction of electronic payment of public fees and royalties. The government is also creating an integrated network of information points and a single one-stop-shop web portal service for citizens to replace more than 500 different websites.

## 3 ORGANIZATIONAL OVERVIEW

The various aspects of Spanish critical information infrastructure policies mainly come under the auspices of the Ministry of Industry, Tourism, and Trade; the Ministry for Public Administration; and the Ministry of the Interior.

There are two State Secretariats under the administration of the Spanish Ministry of Industry, Tourism, and Trade: the State Secretariat of Tourism and Trade and the State Secretariat of Telecommunications and for the Information Society. The State Secretariat of Telecommunications and for the Information Society, in turn, is in charge of two General Directorates—the General Directorate of Telecommunications and Information Technologies (Dirección General de Telecomunicaciones y Tecnología de la Información—DGTTI) and the General Directorate for the Development of the Information Society (Dirección General para el Desarrollo de la Sociedad de la Información—DGDSI) [12].

Three initiatives under the auspices of the Ministry for Public Administration are particularly important as regards Spain's information and communication infrastructure and its security. These are the e-Government Council, its Technical Committee, and the so-called technimap project.

The Police Services and the National Center for the Protection of the Critical Infrastructure operate under the auspices of the Ministry of the Interior.

The two main public-private partnership initiatives include the Information Society and Telecommunications Analysis Center, called Enter, and the Spanish Electronics, Information Technology, and Telecommunications Industries Association, AETIC.

### 3.1 Public Agencies

***3.1.1 General Directorate for the Development of the Information Society.*** The General Directorate for the Development of the Information Society was created by Royal Decree 1554 of 25 June 2004. Article 9 of this decree defines a set of 20 functions and jurisdictions for the general directorate, distributed among the following Sub-Directorates [13]:

- Sub-Directorate for access to the information society;
- Sub-Directorate for companies of the Information Society;

- Sub-Directorate for the services of the Information Society;
- Sub-Directorate for audiovisual tools.

The DGDSI maintains multiple services [14] ranging from Plan Avanza over the provision of ICT technologies to small and medium-sized companies, universities, and the public, to the extension of broadband access and a program for the promotion of technical research. Other departments address a variety of international cooperation programs, e-Government, a range of Information Society services, and information security. The latter comes under the jurisdiction of the Antivirus Early Warning Center (Centro de Alerta Temprana sobre Virus y Seguridad Informática—CATA) [15].

***3.1.2 General Directorate of Telecommunications and Information Technologies.*** The General Directorate for Telecommunications and Information Technologies is in charge of six Sub-Directorates and is organized into 11 sections [16]. It offers manifold services [17], electronic forms [18], and access to legislation relating to telecommunications [19]. Most importantly, several so-called advisory councils and commissions are organized and convened by the DGTTI, including the following three bodies in particular. First, the Advisory Council of Telecommunications and of the Information Society is composed by delegated members of the different administrative units including the national government the autonomous administrations, and the local administrative authorities. Furthermore, representatives of the industrial and commercial sectors, of the telecommunications services providers, of the sectoral trade organizations, and delegates of the educational sector make up this advisory body. The main function of the Advisory Council is to study, deliberate, and advise the government on an informed basis concerning matters of IT policy [20].

Second, the Special Study Commission for the Development of the Information Society has the task of analyzing the consequences of implementing the Information Society for both small and medium-sized companies and for Spanish society in general. It is tasked with issuing written recommendations. It is composed of eminent members who are acknowledged experts in their respective professional fields, both technological and academic.

The third and most wide-ranging council is the Interministerial Commission of the Information Society and of the New Technologies in Spain, which was created with the objective of elaborating, developing, and evaluating the government's strategic initiatives relating to the Information Society and information technology. More precisely, the commission's tasks include:

- To collate a catalog of all activities undertaken by the various ministerial departments and other public entities regarding the Information Society;
- To elaborate and propose to the government a strategic initiative for the development of the Information Society, including objectives, priorities, and an agenda for implementation;
- To evaluate the tools considered for use in the strategic initiative, and to submit an annual report to the Council of Ministers;
- To propose guidelines to the government on the position to be adopted by Spain in the most relevant international forums and bodies in this field;
- To promote the diffusion of the strategic initiative and its tools within Spanish society.

The commission is to carry out its functions through specialized working groups. It is chaired by the Minister of Science and Technology, and its secretary is the General Director for the development of the Information Society. The list of the participating members is composed by representatives of 15 different ministerial secretariats [21].

***3.1.3 Red.es.*** Besides the two General Directorates described above, the State Secretariat of Telecommunications and for the Information Society manages two public entities—the red.es office and the Telecommunications Market Commission—as well as an autonomous organism, the State Agency for Radiocommunications [22]. On the same organizational level as the two General Directorates, the red.es office aims to promote the development of the Information Society through the execution of the programs defined in Plan Avanza; to analyze efforts pertaining to the Information Society by means of the Spanish Telecommunications and Information Society Observatory; to offer advice and specific support to the national government; and it is responsible for handling registrations of domain names under the country-code top level domain .es for Spain [23].

The various programs of red.es aim to promote digital inclusion and ameliorate the quality of services, to enhance the digitalization of the educational sector through the allocation of ICT infrastructures, to support the provision of digitalized public services both for citizens and for companies, to enhance broadband infrastructures, and to raise awareness of security mechanisms that generate confidence in ICT and digital content. The Observatory of red.es analyses the activities of the ICT sector and pursues the development of Plan Avanza for convergence among the autonomous regions and of Spain with Europe. The red.es office advises the Spanish government by submitting studies and reports to the various administrative bodies and by assisting the implementation of e-Government [24].

***3.1.4 The e-Government Council.*** Among the bodies of the Ministry for Public Administration is the e-Government Council (Consejo Superiór de Administración Electrónica). In 2005, it replaced the Council for Informatics and for the Promotion of e-Government, which had replaced the first incarnation of this body—the Council for Informatics—two years before. The task of this council is to prepare, elaborate, develop, and apply the government's IT policies and strategies [25]. It has seven main areas of activities, including statistical services, the promotion of telecommunications in the administration, the enhancement of the quality and productivity of the services, international activities, IT cooperation between the different levels of the administration, organization, and human resources.

Moreover, the council is assigned with the task of elaborating a security policy in collaboration with the National Cryptology Center of the National Intelligence Center for the development of information and communication security measures and systems security [26]. Under this header, it has developed tools for ICT security; issued publications on security criteria, standardization, and conservation of information and communications [27]; and published documentation on methodology for risk analysis and management [28] in information systems—the latest version of which dates from June 2006. The council operates as a plenum, has a permanent commission that is responsible for coordinating the technical support supplied by various bodies under the jurisdiction of different ministries, and its activities are sub-divided into ministerial commissions (Comisiones Ministeriales de Administración Electrónica).

***3.1.5 Technical Committee for the Security of Information Systems and Personal Data Processing.*** The Technical Committee for the Security of Information Systems and Personal Data Processing (Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales—SSITAD) [29] is responsible for cyber-security and for supporting the e-Government Council's task of elaborating a Spanish information security policy. The main task of this committee is to unify activities related to information systems security among all government departments. In order to achieve this objective, the SSITAD defines common information security policies and procedures, provides advice and training, and fosters general awareness. It also works on the adoption of international and European regulations in information systems security [30]. The committee exercises its functions in plenary sessions and also in four ad-hoc working groups. These are responsible, respectively, for personal data protection, the elaboration of directives for information systems security, the evaluation and certification of information systems security, and the use of electronic, information, and telematics technology in the government [31].

***3.1.6 TECNIMAP.*** Tecnimap [32] is a conference that brings together ICT experts from various areas of the public administration, the main companies in the field, and other experts. It aims at creating a space to exchange experiences, ideas, and projects in the field of information technologies and public services. The first conference was held in 1989 (Madrid). The 2007 conference, the tenth one, was organized in association with the Ministry of Public Services, the Government of the Principality of Asturias, and the Gijón City Council, and was held from 27 to 30 November. Over 5,000 participants, 250 enterprises, and representatives of 100 media outlets attended the event. Round tables and workshops were held for four days, during which interesting subjects relating to new technologies and e-administration were discussed.

The 2007 conference also included an opportunity to observe the latest projects developed by the public administration, and a forum was held at which citizens presented their opinions and suggestions. This conference discussed legal issues related to public access to the public administration using IT and other emerging issues.

***3.1.7 The Police Services.*** Under the auspices of the Ministry of the Interior, both the Policía Nacional and the Guardia Civil deal with cyber-crime. The national police operates through the Information Technology Crime Unit (Unidad de Investigación de la Delincuencia en Tecnología de la Información), and the Guardia Civil hosts a High Technology Crime Department (Departamento de Delitos en Alta Tecnología). The National Police Department and the General Judicial Police Department have an emergency service for cyber-crime. This citizen/police contact service allows the police to act rapidly and efficiently to prevent cyber-crime. The 24-hour alert system is active in the areas of cyber-crime, child pornography and telecommunications fraud [30].

***3.1.8 National Center for the Protection of the Critical Infrastructures.*** An organization that is more generally concerned with the protection of critical infrastructures is the National Center for the Protection of the Critical Infrastructures (Centro Nacional de Protección de Infraestructuras Críticas—CNPIC), which was established on 2 November 2007 under the responsibility of the State Security Secretariat of the Ministry of the Interior [33]. This agency is responsible for leading, coordinating, and supervising the

protection of the national critical infrastructures. The Ministry of the Interior had previously elaborated the antiterrorism prevention and protection plan as well as the national plan for the protection of the critical infrastructures, and had forged the agreement by the Ministerial Council of 2 November 2007 that established the CNPIC. Moreover, the State Security Secretariat is also responsible for the application of the National Plan for the Protection of the Critical Infrastructures, for the coordination of Spain's policies with the requirements of the EU, and for the elaboration of consistent best practice procedures. More specifically, the tasks of CNPIC include:[2]

- The maintenance and updating of the national security plan for the critical infrastructures and of the catalog;
- The collection, analysis, integration, and evaluation of the information furnished by the public institutions, police services, and strategic sectors;
- Threat assessment and risks analysis concerning strategic installations;
- The design and establishment of information, communication, and alert mechanisms;
- Coordination with the respective programs of the EU.

### 3.2 Public-Private Partnerships

***3.2.1 The Information Society and Telecommunications Analysis Center/ENTER.*** The Information Society and Telecommunications Analysis Center (Centro de Análisis de la Sociedad de la Información y las Telecomunicaciones) called ENTER is a public-private partnership designated as a center for providing information and analysis on the Information Society from the perspective of digital conversion. It brings together private companies and public institutions.[4] ENTER is structured into four functional units of analysis, including a technology section, an economic section, a societal section, and a regulations section. These four units supply data to a shared knowledge management system. Moreover, ENTER disseminates knowledge on the Information Society, which it holds in a database [35] and in an extensive collection of documents [36].

***3.2.2 AETIC.*** The Spanish Electronics, Information Technology and Telecommunications Industries Association (Asociación de Empresas de Electrónica, Tecnologías de la Información y Telecomunicaciones de España, AETIC) is a non-profit organization representing Spanish companies from the electronic, IT, and telecommunications sectors. AETIC collaborates with various arms of the public administration, including with the Presidential Office, the Ministry of Industry, Tourism, and Commerce, and with the Ministry of Public Administrations.[5] This collaboration between AETIC and the public administrations is mainly guided by the desire to protect the general interests of the industries that AETIC represents to the government at all levels [38].

## 4 EARLY WARNING AND PUBLIC OUTREACH

***4.0.1 A ntivirus Early-Warning Center.*** The Antivirus Early-Warning Center (Centro de Alerta Temprana Antivirus, CATA) became operational in 2001 and is located

[4]For a list of its members see: [34].
[5]For a full list of the ministries that AETIC collaborates with, see: [37].

under auspices of the Ministry of Industry, Tourism, and Trade's Secretariat of Telecommunications and for the Information Society.

It supplies users with current first-hand information about computer viruses, information system vulnerabilities, and identified security loopholes. The center collaborates with numerous public bodies at all levels as well as with ministries, universities, and private entities such as the large internet service providers and the producers of anti-virus programs [39]. The center aims to assure the security of data transmitted by means of electronic devices. Therefore, it provides an information platform for IT experts and users [40]. The services offered by the center are structured into four groups. First, the virus-warning group provides effective virus warnings and background information. Second, CATA issues reports about the emergence of new viruses, and collates statistical reports on electronic traffic between particular Spanish investigation centers and universities searching for virus incidents. Third, users can use a search engine to find information about known viruses within the center's databases, including advice on how to deal with virus incidents. And fourth, CATA provides preventive recommendations, FAQs, a virus encyclopedia, a list of the criteria applied, and a documentation center with all relevant information [41].

***4.0.2 CERT of the National Cryptology Center.*** The CERT-CNN (Equipo de Respuesta ante Incidentes de Seguridad Informática de Centro Criptológico Nacional de España) is dedicated to enhancing the level of security of the information systems of the public administrations of Spain. Its mission is to warn about and respond to security incidents, and to help the public administrations rapidly and efficiently in the case of emerging security threats that affect their information systems. The CERT-CNN, which resides within the National Intelligence Center, furnishes information services such as warnings about new threats and vulnerabilities, provides investigation reports and conducts awareness-raising campaigns, and offers support and coordination services for incident resolution [42]. CERT-CNN is member of the global Forum for Incident Response and Security Teams (FIRST) (see the survey on FIRST in this volume).

***4.0.3 RedIRIS.*** In 1988, the National Plan for Research and Development initiated a special program called IRIS for the interconnection of computer resources (Interconexión de los Recursos InformáticoS) of universities and research centers [43]. In 1991, when the first stage was finished, IRIS became what RedIRIS is today: the national academic and research network, which is still funded by the National Plan for Research and Development and was managed from 1994 to 2003 by the Scientific Research Council [44]. Since January 2004, RedIRIS has become a department within Red.es, but has preserved its autonomy. About 250 institutions are connected to RedIRIS today [45].

***4.0.4 I RIS-CERT.*** IRIS-CERT is the security service of RedIRIS', and is dedicated to the early detection of security incidents affecting RedIRIS centers, as well as the coordination of incident handling in cooperation with these centers. Proactive measures are constantly being developed, including timely warning about potential emerging problems, technical advice, and training. IRIS-CERT also provides incident handling coordination for the rest of the .es domains. IRIS-CERT has been a member of FIRST since 1997 and contributes to CSIRT Coordination in Europe [46].

## 5 LAW AND LEGISLATION

### 5.1 Spanish Penal Code

Three sections of the Spanish penal code in particular apply to cyber-crime. These in include Article 197 On the Discovery and Revealing of Secrets, Articles 248, 264, 256, and 270 On Fraud, and Article 273 On Crimes Involving Corporate Property [47]. No specific cyber-crime laws have been passed yet, but the Ministry of the Interior is preparing a proposal for cyber-crime laws in order to amend several articles of the penal code.

### 5.2 Law on Citizens' Electronic Access to Public Services

On 20 June 2007, the Spanish Congress adopted[6] a new law on electronic access of citizens to public services (Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos). This law recognizes the right of citizens to communicate with the public administrations by electronic means and states the obligation of the administrations to guarantee this right. The most notably innovations introduced by the new law are:

- New rights for citizens vis-à-vis the public administrations;
- The creation of the position of a "users' advocate" (Defensor del usario de la administración electrónica)
- The obligation of public administrations to implement these regulations by 2009;
- Access to e-Government services is to be ensured from everywhere and at all times.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts of the Directorate of the Center for the Protection of National Infrastructure who validated the content of this chapter.

## REFERENCES

1. Invertia.com (2007). "El Congreso insta al Gobierno a concluir en seis meses el catálogo de infraestructuras críticas", 12 July 2007. http://www.invertia.com/noticias/noticia.asp?subclasid=&clasid=&idNoticia=1764166.
2. http://www.publico.es/012947/gobierno/crea/centro/protegera/infraestructuras/criticas/24/horas/dia, 2008.
3. http://www.mir.es/MIR/estrorganica/estructura/subsec/dgas1.html, 2008.
4. http://www.fulp.ulpgc.es/documentacion/temp/texto_infoxxi.pdf, 2008.
5. http://www.fulp.ulpgc.es/index.php?pagina=investigadores&ver=infoxxi, 2008.
6. http://ec.europa.eu/idabc/jsps/documents/dsp_showPrinterDocument.jsp?docID=1483&lg=en, 2008.
7. http://www.gemeinsamlernen.de/euconet/Projects/Spanien/espana?language=en, 2008.

[6]For the full text, see: [48].

8. http://ec.europa.eu/idabc/en/document/5578/343, 2008.
9. (a) http://www.planavanza.es/Canales/CiudadaniaDigital/Todos/CATA.htm?rGuid=B838B40E-72D5-4AED-A8E2-768EE989A730; (b) http://alerta-antivirus.red.es/portada, 2008.
10. http://ec.europa.eu/idabc/en/document/1065/343, 2008.
11. http://ec.europa.eu/idabc/en/document/3316/343, 2008.
12. http://www.mityc.es/es-ES/Ministerio/Estructura, 2008.
13. http://www.mityc.es/DGDSI/Organizacion/FuncionesyCompetencias, 2008.
14. http://www.mityc.es/DGDSI/Secciones/PorServicio, 2008.
15. http://www.mityc.es/DGDSI/Secciones/PorUnidadTematica, 2008.
16. http://www.mityc.es/telecomunicaciones, 2008.
17. http://www.mityc.es/es-ES/Servicios/OficinaVirtual/Procedimientos/SETSI, 2008.
18. http://www.mityc.es/Telecomunicaciones/Servicios/AdmFormularios, 2008.
19. http://www.mityc.es/Telecomunicaciones/Servicios/Legislacion, 2008.
20. http://www.mityc.es/Telecomunicaciones/Organizacion/Consejos/ConsejoTeleco.htm, 2008.
21. http://www.mityc.es/Telecomunicaciones/Organizacion/Consejos/ComisionInterministerial.htm, 2008.
22. http://www.mityc.es/es-ES/Ministerio/Estructura/SecretariaEstadoTelecomunicaciones/Organigrama, 2008.
23. http://www.red.es/sobre_red/index.html, 2008.
24. http://www.red.es/actividades/index.html, 2008.
25. http://www.csi.map.es/csi/nuevo/csae_1.htm, 2008.
26. http://www.csi.map.es/csi/nuevo/pg4000_4.htm, 2008.
27. http://www.csi.map.es/csi/pg5c10.htm, 2008.
28. http://www.csi.map.es/csi/pg5m20.htm (also in English), 2008.
29. http://www.csi.map.es/csi/nuevo/csae_7.htm, 2008.
30. IST-2000-29202 Information Society Technologies (2002). "National Dependability Policy Environments SPAIN".
31. http://www.csi.map.es/csi/nuevo/csae_7.htm, 2008.
32. http://www.tecnimap.es/Tecnimap, 2008.
33. http://www.la-moncloa.es/ActualidadHome/021107-enlacecriticas.htm?FRAMELESS=true, 2008.
34. http://www.enter.es/que_es_enter/quienes_somos/enter_3_1.html, 2008.
35. http://www.enter.es/buscador/enterdata_bbdd.html, 2008.
36. http://www.enter.es/buscador/enterknowledge.html, 2008.
37. http://www.aetic.es/VerLibre.aspx?id=118&idcontenidos=143&Idioma=es, 2008.
38. http://www.aetic.es/CLI_AETIC/INFO%20Introduction%20AETIC.ppt, 2008.
39. http://www.mityc.es/DGDSI/Secciones/PorUnidadTematica/SeguridadInformatica/CATA.htm, 2008.
40. http://www.alerta-antivirus.es/acercade/ver_pag.html?tema=A&articulo=1&pagina=0, 2008.
41. http://www.alerta-antivirus.es/acercade/ver_pag.html?tema=A&articulo=2&pagina=0, 2008.
42. https://www.ccn-cert.cni.es/index.php?option=com_content&task=view&id=12&Itemid=32, 2008.
43. http://wwwn.mec.es/ciencia/jsp/plantilla.jsp?area=plan_idi&id=2, 2008.
44. http://www.csic.es/index.do, 2008.
45. http://www.rediris.es/rediris/index.en.html#inicio, 2008.
46. http://www.rediris.es/cert/servicios/iris-cert/rfc-2350.en.html, 2008.

47. http://www.cybercrimelaw.net/laws/countries/spain.html, 2008.
48. http://www.map.es/iniciativas/mejora_de_la_administracion_general_del_estado/moderniza/Administracion_Electronica/parrafo/04/document_es/a7%20(121-116)%202007-06-14%20Texto_definitivo_aprobado_Congreso.pdf, 2008.

# SWEDEN

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Sweden does not yet have an official definition of CII or CIIP. However, CIIP can be understood as the protection of essential electronic information services, such as IT systems, electronic communications, and radio and television services. CIIP has not only a technical, but also a human aspect. The following are regarded as critical information infrastructure sectors:[1]

- Air Control Systems,
- Supervisory Control And Data Acquisition (SCADA) systems in use within water, transport, and industry,
- Financial Systems,
- National Command Systems,
- Telecommunication Systems,
- The Internet.

Disruption of any of these systems would have immediate serious consequences for society.

[1]Information provided by the country experts.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

CIIP issues have been on the political agenda in Sweden for many decades. Measures to increase the robustness and security of critical national infrastructures have been implemented since World War II. The vulnerability problems associated with society's increasing dependence on IT and information infrastructures were identified early on as a matter of national security. In addition, management of IT-related vulnerabilities has been discussed since the early 1970s. The present Swedish CIIP policy is derived from these historical developments and from some more recent initiatives described below. The CIIP area in Sweden is currently in a transformative phase. The functions and responsibilities of governmental agencies are under review.

### 2.1 Commission on Vulnerability and Security

Following a decision on 23 June 1999, the Swedish government authorized the minister for defense to appoint a special investigator to head a commission of inquiry, with a mandate to analyze and submit proposals for a more integrated approach to civil defense and emergency preparedness planning [1]. The findings and proposals of the Commission on Vulnerability and Security, as presented in May 2001, have been a most important step in the implementation of a new structure for defense and emergency preparedness planning in Sweden.

The commission suggested several strategic measures for improving the general stability of critical technical infrastructure.[2] In its final report, the commission also proposed measures specifically designed to enhance information assurance and improve protection against information operations. The commission's view was that the central government must assume responsibility in these areas. At the same time, the commission emphasized that all managers and system owners are responsible for securing their own systems against computer intrusions and other types of IT-related threats. The role of the government should be to support these activities and to provide functions and facilities that exceed the financial capabilities of other sectors in society. In 2005, it submitted its final report to the Swedish government [3].

### 2.2 Bill on Swedish Security and Preparedness Policy

In March 2002, the government presented its first bill on Swedish security and preparedness policy. The bill was, to a large extent, based on the findings and proposals of the Commission on Vulnerability and Security.

The bill presented the government's framework for a new planning system to prepare for major societal crises and for activities related to a potential threat of war. Furthermore, the bill gave an account of how the crisis management structure would be strengthened. All of this has implications for the security of critical infrastructures in general, and of critical information infrastructures in particular.[3]

[2]Such as cross-sector activity, security standards, Computer Emergency Response Teams, a coordinating body for IT security, an information security technical support team, an intelligence and analysis unit, research and development, international cooperation, a system for the certification of IT products, and more [2].
[3]Information provided by expert of SEMA.

### 2.3 Information Security Policy proposals by the Committee on Information Assurance

The Swedish government on 11 July 2002 instituted the Committee on Information Assurance in Swedish Society. The committee's brief was to present an assessment of information protection requirements in critical sectors of society, and to make a proposal on organizational matters of the Swedish signals protection service.

After monitoring the implementation of the information assurance measures, the Committee on Information Assurance in Swedish Society has presented its proposal for a national strategy on information assurance [4] and also an organization plan [5]. The committee's proposal was processed by the government by March 2006.

### 2.4 SEMA action plan for information security

In January 2007, the Swedish Emergency Management Agency (SEMA) was commissioned by the government to prepare a proposal for a plan of action for implementing and administering the nation's strategy for information security. The plan was submitted to the government in April 2008 and consists of 47 proposed measures. The following four areas have been designated as priorities.[1]

- Improved sector-wide and cross-sectoral work is needed for civil information security. All-embracing directives for the field of information security applying to all government agencies should be prepared. At the same time, sector-specific responsibility must be clarified. Furthermore, there must be opportunities to provide practical recommendations to other civil sectors;
- A fundamental security level must be established for information security. Such a basic level is a prerequisite for being able to secure the information assets that have become increasingly fundamental for both trade and industry and the public sector;
- Society must be able to deal with extensive IT-related disturbances and emergencies. An operative national coordinating function should therefore be established;
- There are competence deficiencies in the field of information security at all levels of society. The rapid development also implies that competence deficiencies on the part of individual users have increasingly greater consequences. For this reason, several proposals are submitted that jointly constitute a broad program to raise competence in the field.

The plan of action proposes measures that address the problems reported in SEMA's annual situational assessment. The proposed measures also take into consideration, among other things, the Commission on Information Security's report Secure Information; the government bill for improved emergency preparedness; and the committee directive for a new agency with responsibility for emergency preparedness and security matters.[1]

### 2.5 Organizational Overview

Swedish government agencies report to their respective ministries, but are formally subordinated only to collective cabinet decisions. The various agencies and organizations in charge of CIIP are presented below under the heading of the ministry they are affiliated with, including the Ministry of Defense; the Ministry of Industry, Employment and Communication; and the Department of Justice.

The bill on Swedish security and preparedness policy contains a few changes of tasks and responsibilities for the actors within the area of information assurance. The bill relates to other issues beyond CIIP. The Committee on Information Assurance in Swedish Society has evaluated the CIIP work and suggested the changes to be introduced in the bill. The suggested changes are presented in the following chapter in connection with each actor. Importantly, in 2009, SEMA and other agencies will be replaced by a new agency called the Swedish Civil Contingencies Agency (SCCA) that will report to the Ministry of Defense; hence, there will be major changes in the overall CIIP system.

The public-private partnership initiatives in Sweden currently include SEMA's efforts to promote interaction between the public and the private sector, the Industry Security Delegation (NSD), and the Swedish Information Processing Society (DFS).

## 2.6 Public Agencies

***2.6.1 The Swedish Civil Contingencies Agency (SCCA).*** As of 1 January 2009, a new national government agency will be established with an all-encompassing task with regard to civil contingencies, that is to say, its work will cover the whole spectrum of contingencies from everyday road traffic accidents, fires, chemical emergencies, power cuts, and other technical failures to even more serious emergencies such as bomb threats and other hostile attacks, epidemics, natural disasters, and war. The responsibilities of this new agency will include information security. SEMA's current work on CIIP will be expanded, and the new agency will be given the authority to issue binding regulations.

The English designation of this new authority will be the Swedish Civil Contingencies Agency (SCCA), and it is being formed from three existing national government authorities, all of which will be closed down at the end of 2008, namely SEMA, the Swedish Rescue Services Agency (SRSA), and the National Board of Psychological Defence (SPF).

Within the Cabinet Offices, cross-departmental work is being performed on ways to implement the findings of the SEMA action plan and to reform CIIP in Sweden further.[1]

***2.6.2 The Swedish Emergency Management Agency (SEMA).*** The Swedish Emergency Management Agency (SEMA) [6] is responsible for the co-ordination of national information assurance at the policy level. This includes analyses of the development of society and the interdependency of critical societal functions. The agency further promotes interaction between the public and private sectors and coordinates and initiates research and development in the area of emergency management. It also has overall governmental responsibility for information assurance in Sweden. The Information Assurance and Analysis Department at SEMA manages these tasks. Its main activities include:

- Maintaining an updated overall picture of society's information security in terms of threats, vulnerabilities, protective measures, and risks; once a year, it presents an annual assessment of information assurance in Sweden to the government;
- Hosting various forums in order to develop a common national culture of information assurance. Certain forums are solely intended for the private sector or the public sector, respectively, while there are also combined forums for the public and private sectors;
- Developing public-private partnerships;

- Gathering, analyzing, and disseminating open-source information related to information assurance;
- The development of preventive IT security recommendations (consistent with ISO/IEC 17799) to support the IT security activities of other organizations;
- Initiating research and development in the area of different important societal systems and summarizing the respective risk and vulnerability assessments;
- Managing the Board of Information Assurance;
- Participating as a member in several international forums.

In its guidelines for emergency planning for 2006 and 2007 and in its annual report on information security in Sweden for 2008, SEMA points out that there is much work to be done to raise standards of information security in Sweden to an acceptable level. SEMA also reiterates the importance of protecting the nation's critical infrastructures. Dealing with the risks of technical collapses in electricity, telecom, and IT systems that are vital for society must be given priority, according to SEMA.[4] As far as the critical infrastructure (especially the technical infrastructure) is concerned, actions designed to mitigate the consequences of serious emergencies are given priority over preventive measures with the purpose of increasing robustness.[4]

SEMA recently conducted a case study on the topic of large-scale internet attacks. The study was prompted by the attacks that Estonia was subjected to in 2007. The study aims to analyze how Sweden would handle a similar attack [7].

***2.6.3 SEMA/Information Assurance Council.*** The Information Assurance Council was established to support SEMA's activities in the area of information assurance. This council will create a network of skilled experts from a variety of important organizations in the area. The council replaced the earlier Cabinet Office Working Group on Information Operations [8]. The council's primary assignment is to assist the senior management of SEMA by supplying:

- Information about trends in research and development in the area of information assurance;
- Suggestions and viewpoints concerning the direction, prioritizing, and realization of SEMA's activities in the area of information assurance.

***2.6.4 SEMA/Agency Cooperation Forum.*** The SEMA/Agency Cooperation Forum consists of seven agencies, and the main task of this forum is to secure the information assets of Swedish society in order to obtain a certain level of confidentiality, integrity, and availability. This is done through information exchange and cooperation. The focus areas of this group are:

- Strategy and regulatory framework;
- Technical and standardization issues;
- Information assurance issues at the national and international levels.

***2.6.5 The Swedish Defense Materiel Administration (FMV) and the Certification Body for IT Security (CSEC).*** The Swedish Defense Materiel Administration (FMV) [9] is the procurement agency for the armed forces. The FMV has been involved in the

[4]Information provided by the country expert.

area of IT security evaluations since 1989, performing in-house evaluations of equipment intended for use by the armed forces.

In the summer of 2002, the FMV was tasked by the government with establishing a national scheme for the evaluation and certification of IT security products to be used within Swedish governmental organizations. The certification body is now established as an independent entity within the FMV and is known as the Swedish Certification Body for IT Security (CSEC). Its work includes the production of quality manuals, descriptions of responsibility, descriptions of processes for licensing of evaluation laboratories, rules for implementation of certificates, and training of certification staff and evaluation companies [9].

***2.6.6 FRA / Information Security Technical Support Team.*** The Information Security Technical Support Team is associated with the Swedish National Defense Radio Establishment (FRA) [10], which is the Swedish signals intelligence organization. It is a civilian agency directly subordinated to the Ministry of Defense. The Information Security Technical Support Team consists of 20 experts in the field of IT security. The team is specifically intended to support:

- National crisis management where IT-security qualifications are required;
- Identification of individuals and organizations involved in IT-related threats against critical systems.

On request, the team supports the Swedish authorities, agencies, and state-owned corporations that are responsible for critical functions in Swedish society with IT-security expertise and services. The customized services consist of penetration tests, forensic computer investigations, source code analysis, audits, risk analyses, etc. The team co-operates on a regular basis with the national and international IT security community.

The changes suggested by the Committee on Information Assurance in Swedish Society concerning FRA are:

- Technical responsibility for coordination in the field of information security;
- Responsibility for signals protection;
- Creation of a group that can support initiatives in national crises with an IT component and in the case of related threats to important public systems.

***2.6.7 The Swedish Armed Forces.*** The Swedish Armed Forces [11] must be able to quickly respond to different types of threats and risks. The Swedish parliament has therefore decided to develop the armed forces according to the concept of network-based defense. This places a great demand on the information infrastructure in terms of availability and security. The armed forces are therefore heavily involved in research and development in areas such as IT security and information infrastructures.

The Swedish Military Intelligence and Security Service handles operational IT security in the armed forces during peacetime. In addition, the National Communications Security Group (TSA) offers advice and inspections of cryptographic systems to Swedish defense organizations and industries.[1]

***2.6.8 Center for Asymmetric Threat Studies (CATS).*** The National Center for IO/CIP Studies (CIOS) is now broadening its perspective from Information Operations (IO) to include terrorism, e.g., cyber-terrorism. In order to do so, the center's name has been

changed to "Center for Asymmetric Threat Studies (CATS)" [12]. CATS is located at the Swedish National Defense College [13]. It conducts research and policy development in the fields of CIIP, IO (Information Operations), PSYOPS (psychological warfare), and CIP. Research at CATS is funded by the Ministry of Defense and the Swedish Emergency Management Agency (SEMA).

***2.6.9 The Swedish Defense Research Agency (FOI).*** The Swedish Defense Research Agency (FOI) [14] focuses on research and development in the fields of applied natural sciences and political sciences, such as security policy analysis. At the Division of Defense Analysis, the Critical Infrastructure Studies Unit (CISU) research group is carrying out a long-term research program on CIP sponsored by SEMA, in cooperation with Systems Analysis and IT Security – another FOI department. This department has acquired a deep knowledge of commercial and military IT systems and applications.

***2.6.10 The Swedish National Post and Telecom Agency (PTS).*** The Swedish National Post and Telecom Agency (PTS) is a government authority that monitors all issues relating to ICT and postal services. One of its key tasks is to ensure the development of functioning postal and telecom markets. Within the PTS, the Department of Network Security is responsible for security issues concerning ICT.

The Department of Network Security is tasked with monitoring developments related to security issues and with implementing measures to reduce the threats to ICT from sabotage and terrorism. Emergency measures are planned in consultation with the ICT operators, the Swedish armed forces, and other agencies. As an example, critical nodes in the ICT structures are hardened, and all nodes that are crucial for running the ".se" domain autonomously have been installed within Sweden's borders. The Swedish IT Incident Center (see chapter on Early Warning and Public Outreach) is associated with this department.

***2.6.11 The Swedish National Police Board (NPB).*** The Swedish National Police Board (NPB) [15] is the central administrative and supervising authority of the police service. The NPB administers the National Criminal Police and the Swedish Security Service. Within the NPB, the IT Crime Squad has expert knowledge in investigating IT crime. This group supports the local Swedish police departments in IT crime investigations, participates in the education of parts of the judicial system, and assembles and communicates information about IT crime. The Internet Reconnaissance Unit is linked to this squad.

Additionally, the Swedish Security Service (SÄPO) has the fundamental duty of preventing and detecting crimes against the security of the realm. SÄPO is engaged in four main fields: protective security (including personal protection), counter-espionage, counter-terrorism, and protection of the constitution. Whenever IT-related criminal activity touches upon these fields, the Swedish Security Service is involved.

## 2.7 Public-Private Partnerships

***2.7.1 SEMA's Private Sector Partnership Advisory Council and Board of Information Assurance.*** SEMA promotes interaction between the public sector and the private sector, and works to ensure that the expertise of non-governmental organizations (NGOs) is taken into account in emergency management.

There are two advisory councils connected to SEMA: the Private Sector Partnership Advisory Council and the Board of Information Assurance.

SEMA has two forums for sharing information between private and public actors in the area of information assurance. The two established forums in the area of Supervisory Control And Data Acquisition (SCADA) and the financial sector. In these forums, the actors share information about threats and vulnerabilities in order to learn from each other. This concept is largely based on the British model for Information Exchange (IE).[5]

***2.7.2 The Industry Security Delegation (NSD).*** The Industry Security Delegation (NSD) [16] is part of the Confederation of Swedish Enterprise [17], whose objective is to increase cooperation between enterprises, organizations, and authorities, and to promote comprehensive views on vulnerability and security issues. The overall goal of this network structure is to enhance security and risk awareness among the general public and in the business sector. The NSD arranges courses in information assurance as well as crisis and risk management to help its members improve security.

***2.7.3 The Swedish Information Processing Society (DFS).*** The Swedish Information Processing Society (DFS) [18] is an independent organization for IT professionals with 32,000 members. The DFS owns the SBA brand of security products (the abbreviation stands for SårBarhetsAnalys, or "vulnerability assessment" in Swedish), which are focused on risk analysis and information security. SBA is regarded as the de-facto Swedish standard.

## 3 EARLY WARNING AND PUBLIC OUTREACH

### 3.1 PTS/The Swedish IT Incident Centre (SITIC)

In May 2002, the Swedish government tasked the Swedish National Post and Telecom Agency (PTS) with establishing the Swedish IT Incident Centre (SITIC) [19]. The center was officially opened on 1 January 2003 and can be considered to be the Swedish government CERT. SITIC supports national activities for protection against IT incidents by:

- Operating a system for information exchange on IT incidents between both public and private organizations and SITIC;
- Rapidly communicating to the public information on new problems that can disrupt IT systems;
- Providing information and advice on preventive measures;
- Compiling and publishing incident statistics as input to the continuing improvements of preventive measures.

## 4 LAW AND LEGISLATION

### 4.1 The Swedish Penal Code (SFS 1962:700)

The Swedish Penal code, in Chapter 4, Section 9 c, states that any person who, in cases other than those defined in Section 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a

[5]Information provided by an expert.

register, shall be sentenced for breach of data secrecy to a fine or imprisonment for no more than two years, unless the deed is punishable under the Criminal Code or the 1990 Protection of Trade Secrets Act. A recording in this context includes even information that is being processed by electronic or similar means for use through automatic data processing (Law 1998:206). Attempts and preparations to do so shall be punished as stated in Chapter 23 of the Criminal Code, unless the completed act would have been regarded as a petty crime. A proposal for amendments of the Act of the Penal Code has been presented. According to the draft, denial of service attacks (DoS) will be made a criminal offence.

Other important legal texts in Sweden in this context are the Personal Data Act (SFS 1998:204) and the Electronic Communications Act (SFS 2003:389).

### 4.2 The Electronic Communications Act (SFS 2003:389)

In its report, the Commission on Vulnerability and Security [20] concluded that there was a need for legislative amendments in order to support the proposals with respect to IT security and protection against information operations. A particular need for legislative amendments is seen in the following areas:

- Statutory and administrative provisions relating to the activities of local authorities and national administrative boards during major crises;
- The possibility of reallocating resources in the health services during major crises;
- Stricter safety regulations and more effective supervision of the power supply sector.

The government has decided to review the legislation relevant to CIIP and emergency management.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Linda Englund and Jan Lundberg of the Swedish Emergency Management Agency, who validated the content of this chapter.

## REFERENCES

1. Ministry of Defence (2001). *Vulnerability and Security in a New Era–A Summary*, (A summary of Swedish Government Official Report SOU). p. 41. http://www.sweden.gov.se/sb/d/574/a/25658.
2. Ministry of Defence (2001). *Vulnerability and Security in a New Era–A Summary*. A summary of Swedish Government Official Report SOU 2001. http://www.sweden.gov.se/sb/d/574/a/25658, pp. 41–60.
3. SOU (2005). *Informationssäkerhetspolitik–Organisatoriska konsekvenser*, p. 71, http://www.regeringen.se/sb/d/108/a/49614 and http://www.regeringen.se/sb/d/5101/a/49614 (Swedish).
4. SOU (2005). *Secure information—proposals on information security policy*, p. 42.
5. SOU (2005). *Organizational consequences*, p. 71.
6. http://www.krisberedskapsmyndigheten.se/defaultEN_224.aspx, 2008.
7. Swedish Emergency Management Agency (SEMA). (2008). *Large scale Internet attacks. The Internet attack on Estonia. Sweden's emergency preparedness for Internet attacks*, *SEMA's*

*Educational Series 2008:2*, http://www.krisberedskapsmyndigheten.se/upload/3040/Large-%20scale%20Internet%20attacks_utb-ser_2008-2.pdf.

8. SEMA document 0160/2003. *Account of Measures Taken in Assuming Responsibilities from the Working Group on Information Operations*, (2003). (Redovisning av åtgärder för att överta arbetsuppgifter från Ag IO 0160/2003).
9. http://www.fmv.se/default.aspx?id=121, 2008.
10. http://www.fra.se/english.shtml, 2008.
11. http://www.mil.se/en/, 2008.
12. http://www.fhs.se/en/Research/Centers-and-Research-Programmes/CATS/, 2008.
13. http://www.fhs.se/en/, 2008.
14. http://www.foi.se/FOI/templates/startpage_96.aspx/, 2008.
15. National Police Board. (2008). http://www.polisen.se/inter/nodeid=10230&pageversion=1.html.
16. http://www.svensktnaringsliv.se/nsd/article17105.ece, 2008.
17. Svenskt, N. http://www.svensktnaringsliv.se/english/?csref=_umk_english, 2008.
18. http://www.dfs.se (in Swedish), 2008.
19. http://www.sitic.se/in-english, 2008.
20. *Vulnerability and Security in a New Era*, op. cit.

# SWITZERLAND

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

Since the end of the Cold War, risks and vulnerabilities involving information and communications technologies have become a growing issue in the Swiss debate on security policy. The high density of information and communication technology (ICT) in Switzerland's public and private sectors offers a high potential for vulnerabilities. Critical

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

Infrastructure Protection (CIP) in general and the protection of information infrastructures in particular are therefore of high relevance for Swiss security policy.

In July 2007, the Federal Council approved the First Report to the Federal Council on the Protection of Critical Infrastructures, submitted by an interdepartmental working group under the lead of the Federal Office for Civil Protection (FOCP) [1]. This report defines critical infrastructures as "those infrastructures whose disruption, failure, or destruction would have a serious impact on the public health, the environment, the political affairs, the security, and the economic and social well-being of a population" [2]. The report defines the following ten sectors:

- Public Administration,
- Chemical Industry,
- Energy,
- Waste Disposal,
- Financial Services,
- Public Health,
- Information and Communication Technology,
- Water and Food,
- Public Safety, Rescue and Emergency Services,
- Transport [3].

These ten sectors are further divided into 31 sub-sectors. In May 2008, the working group launched a project to define criteria to identify critical elements and parts of the Swiss infrastructure.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

Since the end of the 1990s, several important steps have been taken in Switzerland to improve the management of CIIP. Strategic exercises and new threats such as the Millennium Bug have highlighted the importance of information assurance. From the beginning, the private sector was involved in the development of policies for information assurance and CIIP.

### 2.1 Strategic Leadership Exercise

Two strategic exercises were crucial for the development of Swiss protection policies in the field of information security:

- A key experience, and in fact the impetus for many later steps in Switzerland, was the Strategic Leadership Exercise in 1997 (SFU 97).[1] The exercise dealt with the revolution in information technologies and related challenges to modern society, politics, economics, and finance, as well as to other critical sectors [5]. The exercise

[1]This exercise was organized by a unit of the Swiss Federal Chancellery called "Strategische Führungsausbildung" (SFU), which is now called "Federal Crisis Management Training" (CMT). The unit is responsible for the periodical training of federal decision makers [4].

revealed that Switzerland's CI was facing new threats. For the first time, the idea of developing an early-warning system for threats to information security was raised.

- After a two-year planning process, the Strategic Leadership Training in 2001 conducted the three-day exercise INFORMO 2001. The goals were to review the information assurance process established after 1997 and to train a newly-established Special Task Force on Information Assurance.

### 2.2 Information Assurance Policy

The first Concept of Information Assurance was elaborated by the Information Society Coordination Group (ISCG) in 2000. It recommended the establishment of a crisis management system of a special task force on "Information Assurance" [6]. This strategy of the Swiss Federal Council was accompanied by a large number of parliamentary initiatives and was further developed.

In December 2001, the Swiss Federal Strategy Unit for Information Technology (FSUIT) presented a four-pillar model for information assurance in Switzerland [7]. Since then, the Swiss CIIP policy has been based on the following four pillars:

- *Prevention.* Suitable preventive measures must be implemented to limit the number of incidents;
- *Early recognition.* Dangers and threatening situations have to be recognized as early as possible to provide the necessary defensive measures or to avoid particularly vulnerable technology. The Reporting and Analysis Center for Information Assurance (MELANI) is the main actor in this field.
- *Crisis management.* The effects of disruptions on society and the state must be kept to a minimum. The major actors in charge for this are the Special Task Force on Information Assurance (SONIA), together with MELANI and the Federal Office for National Economic Supply (NES), which includes the ICT Infrastructure Unit.
- *Technical problem solution.* The technical causes of the disruption must be identified and corrected. This area is covered by MELANI together with the experts in charge in the private sector.

It is a tenet of Swiss information assurance policy that all four of the above pillars, or principles, must be taken into account to achieve a complete and strong system of CIP/CIIP.

### 2.3 Risk Analysis: InfoSurance and the Federal Office for National Economic Supply (NES)

The InfoSurance Foundation (see the chapter on Organizational Overview) started its work in 2002 with the initiation of a nation-wide risk analysis covering various sectors and branches such as telecommunications, finance, energy (electricity), emergency and rescue services, transportation and logistics, and health care. The risk analysis focuses on interdependencies of information infrastructures both within and between the various sectors and on potential preventive measures that can be derived from the analysis. Since 2004, the NES has been responsible for working out and reworking the risk analysis in cooperation with the private-sector experts.

### 2.4 Report on Critical Infrastructure Protection

Based on a first analysis—which was requested by the Control Delegation of the Federal Assembly—on the protection and safety of critical infrastructures in Switzerland, the Federal Council decided in 2005 to launch an interdepartmental CIP project. The FOCP was mandated to establish a working group that includes all relevant federal agencies.[2] It is the goal of the working group to improve the collaboration between all offices involved with CIP and ultimately to establish a national CIP strategy together with the private sector.

In 2007, the FOCP submitted a first report on CIP in Switzerland to the Federal Council [8]. The report was developed in close cooperation with all relevant federal agencies. It represents a first major step towards the elaboration of a national strategy. It establishes a common understanding of the problem in that it clarifies key concepts and identifies the critical infrastructure sectors relevant for Switzerland. It highlights threat scenarios from natural and technical hazards to violent and armed conflicts. It further defines the need for future action in the area of CIP. The appendix lists previous CIP activities and compares policies on international level, and highlights former and ongoing CIP developments of the relevant federal agencies.

The FOCP will submit a follow-up report to the Federal Council in spring 2009 and will elaborate a national CIP strategy by 2011.[3]

## 3 ORGANIZATIONAL OVERVIEW

The issue of CIP/CIIP involves agencies from different departments as well as the cantonal and local governments. The first part of this section provides an overview of the most important federal agencies. In the second part, the most important public-private partnerships are listed. Switzerland has a long-standing tradition of public-private collaboration. Historically, this is due to the tradition of part-time service in a strong militia system, both in the military and in politics. Accordingly, there are several important public-private partnerships in the field of CIP and CIIP (those partnerships with an early-warning function are listed in the section on Early Warning and Public Outreach).

### 3.1 Public Agencies

***3.1.1 Federal Office for Civil Protection (FOCP).*** The Federal Office for Civil Protection (FOCP) [9] is part of the Federal Department of Defence, Civil Protection, and Sports (DDPS). It supports the cantons and municipalities—which bear the principal responsibility for civil protection services in the intervention phase—in their efforts in that regard. As the responsible federal agency in the areas of both manmade and natural disasters, the FOCP ensures cooperation between the federation, the cantons, and the municipalities. The legal underpinnings of civil protection, especially the explicit aim of "protecting the population and its vital resources", are of particular relevance to critical infrastructure protection.[4]

[2]Currently the working group comprises 23 offices from all seven federal departments, including the Federal Chancellery. The working group usually meets four times a year. Its work is supported by sub-working groups where the actual CIP projects are conducted (information provided by an expert).

[3]Information provided an expert.

[4]Art. 2, Federal Law of Civil Protection.

In the field of CIP, the FOCP was therefore mandated in 2005 to coordinate the CIP interagency activities. As mentioned above, the FOCP established a working group and issued a first report for the attention of the Federal Council, summarizing the current state of work of the working group. A national CIP strategy will be elaborated by 2011.

***3.1.2 Federal Strategy Unit for Information Technology (FSUIT).*** One of the main bodies on CIIP in Switzerland is the Federal Strategy Unit for Information Technology (FSUIT) [10]. It is part of the Swiss Federal Department of Finance (FDF). The FSUIT reports to the FDF and is charged with producing instructions, methods, and procedures for the federal administration's information security. It collects data on incidents within the Swiss federal government and is responsible for the Special Task Force on Information Assurance (SONIA) and for the Reporting and Analysis Center (MELANI). The FSUIT itself runs the Swiss Government Computer Emergency Response Team GovCERT.ch (see the chapter on Early Warning and Public Outreach).

***3.1.3 Federal Office of Communications (OFCOM).*** The Federal Office of Communications (OFCOM) [11] is the main regulatory body in the field of telecommunications and ICT in Switzerland. The OFCOM studies various aspects of the information revolution. It includes consumer protection and management of the frequency spectrum as well as conformity assessment rules in the telecommunications equipment area. The OFCOM deals with risks affecting the information society, such as the formation of a new two-tier society, information overload, and the resulting inability to analyze problems and make decisions, and new opportunities for the manipulation of information of a technical, political, or economic nature.

***3.1.4 Federal Office for National Economic Supply (NES).*** The Federal Office for National Economic Supply (NES) [12], which includes the ICT Infrastructure Unit (see below, in the section on Public-Private Partnerships), reports to the Swiss Federal Department of Economic Affairs. Its main task is to ensure that the Swiss population is able to obtain vital goods and services at all times. The NES provides governmental support when the private sector is unable to resolve supply problems of vital goods and services on its own. However, measures to ensure a steady flow of supplies to the national economy would only be undertaken if the free-market system were seriously disrupted. In the four pillars of the Swiss information assurance policy, the NES plays an important strategic role in the fields of prevention and crisis management.

***3.1.5 Federal Office of Information Technology and Telecommunication (FOITT).*** The Swiss Federal Office of Information Technology, Systems, and Telecommunication (FOITT) [13] is part of the Swiss Federal Department of Finance. Its responsibilities include security and emergency preparedness for the federal administration's information systems on an operational level.

***3.1.6 Coordination Unit for Cybercrime Control (CYCO).*** Citizens can report suspected internet crimes, including unlawful access to IT systems, spreading of computer viruses, destruction of data, and similar offenses to the Swiss Coordination Unit for Cybercrime Control (CYCO) [14], which is part of the Federal Office of Police (fedpol). The offenses reported are then forwarded to the respective national or foreign prosecution authorities. CYCO also scans the internet for criminal content and is responsible for in-depth analysis of cyber-crime. In addition, CYCO collaborates closely with MELANI.

### 3.2 Public-Private Partnerships

***3.2.1 InfoSurance Association.*** InfoSurance was established as a foundation in 1999 by a number of companies with the support of the Swiss government. Today, it is an association that aims to increase awareness of the information assurance issue and to establish networks of cooperation among various players from both the public and the private sectors. The association aims at creating a closely-linked network that promotes the organizational and structural conditions for recognizing and analyzing Switzerland's growing dependency on information technologies and the associated risks. The target group of InfoSurance consists of SMEs, and the focus lies on prevention [15].

***3.2.2 Federal Office for National Economic Supply (NES): ICT Infrastructure Unit (ICT-I).*** Another important public-private partnership is the NES. It works in close cooperation with the private sector as well as with cantonal and municipal authorities. The federal government has requested that the NES deal with all prolonged disruptions of the information and communications infrastructure affecting the whole of Switzerland (ICT Infrastructure Unit, ICT-I) [16]. The NES also conducts sector-specific risk analysis in cooperation with the private-sector experts involved. These analyses were formerly conducted by the InfoSurance association.

***3.2.3 CLUSIS.*** The non-profit association CLUSIS (Club de la sécurité des systèmes d'information—Suisse) [17] has existed in Switzerland since 1989 and represents about 230 members, including Swiss public administrations, IT suppliers, providers, banks, industries, consultants, etc. CLUSIS organizes seminars related to information security practices and technologies, issues whitepapers and publications, and is involved in education. The aim is to provide networking opportunities for their members and to share experiences. CLUSIS mainly covers the French- and Italian-speaking parts of Switzerland.

## 4 EARLY-WARNING APPROACHES AND PUBLIC OUTREACH

In addition to the public-private partnerships listed above, collaboration between government agencies and private companies is also essential for early warning and public outreach.

### 4.1 The Reporting and Analysis Center for Information Assurance (MELANI)

On 29 October 2003, the government decided to create a center for CIIP that would collect information on the security of the IT infrastructure, especially of the internet. This new center, called the Reporting and Analysis Center for Information Assurance (MELANI) [18], has been operational since October 2004 and is now the core of the Swiss CIIP early-warning system. It plays a role in all four pillars of the Swiss information assurance policy (prevention, early warning, crisis management, and technical problem solution) and is the central office for CIIP in Switzerland. In addition to its own investigations, it depends on close cooperation with the public and private sectors.

It is designed as a cooperative undertaking between the Federal Strategy Unit for Information Technology (FSUIT) and the Federal Office of Police (fedpol). These two partners of MELANI have the following main tasks [19]:

- The FSUIT is responsible for strategic issues and the management of MELANI. Since 1 April 2008, it has also run the Swiss government's Computer Emergency Response Team (GovCERT.ch). GovCERT.ch is MELANI's technical competence center, and is responsible for dealing with technical incidents, in particular concerning the internet and computer operating systems;
- The fedpol operates the MELANI analysis center and is responsible for collecting, condensing, and presenting operational information from different sources in the public and private sectors.

MELANI offers warnings and advice for the broader public via a website, but also runs a special program for the owners and operators of critical infrastructures. For members of the so-called "closed constituency" MELANI organizes workshops, disseminates detailed warnings, and operates a 24/7 help-desk. The "closed constituency" of MELANI can be described as a dedicated public-private partnership for CIIP.

The cooperation between the involved partners as well as the conceptualization of MELANI as a public-private partnership has proven to be successful. By pooling existing resources, new threats to information security can be confronted effectively and effectively. On 24 January 2007, the Federal Council decided definitely to establish MELANI as a federal office for information assurance [20].

### 4.2 Special Task Force on Information Assurance (SONIA)

The Special Task Force on Information Assurance (SONIA) [21] is also directed by the FSUIT. SONIA is a crisis-management organization and constitutes the core element of the third pillar of the Swiss information assurance policy, namely damage limitation. Its main task is to advise the Swiss Federal Council and senior management representatives from the private sector in crisis situations and to act as a link between the public and private sectors. SONIA would be activated after a breakdown in the information and communication infrastructure that resulted in (massive) disruptions in CI. Unlike MELANI, it is not a permanent body, but would only be convened for damage limitation in genuine crises.

SONIA is mainly supported by the following organizations:

- The ICT Infrastructure Unit of NES, to raise awareness and to give guidance in threat and risk analysis, and to establish contacts among the experts in charge in the private sector;
- MELANI, as a provider of reliable information about a possible imminent threat and its consequences, and as an information base in case of a crisis [22].

## 5 LAW AND LEGISLATION

### 5.1 Swiss Penal Code

A number of articles in the Swiss Penal Code are of relevance in the context of CIIP:

- Article 143 (unauthorized procurement of data);
- Article 143 bis (unauthorized access to a computing system): This article states that any person who, by means of a data transmission device, gains unauthorized access

to a computing system belonging to others that is specially protected against access by the intruder shall be punished by imprisonment or a fine if a complaint is made;[5]

- Article 144 (damage to property): The article states that any person who damages, destroys, or renders unusable any property belonging to others shall be punished by imprisonment or a fine if a complaint is made;[5]
- Article 144 bis (damage to data): The article states that any person who alters, deletes, erases, or renders unusable data stored or transferred by electronic or similar means without authorization shall be punished by imprisonment or a fine if a complaint is made;[5]
- Article 147 (fraudulent use of a computer): The article states that any person who, with the intention of unlawfully obtaining financial rewards for himself or another, interferes with an electronic procedure through the unauthorized use of data shall be punished by community service of up to five years or imprisonment.[5]

Switzerland's laws against virus creation and the use of malicious software in general are widely applicable. However, the structure of the Swiss legal system makes prosecution difficult, due to the complexities of different laws (comprising laws on both the federal and cantonal level) and law enforcement procedures.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts of the Federal Office for Civil Protection, the Reporting and Analysis Center for Information Assurance, and the Federal Office for National Economic Supply, who validated the content of this chapter.

## REFERENCES

1. http://www.news.admin.ch/message/index.html?lang=en&msg-id=13516&print_style=yes, 2008.
2. Federal Office for Civil Protection (2007). *Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen*, (First Report to the Federal Council on Critical Infrastructure Protection),Berne, p. 7.
3. Federal Office for Civil Protection (2007). *Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen*, (First Report to the Federal Council on Critical Infrastructure Protection), Berne, p. 8.
4. http://www.bk.admin.ch/org/bk/00351/00423, 2008.
5. Swiss Federal Chancellery (1997). *Strategische Führungsübung 1997—Kurzdokumentation über die SFU 97*, Berne, p. 2.
6. Swiss Federal Strategy Unit for Information Technology (2002). *Vulnerable Information Society—Challenge Information Assurance*, Berne, p. 19.
7. Swiss Federal Strategy Unit for Information Technology (2002). *Vulnerable Information Society—Challenge Information Assurance*, Berne, p. 23ff.
8. *Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen*, op. cit.
9. http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/das_babs.html, 2008.
10. http://www.isb.admin.ch/index.html?lang=en, 2008.

[5]Based on the official English translation of the Swiss Penal Code.

11. http://www.bakom.ch/index.html?lang=en, 2008.
12. http://www.bwl.admin.ch/index.html?lang=en, 2008.
13. http://www.efd.admin.ch/org/org/00582/00806/index.html?lang=en, 2008.
14. http://www.cybercrime.ch/index.php?language=en, 2008.
15. http://www.infosurance.ch, 2008.
16. http://www.bwl.admin.ch/themen/00507/00520/index.html?lang=en, 2008.
17. http://www.clusis.ch, 2008.
18. http://www.melani.admin.ch, 2008.
19. Ruedi, R., and Jürg, R. (2003). MELANI—an analysis centre for the protection of critical infrastructures in the information age. *Paper for the Workshop on Critical Infrastructure Protection*. Frankfurt, (September 2003), p. 49.
20. http://www.news.admin.ch/dokumentation/00002/00015/index.html?lang=de&msg-id=10361, 2008.
21. http://www.isb.admin.ch/themen/sicherheit/00152/00176/index.html?lang=en.
22. Haefelfinger, R. L. (2003). The Swiss perspective on critical infrastructure. *Presentation at the PfP Seminar on Critical Infrastructure Protection and Civil Emergency Planning—New Concepts for the 21st Century*. Stockholm, 17–18 November.

# UNITED KINGDOM

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

In the United Kingdom, the critical national infrastructure (CNI) comprises those key elements of the national infrastructure that are crucial to the continued delivery of essential services to the UK. Without these key elements, essential services could not be delivered and the UK could suffer serious consequences, including severe economic damage, grave social disruption, or even large-scale loss of life [1]. Many of the critical

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

services that are essential to the well-being of the UK depend on IT and are provided by both the public and private sectors. Nine sectors are considered to deliver "essential services". These are outlined below:

- Communications (Data Communications, Fixed Voice Communications, Mail, Public Information, Wireless Communications),
- Emergency Service(Ambulance, Fire and Rescue, Coastguard, Police),
- Energy(Electricity, Natural Gas, Petroleum),
- Finance(Asset Management, Financial Facilities, Investment Banking, Markets, Retail Banking),
- Food(Produce, Import, Process, Distribute, Retail),
- Government and Public Services (Central, Regional, and Local Government; Parliaments and Legislatures; Justice; National Security),
- Public Safety (Chemical, Biological, Radiological, and Nuclear (CBRN) Terrorism; Crowds and Mass Events),
- Health (Health Care, Public Health),
- Transport (Air, Marine, Rail, Road),
- Water (Mains Water, Sewerage).

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

The UK government aims to protect the CNI from both two kinds of threats: physical attacks against physical installations and electronic attacks against computers or communications systems [2]. It has therefore developed a National Information Assurance Strategy. Another important field of action is data security. In reaction to a data security incident in 2007, the government has elaborated data security guidelines.

### 2.1 National Information Assurance Strategy

The UK Cabinet Office produces and maintains the National Information Assurance Strategy [3]. This was first produced in 2003 by the Central Sponsor for Information Assurance (CSIA), a unit within the Cabinet Office, and aims to provide ongoing assurance to the government that the risks to information systems and the information they hold are appropriately managed. The CSIA, with partner organizations, coordinates and sponsors work programs to deliver the strategy's recommendations.

Information assurance (IA) is defined as the confidence that information systems will protect the information they carry and will function as they need to, when they need to, and under the control of legitimate users. The CSIA has a lead role in helping governments to improve IA. That involves the following tasks:

- Enabling the government to deliver public services through the appropriate use of information and communications technology (ICT);
- Strengthening the UK's national security by protecting information and information systems at risk of compromise;
- Enhance the UK's economic and social well-being as the government, businesses, and citizens realize the full benefits of ICT.

Most importantly, the strategy recognizes that within an increasingly interdependent and interconnected information infrastructure, the government must concern itself with the confidentiality, availability, and integrity of all information systems [3].

### 2.2 Government Data Security

Following a data security incident in November 2007, the prime minister asked the Cabinet Office to review data handling procedures in all government departments. An interim report was presented to parliament on 20 December 2007, and the final report is expected in 2008. The government has already accepted a number of recommendations in the interim report to bring about greater transparency, increased monitoring, improved guidance, and better mandatory training.[1]

A number of other reviews are being conducted across the UK government that will have an effect on data security measures. The Poynter Review [4] is looking into the specific incident of the loss of child benefit data at HM Revenue & Customs (HMRC)[2] and is expected to report in 2008 [5]. In October 2007, before the HMRC-incident, the government had already identified the need to do more to protect the data it controls, and the prime minister commissioned the independent Walport/Thomas review on the use of information in both the public and private sectors. The review is expected to report in the first half of 2008. The Burton report, looking at data losses in the Ministry of Defence, is also due to be published in 2008.[1]

## 3 ORGANIZATIONAL OVERVIEW

In the UK, the main responsibility for CIIP lies with the home secretary [6]. However, a number of other departments play a role in the protection of the various CNI sectors and contribute resources and expertise to the UK CIIP effort. These contributions are coordinated by the Centre for the Protection of the National Infrastructure (CPNI) [7]. CPNI was formed on 1 February 2007 from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and the National Security Advice Centre (NSAC).

CIIP policy is developed and delivered by several government departments and bodies including CPNI, the Central Sponsor for Information Assurance (CSIA), the Civil Contingencies Secretariat (CCS), the Cabinet Office Security Policy Division, the Home Office, and the Government Communications Headquarters (GCHQ).

Responsibility for the provision of advice on physical protection to the CNI is shared between CPNI, the Security Service, and the police. CSIA is in charge of the UK's broader information assurance strategy, which deals with all aspects of the Information Society. The coordination of the government's contingency and emergency response effort (regardless of the cause of the disruption) is the responsibility of the CCS (part of the Cabinet Office).

Furthermore, there are several public-private partnerships in the field of CIIP. The government collaborates closely with the private sector. The CPNI shares information with the owners and operators of CNI in so-called Information Exchanges.

[1]Information provided by an expert.

[2]Her Majesty's Revenue & Customs (HMRC) is responsible for collecting the bulk of tax revenue and paying tax credits and child benefits. See: http://www.hmrc.gov.uk/. For more information on the incident, see: http://www.infosecurity-magazine.com/news/071121_hmrc_bamford.html.

### 3.1 Public Agencies

***3.1.1 Centre for the Protection of National Infrastructure (CPNI).*** Since 1 February 2007, the Centre for the Protection of National Infrastructure (CPNI) has worked to protect the UK's CNI from both physical and electronic attack. CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organizations that make up the national infrastructure. Through the delivery of this advice, it protects national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

CPNI advice is targeted primarily at the critical national infrastructure (CNI)—the key elements of the national infrastructure that are crucial to the continued delivery of essential services to the UK. Recommendations are drawn from the expertise, knowledge, and information of the organizations that contribute to its work. CPNI sponsors research and works in partnership with academia, other government agencies, research institutions, and the private sector to develop applications that can reduce vulnerability to terrorist and other attacks and reduce the impact when attacks take place. CPNI also has special access to intelligence and information about terrorism and other threats, and this informs its advice and priorities.

CPNI shares information, such as warnings of specific threats and vulnerabilities, with its CNI partners so that operators can install suitable defenses, and offers periodic assessments of the nature of the threat from electronic attack. This information on vulnerabilities and alerts is disseminated by the Combined Security Incident Response Team (CSIRTUK) [8]. together with GovCertUK (part of GCHQ) [9].

CPNI works with vendors and researchers to co-ordinate the release of vulnerabilities in a controlled way, so that fixes are in place before the software weaknesses are publicly disclosed. This work enhances the understanding of the potential impact of vulnerabilities.

CPNI's advice is provided to national infrastructure organizations in a variety of ways, including:

- Face-to-face advice through teams of sector-based and specialized, highly experienced advisers;
- Training;
- Online information;
- Written advisory products.

CPNI advice is integrated across the physical, personnel, and information security disciplines both in response to user requirements and derived from expert knowledge about how to make the national infrastructure less vulnerable. Its closest relationship, which has been built up over many years, is with those organizations that operate the key elements on which essential services depend.

CPNI discharges its responsibilities through government departments that have overall responsibility for ensuring that appropriate steps are taken to improve protective security within their sectors. They are also in charge of the identification of critical infrastructure within their sectors in consultation with CPNI and sector organizations. The following departments and agencies have responsibility for sectors or sub-sectors of the CNI:

- Cabinet Office (government and public services),
- Communities and local government (emergency services),

- Department for Business, Enterprise and Regulatory Reform (communications, energy),
- Department for Environment, Food and Rural Affairs (food supply, water),
- Department for Transport (emergency services, transport),
- Department of Health (emergency services, health),
- Food Standards Agency (food safety),
- HM Treasury (finance),
- Home Office (emergency services),
- Maritime and Coastguard Agency (emergency services).

CPNI also works closely with the police. It has a particularly strong partnership with the police National Counter Terrorism Security Office (NaCTSO) [10], which is co-located with CPNI, and the nationwide network of specialist police Counter Terrorism Security Advisers (CTSAs) that they co-ordinate. NaCTSO and the CTSAs support CPNI in the delivery of advice to critical sites within the national infrastructure.

***3.1.2 Civil Contingencies Secretariat (CCS).*** The Cabinet Office Civil Contingencies Secretariat (CCS) [11] was established in July 2001 and reports to the prime minister through the prime minister's security adviser. The CCS works in partnership with government departments, the devolved administrations of Scotland and Wales, and key stakeholders to enhance the UK's ability to prepare for, respond to, and recover from emergencies.

The aim of the CCS is to improve the UK's resilience to disruptive challenges by working with others inside and outside government on the anticipation, preparation, prevention, and resolution of threats. Its current objectives are:

- To make sure that the government can continue to function and deliver public services during a crisis. To work with departments and the wider Cabinet Office to make sure that plans and systems are in place and cover the full range of potential disruption;
- To ensure improved resilience of the government and the public sector, and to support ministers in developing policy;
- To lead horizon-scanning activity to identify and assess potential and imminent disruptions. To build partnerships with other organizations and countries to develop and share best practice in horizon-scanning and knowledge of the UK's critical networks and infrastructure;
- To improve the capability of all levels of government, the wider public sector, and the private and voluntary sectors to prepare for, respond to, and manage potential challenges.

Like all Cabinet Office Secretariats, the CCS supports ministers collectively. In times of national crisis, it supports the Civil Contingencies Committee, which manages and exercises arrangements to handle national crises in the Cabinet Office Briefing Room (COBR) to deliver an integrated government response.

The Emergency Planning College is an integral part of the CCS. It has a key role to play in the development and promulgation of the UK's resilience doctrine, and in the development of cross-organizational communities to deliver it.[1]

### 3.2 Public-Private Partnerships

***3.2.1 CPNI's Public-Private Partnerships.*** In addition to the assurance advice that it provides to specific CNI companies, the Centre for the Protection of the National Infrastructure (CPNI) actively promotes information-sharing. Based on the assumption that the sharing of information about the risks facing networks is beneficial to both government and industry, CPNI works with its CNI partners in Information Exchanges. These aim to create a mechanism through which one company can learn from the experiences, mistakes, and successes of another, without fear of exposing company sensitivities to competitors and the media.

The success of Information Exchanges is based on the personal trust of representatives sharing information in a confidential meeting. In face-to-face meetings, CPNI helps to build a trusted community with a common interest. Each member organization can have a maximum of two representatives. Substitutes are not permitted, as a stranger turning up at a meeting would inhibit the sharing of sensitive information.

Warning Advice and Reporting Points (WARPs) are another way for an organization to share information from which lessons can be abstracted and shared with the CPNI. A WARP is a community-based service where members can receive and share up-to-date advice on information security threats, incidents, and solutions. Currently, there are WARPs for local governments, public services, businesses, and voluntary and international organizations [12].

***3.2.2 Other Private-Public Partnerships.*** There is a wide range of private-sector organizations that work with the public sector to promote information assurance. These include:

- The Information Assurance Advisory Council [13];
- The British Computer Society,
- The Internet Security Forum,
- The National Computing Centre,
- The Internet Watch Foundation,
- The Confederation of British Industry,
- The Institute of Information Security Professionals,
- European Information Society Group,
- Royal United Services Institute,
- Chatham House [14].

## 4 EARLY WARNING AND PUBLIC OUTREACH

### 4.1 Combined Security Incident Response Team (CSIRTUK)

CPNI runs a Computer Emergency Response Team (CERT) for its partners in the private sector who operate elements of the national infrastructure. This service, which advises on how to manage the response to incidents and produces advisories on security matters, is called the Combined Security Incident Response Team (CSIRTUK). CSIRTUK receives,

reviews, and responds to computer security incident reports, providing advisories and related activity for its CNI partners [8].

An important part of risk management is to learn from the experiences of others, and national infrastructure organizations can contact CSIRTUK about potential security vulnerabilities, incidents, or events, whether they be electronic, physical, or personnel-related. Information received is treated confidentially and, if necessary, particular details that would identify individuals or organizations are removed so the information can be incorporated into generic security advice. In this way, valuable experience can be shared to help others.

By enhancing the traditional CERT role to cover holistic advice—including physical, personnel, and electronic issues—CSIRTUK provides a central point for reporting security incidents and for receiving advice and guidance.

### 4.2 GovCertUK

The Communications-Electronics Security Group (CESG), the national technical authority for Information Assurance within GCHQ [15], has the lead responsibility within the government for providing IA advice to public-sector organizations. This role includes providing an emergency response capability to public-sector organizations that may require technical support and advice during periods of electronic attack or other network security incidents. CESG therefore runs the GovCertUK, which assists public-sector organizations in the response to computer security incidents and provides advice to reduce exposure to threat [16].

Together, CSIRTUK and GovCertUK have replaced the Unified Incident Reporting and Alert Scheme (UNIRAS), which has been the UK government CERT in the past.

### 4.3 Ministry of Defence Computer Emergency Response Team

The UK Ministry of Defence Computer Emergency Response Team (MODCERT) is responsible for information security within the Ministry of Defence. It is a member organization of both the international Forum of Incident Response Security Teams (FIRST, see the chapter on FIRST in this volume) and the Trusted Introducer (TI) [17] scheme, both of which provide a mechanism for sharing information on computer security incidents among the communities concerned. MODCERT [18] consists of a central co-ordination center and a number of monitoring and reporting centers, Warning, Advice, and Reporting Points (WARPs), and incident response teams. It also works closely with GovCertUK and CSIRTUK.

### 4.4 GetSafeOnline

GetSafeOnline, designed to educate the public about IT security, is the result of collaboration between the government and private-sector companies. The website has been available since October 2005 and offers comprehensive advice on safe internet use for home users and for micro-businesses about how to protect computers, mobile phones, and other devices against electronic attack. The aim of this free service is to reduce occurrences of ID theft, viruses, and spam by educating internet users and helping them to protect themselves and their computers from online threats [19].

## 5 LAW AND LEGISLATION

The UK has created a legal framework to protect information systems. This includes a number of pieces of legislation. These are outlined below.

- Telecommunications (Fraud) Act 1997: This act amends the Telecommunications Act 1984 to make further provision for the prevention of fraud in connection with the use of a telecommunication system;
- Data Protection Act 1998: This act regulates the processing of information relating to individuals, including the obtaining, holding, use, or disclosure of such information;
- Electronic Communications Bill 2000: This Bill makes provision to facilitate the use of electronic communications and electronic data storage. It also makes provision for the modification of licenses granted under Section 7 of the Telecommunications Act 1984; and for connected purposes;
- Terrorism Act 2000: This act relates to terrorism. It makes temporary provision for Northern Ireland about the prosecution and punishment of certain offences, the preservation of peace, and the maintenance of order. It also makes the deliberate interference with or disruption of electronic systems a criminal act;
- Police and Justice Act 2006: This act makes provision for a range of items relating to policing, crime, and disorder. It also amends the Computer Misuse Act 1990.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts of the Center for the Protection of National Infrastructures who validated the content of this chapter.

## REFERENCES

1. http://www.cpni.gov.uk/glossary.aspx, 2008.
2. http://www.mi5.gov.uk, 2008.
3. Central Sponsor for Information Assurance (CSIA) (2007). *A National Information Assurance Strategy*, http://www.cabinetoffice.gov.uk/csia/national_a_strategy.aspx.
4. http://www.hm-treasury.gov.uk/independent_reviews/poynter_review/poynter_review_index.cfm, 2008.
5. http://www.hm-treasury.gov.uk/media/E/E/poynter_review171207.pdf, 2008.
6. http://www.homeoffice.gov.uk, 2008.
7. http://www.cpni.gov.uk, 2008.
8. http://www.cpni.gov.uk/Products/advisories.aspx, 2008.
9. http://www.govcertuk.gov.uk, 2008.
10. http://www.nactso.gov.uk, 2008.
11. http://www.ukresilience.info/ccs.aspx, and http://www.cabinetoffice.gov.uk/secretariats/civil_contingencies.aspx, 2008.
12. http://www.warp.gov.uk, 2008.

13. http://www.iaac.org.uk, 2008.
14. http://www.chathamhouse.org.uk, 2008.
15. http://www.cesg.gov.uk, 2008.
16. http://www.govcertuk.gov.uk/index.shtml, 2008.
17. http://www.ti.terena.nl, 2008.
18. http://www.mod.uk/DefenceInternet/AboutDefence/WhatWeDo/SecurityandIntelligence/CERT, 2008.
19. http://www.getsafeonline.org, 2008.

# UNITED STATES

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 CRITICAL SECTORS

In the US, critical infrastructures are defined according to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, section 1016e: "[ ... ] the term 'critical infrastructure' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters" [1].

Based on this definition, Homeland Security Presidential Directive 7 (HSPD-7), issued on December 2003, identified 17 critical infrastructures and key resources (CI/KR) and delineated the roles and responsibilities for the protection of these sectors. The most recent policy plan (the National Infrastructure Protection Plan, issued in 2006) [2] and the current strategy for Homeland Security (issued in 2007) [3] both reconfirm the HSPD-7 list of 17 critical sectors and the corresponding assignment of responsibilities. However, the list of critical infrastructures and key resources is not meant to be final and conclusive—HSPD-7 states that the Department of Homeland Security (DHS) "shall [...]

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate" [4]. In March 2008, the DHS announced the establishment of the critical manufacturing sector as the 18th CI/KR sector. While further changes and additions are still possible, the following sectors are currently defined as critical infrastructures and key resources:

- Information Technology,
- Telecommunications,
- Chemicals,
- Commercial Facilities,
- Dams,
- Commercial Nuclear Reactors, Materials, and Waste,
- Government Facilities,
- Transportation Systems (including Mass Transit, Aviation, Maritime, Ground/Surface, and Rail and Pipeline Systems),
- Emergency Services,
- Postal and Shipping Services,
- Agriculture and Food,
- Public Health and Healthcare,
- Drinking Water and Waste Water Treatment Systems,
- Energy, including the Production Refining, Storage, and Distribution of Oil and Gas, and Electric Power (except for commercial nuclear power facilities),
- Banking and Finance,
- National Monuments and Icons,
- Defense Industrial Base,
- Critical Manufacturing.

## 2 PAST AND PRESENT INITIATIVES AND POLICIES

There have been several efforts since the 1990s to manage Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) better in the US, and CIIP still plays an important role in the overall US security strategy. The 2007 Strategy for Homeland Security highlights the importance of CIIP for the nation's safety and security: "Many of the Nation's essential and emergency services, as well as our critical infrastructure, rely on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyber attack could be debilitating to our highly interdependent CI/KR and ultimately to our economy and national security" [5].

Whereas traditionally, national security has been recognized as the responsibility of the federal government and is underpinned by the collective efforts of the military, the foreign policy establishment, and the intelligence community with respect to defense, homeland security in general— and CIIP in particular—is viewed as a shared responsibility that requires coordinated action across many sectors [6]. In consequence, a multitude of actors is involved with CIIP. In order to ensure coordination among all relevant stakeholders, the US government has developed various initiatives and policies.

### 2.1 Presidential Commission on Critical Infrastructure Protection (PCCIP)

Based on the recommendations of the Critical Infrastructure Working Group (CIWG), President Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996, the first national effort to address the vulnerabilities of the information age.

The PCCIP included representatives from all relevant government departments as well as from the private sector. The PCCIP presented its report to the president in October 1997 [7]. The commission's most important decision was to foster cooperation and communication between the private sector and the government. The commission no longer exists, as its functions have been reallocated per HSPD-7.

### 2.2 Presidential Decision Directives (PDD) 62 and 63

Clinton followed the recommendations of the PCCIP and issued Presidential Decision Directives (PDD) 62 and 63 in May 1998 [8]. Those directives established policy-making and oversight bodies making use of existing government agency authorities and expertise. PDD-63 set up groups within the federal government to develop and implement plans to protect government-operated infrastructure, and called for a dialog between the government and the private sector to develop a National Infrastructure Assurance Plan [8].

### 2.3 National Plan for Information Systems Protection

On 7 January 2000, Clinton presented the first comprehensive national plan for CIIP—focusing on securing the cyber-components of critical infrastructures, but not the physical components—called Defending America's Cyberspace. National Plan for Information Systems Protection Version 1.0—An Invitation to a Dialogue [9]. This plan reinforced the perception of cyber-security as a responsibility shared between the government and the private sector.

### 2.4 Homeland Security Executive Orders

In the aftermath of attacks in the US on 11 September 2001, President George Bush signed two executive orders (EO) affecting CIP. With EO 13228, entitled Establishing the Office of Homeland Security and the Homeland Security Council and issued on 8 October 2001, the Office of Homeland Security was established, headed by the assistant to the president for homeland security [10]. One of the functions of the assistant to the president is to coordinate efforts to protect the country and its CI from terrorist attacks. The EO further established the Homeland Security Council, which advises and assists the president in all aspects of homeland security.

The second executive order, EO 13231 Critical Infrastructure Protection in the Information Age, established the President's Critical Infrastructure Protection Board. The board's responsibility is to "recommend policies and coordinate programs for protecting information systems for critical infrastructure" [11]. Finally, the EO also established the National Infrastructure Advisory Council (NIAC), a presidential advisory committee of owners and operators of the nation's critical infrastructures [11].

### 2.5 Homeland Security Presidential Directive/HSPD-7

On 17 December 2003, Bush released Homeland Security Presidential Directive/HSPD-7, which supersedes PDD 63 of May 1998, and any presidential directives issued prior to this HSPD-7.

This new directive established a national policy for federal departments and agencies to identify and prioritize US critical infrastructure and key resources and protect them from terrorist attack. It identified the government agencies responsible for coordinating the protection of specific critical infrastructure sectors. A key element of this directive is the designation of federal sector-specific agencies that are charged with collaborating with specific elements of the private sector.

Also, HSPD-7 required that by July 2004, the heads of all federal departments and agencies develop plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate, including identification, prioritization, protection, and contingency planning [12].

Finally, HSPD-7 designated the secretary of homeland security as "the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources" [12].

### 2.6 National Strategies

The National Strategy for Homeland Security was released in July 2002 and established the base for CIP and CIIP in the US. On February 2003, the White House released two presidential national strategies that are follow-on documents to the National Strategy for Homeland Security, namely the National Strategy to Secure Cyberspace and the National Strategy for Physical Protection of Critical Infrastructure and Key Assets.

***2.6.1 National Strategy for Homeland Security.*** In July 2002, the Office of Homeland Security issued the National Strategy for Homeland Security [13] to secure the US from terrorist attacks. It provides direction to the federal government departments and agencies that have a role in homeland security. One of the six "critical mission areas" identified in the strategy is protecting critical infrastructure and key assets.

In October 2007, President Bush issued an updated version of the Strategy for Homeland Security [14]. The protection of critical infrastructures and key resources is maintained as a central element of the strategy. In reference to the National Infrastructure Protection Plan (see below), the strategy defines 17 critical sectors and key resources, each with cross-cutting physical, cyber, and human elements.

***2.6.2 National Strategy to Secure Cyberspace.*** The National Strategy to Secure Cyberspace (NSSC) [15] recognizes that securing cyberspace is an extraordinary challenge that requires a coordinated effort from all parts of society and government. It defines cyberspace as an "interdependent network of information technology infrastructures" and depicts cyberspace as the nervous system or control system of society. Its main aim is to set national policies to engage US citizens in securing the portions of cyberspace they own, operate, control, or with which they interact. The NSSC therefore outlines an initial framework both for organizing and prioritizing national efforts in combating cyber-attacks committed by terrorists, criminals, or nation-states, while highlighting the role of public-private engagement.

Consistent with the National Strategy for Homeland Security, the strategic objectives of the NSSC are:

- To prevent cyber-attacks against the national CI;
- To reduce the national vulnerability to cyber-attacks;
- To minimize damage and recovery time from cyber-attacks.

The strategy recognizes that, as owners and operators of much of the internet infrastructure, the private sector is best equipped and structured to respond to cyber-threats. Therefore, public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

***2.6.3 The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.*** The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets [16] states that the CI sectors of the US provide the foundation for national security, governance, economic vitality, and "the American way of life". Its main aim is to reduce the nation's vulnerability to acts of terrorism by reducing the vulnerability of national critical infrastructure and key assets to physical attack. An attack on the nation's critical infrastructures and key assets could not only result in large-scale human casualties and property destruction, but also damage the national prestige, morale, and confidence, as experienced in the 11 September 2001 attacks. As a result, the following strategic objectives are considered:

- To identify and assure the protection of those infrastructures and assets that are deemed most critical in terms of national-level consequences for public health and safety, governance, economic and national security, and public confidence;
- To provide timely warning;
- To assure the protection of other infrastructures and assets that may become terrorist targets over time.

By pursuing these objectives, coordinated action is required on the part of federal, state, and local governments, as well as the private sector and concerned citizens. The Department of Homeland Security (DHS) provides overall cross-sector coordination in this new organizational scheme, acting as the primary liaison and facilitator for cooperation among federal agencies, state and local government, and the private sector. Cross-sector initiatives should be fostered in the areas of planning and resource allocation, in information-sharing, in personnel security (including background checks where appropriate) and awareness, in research and development, and in modeling, simulation, and analysis.

## 2.7 National Infrastructure Protection Plan (NIPP) and Sector-Specific Plans (SSP)

The National Infrastructure Protection Plan (NIPP) [17] was issued by the DHS in June 2006. It provides an overall framework for existing and future programs and activities for the protection of critical infrastructures and key resources. The NIPP defines three different protection policies: deterrence of the terrorist threat, mitigation of vulnerabilities,

and mitigation of potential consequences. In addition, it specifies key initiatives; lists the public and private actors involved in CIP; sets milestones and targets that are to be achieved; and provides a risk management framework for critical infrastructures.

One of the key elements of the NIPP is that it formalizes the institution of public-private partnerships in the field of CIP and CIIP. Each sector is supposed to create a sector coordinating council for policy coordination and designate an operational entity (such as Information Sharing and Analysis Centers, ISACs) for information sharing. Likewise, the government is to form a Government Coordinating Council and sector-specific agencies for coordinating efforts on specific sectors. This collaboration takes place through the Critical Infrastructure Advisory Council framework, which provides legal protections for this collaboration.

The NIPP gives special consideration to the cyber dimension of critical infrastructure protection. Cybersecurity is addressed in two ways: first, as a cross-sector element that needs to be considered in all sectors; and second, as a major component of the IT sector's responsibility in partnership with the telecommunications sector.

The responsibility of the IT sector is further outlined in the Sector-Specific Plan for Information Technology [18], which was published in May 2007. Sector-Specific Plans (SSPs) complement the NIPP and provide the means by which the NIPP is implemented across all critical infrastructure and key resource sectors. The SSP for the IT sector was developed collaboratively by all relevant public and private actors in the field. The plan outlines the implementation of the NIPP risk management framework; establishes sector-specific goals and objectives; aligns initiatives to meet the goals and objectives; and describes roles and responsibilities.

### 2.8 National Strategy for Information-Sharing

The Strategy for Homeland Security, the National Infrastructure Protection Plan (NIPP), and the Information Technology Sector-Specific Plan all emphasize the importance of information-sharing between different sectors as well as between the government and the private sector. Various organizations and initiatives have been established to enable information-sharing within and among sectors. The National Strategy for Information Sharing [19], which was published in October 2007, builds upon the existing efforts and provides guidelines for sharing information to protect critical infrastructures. The strategy clearly highlights the need to share information with those who need it, rather than to conceal information. It states that "the exchange of information should be the rule, not the exception" [20].

## 3 ORGANIZATIONAL OVERVIEW

In the early days, two agencies had primary responsibility for coordinating US CIP policy: The Critical Infrastructure Assurance Office (CIAO), which used to be part of the Department of Commerce, and the National Infrastructure Protection Center (NIPC), formerly a division within the Federal Bureau of Investigation (FBI). However, in accordance with the various presidential directives discussed above and the creation of the DHS, the functions of the CIAO and the NIPC have been absorbed by the DHS.

Today, DHS coordinates the governmental CIP efforts. However, within the different sectors, various agencies are deeply involved in CIP, for instance as sector-specific

agencies (the National Infrastructure Protection Plan assigns the responsibility for CI/KR protection activities to different federal departments) [21]. Thus, while this section focuses on agencies and offices with a coordinative task (and as a result, mainly on DHS offices), this does not mean that other government agencies are no longer involved in CIP.

## 3.1 Public Agencies

***3.1.1 Department of Homeland Security (DHS).*** The attacks of 11 September 2001 provided the impetus to restructure the overall organizational framework for the protection of homeland security, including CIP and CIIP. In March 2003, 23 federal agencies, programs, and offices were merged to become the Department of Homeland Security (DHS) [22]. The DHS coordinates the efforts of several federal, state, and local governments and encompasses a variety of agencies for all different tasks related to homeland security [23]. Within the DHS, the agencies dealing with CIP and CIIP are affiliated with the National Protection and Programs Directorate, which focuses on the reduction of physical and virtual risks to homeland security [24]. The following two offices are dedicated to deal with CIP and CIIP:

***3.1.2 Office of Infrastructure Protection (OIP).*** The Office of Infrastructure Protection (OIP) [25] coordinates the different sectoral efforts to protect critical infrastructures and key resources (CI/KR). Its functions include:

- Leading a robust organizational framework to facilitate the identification, prioritization, coordination, and protection of critical infrastructures/key resources (CI/KR);
- Developing and maintaining the National Infrastructure Protection Plan (NIPP);
- Coordinating and assisting the vulnerability assessments of all 18 CI/KR sectors in the US and communicating standards to the infrastructure owners/operators and key stakeholders;
- Ensuring the maintenance of a CI/KR sector governance and information-sharing framework;
- Collecting data, analyzing risks to CI/KR, and providing government and private-sector stakeholders with a means of prioritizing resource allocation and assistance;
- Establishing and maintaining international programs and relationships that promote a global culture for the protection of CI/KR.

***3.1.3 Office for Cybersecurity and Communications (CS&C).*** The Office of Cybersecurity and Communications (CS&C) [26] coordinates with the private sector on identifying threats, managing risks and improve situation awareness. In order to be prepared for catastrophic incidents that could damage or even destroy the ICT-network, CS&C has implemented three programs:

- The National Communications System (NCS) [27] has the mission to ensure national security and emergency communication for the federal government under all circumstances.
- The National Cyber Security Division (NCSD) [28] works collaboratively with private, public, and international partners to protect the information infrastructure. It does so by building and maintaining response systems (e.g., US-CERT, see the

chapter on Early Warning and Public Outreach) and by working with security partners to develop and implement risk management programs for cyber-risks in critical infrastructures.

- The Office of Emergency Communications (OEC) [29] develops, implements, and coordinates interoperable and operable communications for emergency response at all levels of government.

***3.1.4 US Department of State.*** With respect to the formulation of an international CIP program in the US, the Department of State has overall statutory authority to conduct foreign affairs, and therefore takes the lead in the interagency process of coordinating international CIP matters. The Department of State collaborates closely with the Department of Defense (DoD) to develop and implement international initiatives designed to encourage allied nations to enhance the security of those critical infrastructure and key resources on which the US military depends for its operations [30].

***3.1.5 Congressional Focus.*** Both Houses of Congress have created bodies to focus on CIIP issues. Within the Committee on Homeland Security in the House of Representatives [31], the following subcommittees deal with questions related to CIP and CIIP:

- Subcommittee on Transportation Security and Critical Infrastructure Protection;
- Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology;
- Subcommittee on Emergency Communications, Preparedness, and Response;
- Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment.

Within the Senate Committee on the Judiciary [32], the Subcommittee on Terrorism, Technology, and Homeland Security has oversight of laws related to government information policy, electronic privacy, security of computer information, and the Freedom of Information Act [33]. The House Government Reform Committee [34] has similar, but not identical, jurisdiction.

The Senate Homeland Security and Government Affairs Committee [35] has overall jurisdiction, for the Senate, on most homeland security issues, including critical infrastructure protection. Its Subcommittee on Federal Financial Management, Government Information, and International Security has jurisdiction on matters related to cyber-security.

***3.1.6 Government Accountability Office (GAO).*** The Government Accountability Office (GAO) [36] is the investigative arm of Congress. It is an independent and nonpartisan body that studies federal government spending and helps to improve the performance and ensure the accountability of the federal government. Congress often asks the GAO to study the programs and expenditures of the federal government. The GAO has released several reports and testimonies addressing critical infrastructure protection and information security. For example:

- In July 2004, the GAO reported on Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sectors. In this report, the GAO recommends that the DHS proceed with the development of an information-sharing plan that defines roles and responsibilities and establishes appropriate policies for interacting with ISACs and the various stakeholders involved [37].

- In May 2005, the GAO reported on Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems, addressing the problems of spam, phishing, and spyware and the resulting security risks to federal information systems [38].
- In May 2005, the GAO reported on Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities. The following issues were identified as key challenges facing the DHS: achieving organizational stability; gaining organizational authority; overcoming hiring and contracting issues; increasing awareness about cyber-security roles and capabilities; establishing effective partnerships with stakeholders and sharing information with these stakeholders [39].
- In May 2005, the GAO report Information Security: Federal Agencies Need to Improve Controls over Wireless Networks advised federal agencies to implement various controls, including policies, practices, and tools, to secure their wireless networks [40].

***3.1.7 Defense Community.*** In May 2007, the DoD published the Sector-Specific Plan for the Defense Industrial Base as input to the National Infrastructure Protection Plan of 2006 [41]. The Defense Industrial Base (DIB) includes the DoD, the US government, and the private sector companies that design, produce, deliver, or maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB does not include commercial communication and information infrastructure, which are addressed by the respective Sector-Specific Plans.

Nevertheless, the information infrastructure is of course crucial for the DoD. The latter has therefore established information assurance programs in the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD/NII) [42] that are headed by a Chief Information Officer of the DoD.

***3.1.8 Computer Crime and Intellectual Property Section (CCIPS).*** The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the Department of Justice is responsible for implementing the department's national strategies in combating computer and intellectual property crimes worldwide. The Computer Crime Initiative is a comprehensive program designed to combat electronic penetration, data theft, and cyber-attacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts [43].

## 3.2 Public-Private Partnerships

The cornerstone of US CIP policy is active cooperation between the public and private sectors. The President's Commission on Critical Infrastructure Protection (PCCIP) concluded that "the need for infrastructure protection creates a zone of shared responsibility and potential cooperation for industry and government" [44]. Since then, public-private partnerships and information-sharing between public and private sectors have been central for CIP efforts in the US. This section provides an overview on the most important organizations and programs for public-private partnerships in the field of critical infrastructure protection and cybersecurity.

***3.2.1 DHS Interagency Committees.*** As the leading department for CIP, it is one of the DHS's main tasks to facilitate partnership efforts between the government and the private sector. The two following interagency committees within the DHS are responsible for coordination and supervision of partnership efforts:

- The National Infrastructure Advisory Council (NIAC) [45] advises the President on the security of the critical infrastructure sectors and their information systems. The council is composed of a maximum of 30 members appointed by the President from private industry, academia, and state and local government;
- Critical Infrastructure Partnership Advisory Council (CIPAC) [46] was established in 2006 to facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial, and tribal governments. CIPAC's membership encompasses representatives from the individual sector coordinating councils as well as from federal, state, local, and tribal governmental entities;
- The president's National Security Telecommunications Advisory Committee (NSTAC) is a CEO-level advisory committee on telecommunications issues.

***3.2.2 Protected Critical Infrastructure Information Program (PCIIP).*** The Protected Critical Infrastructure Information Program (PCIIP) aims to protect certain information shared by the private sector from being disclosed under the federal Freedom of Information Act. Under this program, only people who are trained and certified as PCII-compliant can receive protected critical infrastructure information. The program's goal is to encourage private-sector companies to voluntarily share information so that the DHS and other federal, state, and local analysts can:

- Analyze and secure critical infrastructure and protected systems;
- Identify vulnerabilities and develop risk assessments;
- Enhance recovery preparedness measures [47].

***3.2.3 Information Sharing and Analysis Centers (ISACs).*** Today, most critical infrastructure industry sectors have established their own Information Sharing and Analysis Center (ISAC). Private-sector ISACs are membership organizations managed by the private sector. Each ISAC has a board of directors that determines its institutional and working procedures. The function of an ISAC is to collect, analyze, and share security, incident, and response information among ISAC members and with other ISACs, and to facilitate information exchange between the government and the private sector. The following list gives an overview of the most mature ISACs with regard to CIIP:

- The IT-ISAC started operations in March 2001. Members include 20 major hardware, software, and e-commerce firms, including Microsoft, Intel, CA, Symantec, CSC, IBM, Oracle, Ebay, EWA-IIT, Harris, Hewlett Packard, BAE Systems, IT, and VeriSign, Inc. The ISAC is overseen by a board made up of members, and its operations center is managed by Internet Security Systems; [48]
- The telecommunications industry has established an ISAC through the National Coordinating Center (NCC). Each member firm of the NCC monitors and analyzes its own networks. Incidents are discussed within the NCC, and members decide

whether the suspect behavior is serious enough to report to the appropriate federal authorities; [49]

- The electric power sector has created a decentralized ISAC through its North American Electricity Reliability Council (NERC). Much like the NCC, the NERC monitors and coordinates responses to disruptions in the nation's supply of electricity [50]. The government and industry work together in the NERC to ensure the resilience of the electricity infrastructure in case of potential physical and cyberspace attacks; [51]
- A number of the nation's largest banks, securities firms, insurance companies, and investment companies have joined in a limited liability corporation to form a Financial Services Information Sharing and Analysis Center (FS/ISAC); [52]
- In addition to the individual sector ISACs, several ISAC leaders have convened as an ISAC Council [53]. This council strives to strengthen the relationship between the ISAC community and government, and to solve problems common to all ISACs.

***3.2.4 InfraGard.*** InfraGard is a partnership between industry and the US government as represented by the FBI. The InfraGard initiative was developed to encourage the exchange of information by members of the government and the private sector. With help from the FBI, private-sector members and FBI field representatives form local chapter areas. These chapters set up their own boards to share information among their membership. This information is then disseminated through the InfraGard network and analyzed by the FBI [54].

***3.2.5 National Cyber Security Alliance (NCSA).*** The National Cyber Security Alliance (NCSA) is a cooperative effort between industry and government organizations to foster awareness of cyber-security through educational outreach and public awareness. Its goal is to raise citizens' awareness of the critical role that computer security plays in protecting the nation's internet infrastructure, and to encourage computer users to protect their home and small-business systems [55]. It offers computer security advice and tools for private users as well as small businesses on its website. The NCSA is sponsored by a variety of organizations.

***3.2.6 Partnership for Critical Infrastructure Security (PCIS).*** The Partnership for Critical Infrastructure Security (PCIS) [56] grew out of initiatives outlined in Presidential Decision Directive 63 (PDD 63) as a means to coordinate CIP efforts across critical infrastructure sectors. In October 2005, the National Infrastructure Advisory Council (NIAC) recommended that the PCIS serve as the cross-sector coordinating mechanism, as part of the DHS partnership model. Today, the PCIS serves that role, and its membership consists of the leaders of the various sector coordinating councils. The PCIS works to develop joint policies to secure CI and examines cross-sector issues.

***3.2.7 The Cross Sector Cyber Security Working Group (CSCSWG).*** The Cross Sector Cyber Security Working Group (CSCSWG)[1] serves as a forum to bring together representatives of the government and the private sector to address risk collaboratively across the CI/KR sectors. In this function, it replaces the National Cyber Security Partnership [57], which was the forum for cross-sector coordination until 2005.

The CSCSWG is co-chaired by the industry and the government. It focuses on strategic cross-sector cybersecurity issues such as:

[1]The information on CSCSWG was provided by the US expert involved.

- Identifying opportunities to improve sector coordination around cyber security issues and topics (e.g., the internet, control systems);
- Considering the policy implications of cross-sector cyber dependencies and interdependencies; and
- Providing a conduit for sharing the group's products and findings with the sectors through their Sector Coordinating Council (SCC), Information Sharing and Analysis Center (ISAC), and Sector-Specific Agency (SSA) representatives.

***3.2.8 Institute for Information Infrastructure Protection (I3P).*** The Institute for Information Infrastructure Protection (I3P), managed by Dartmouth College, is a consortium of leading national cyber-security institutions, including academic research centers, government laboratories, and non-profit organizations. Founded in September 2001, the institute's main role is to coordinate a national cyber-security research and development program and to help build bridges between academia, industry, and the government. The I3P identifies and addresses critical research problems in CIIP and opens information channels between researchers, policy-makers, and infrastructure operators [58].

## 4 EARLY WARNING AND PUBLIC OUTREACH

Information-sharing is one of the driving factors behind effective early-warning networks. Many entities focused on information-sharing are also engaged in early-warning activities.

### 4.1 CERT Coordination Center, Carnegie Mellon University

The Computer Emergency Response Team Coordination Center (CERT/CC) is the oldest and still one of the most important early-warning programs in the field of information security. It is a federally funded research and development center operated by Carnegie Mellon University. It was established in 1988 after the Morris worm crashed 10 per cent of the world's internet systems. CERT/CC acts as a coordination hub for experts during security incidents, and works to prevent future incidents.

The CERT/CC acts through several mechanisms. First, its experts research and assess network vulnerabilities and develop risk assessments. Second, they disseminate information to the public through regular security alerts and presentations to the public. Finally, members of the CERT/CC participate in various security groups to improve internet security and network survivability. The CERT/CC is a primary contributor to the US-CERT [59].

### 4.2 US-CERT

On 15 September 2003, the Department of Homeland Security, in conjunction with the CERT Coordination Center (CERT/CC) at Carnegie Mellon University, announced the creation of the US-CERT. The US-CERT works with the National Cyber Security Division (NCSD) of the IAIP to prevent and mitigate cyber-attacks and to reduce vulnerabilities to cybernetic attacks. Together, they have set up the National Cyber Alert System, a trusted warning system offered by the government to help home users and technology experts. It sends e-mails about major virus outbreaks and other internet attacks as they occur, along with detailed instructions to help computer users protect themselves.

The US-CERT initiative is designed to help accelerate the nation's response to cyber-attacks and vulnerabilities. The initiative also enables the DHS to provide expanded analysis, warning, and response coordination [60].

### 4.3 Federal Bureau of Investigation (FBI)

The 1997 PCCIP Report stated that efforts were required to establish a system of surveillance, assessment, early warning, and response mechanisms [61]. The FBI was chosen to serve as the preliminary national warning center for infrastructure attacks and to provide information on law enforcement and intelligence. Under PDD 63, the National Infrastructure Protection Center (NIPC) as part of the FBI was given responsibility for developing analytical capabilities to provide information on changes in threat conditions and newly identified system vulnerabilities, as well as timely warnings of potential and actual attacks [62]. The NIPC, as discussed above, was incorporated into the DHS, but the FBI still retains its responsibilities for addressing cyber-crime.

### 4.4 Information-Sharing and Analysis Centers (ISACs)

The Information Sharing and Analysis Centers (ISACs) serve as an early warning and situational awareness capability by providing a forum for members to report information on threats, vulnerabilities, and incidents. ISACs then collate the information, as well as information they receive from other sources, analyze it, and issue warnings and alerts to members. Many ISACs, such as the IT-ISAC, for example, now distribute information more broadly throughout the sector, beyond its own individual membership (see the chapter on Organizational Overview).

### 4.5 OnGuardOnline.gov

OnGuardOnline.gov provides practical recommendations from the federal government and the technology industry to help users be on guard against internet fraud, to secure their computers, and to protect their personal information. The comprehensive website has tips, articles, videos, and interactive activities. The Federal Trade Commission (FTC) maintains OnGuardOnline.gov with contributions from various government departments, including the DHS [63].

## 5 LAW AND LEGISLATION

### 5.1 Federal Advisory Committee Act (FACA) 1972

One obstacle to fully implementing a robust public-private partnership is the 1972 Federal Advisory Committee Act (FACA). The FACA (Public Law 92-463, 5 U.S.C., App) was enacted by Congress in 1972. Basically, this act is designed to prevent any person or company (or groups of them) from having undue influence in government decision-making. Its purpose was to ensure that advice rendered to the executive branch by the various advisory committees, task forces, boards, and commissions formed over the years by Congress and the president be both objective and accessible to the public. The act not only formalized a process for establishing, operating, overseeing, and terminating these advisory bodies, but also created the Committee Management Secretariat, whose task it is to monitor and report executive branch compliance with the act [64].

In the field of CIP/CIIP, the delicate issue is that CIP is based on partnership with the DHS, which requires meetings. If these meetings are open to the public and subject to other government restrictions, the industry will be unwilling to be frank or overly commit itself, since businesses would be putting sensitive information in the public domain.

In the US, the challenge has been to ensure that the private sector and its representatives have the opportunity to provide comments and input on CIP policy without violating FACA considerations. One solution to this is found in Section 871 of the Homeland Security Act, which gives the Secretary of Homeland Security the authority to create FACA-exempt advisory panels. Secretary Chertoff used the authority granted to him in Section 871 to create a FACA exempt organization to work on CIP issues. This is the Critical Infrastructure Partnership Advisory Council referred to earlier.[2]

### 5.2 Computer Fraud and Abuse Act (CFAA) 1986

In the US, legislative awareness of computer crimes grew dramatically in the early 1980s as computers became increasingly important for the conduct of business and politics. The Computer Fraud and Abuse Act (CFAA) of 1986 was the conclusion of several years of research and discussion among legislators [65]. It established two new felony offenses of unauthorized access to "federal interest" computers[3] and unauthorized trafficking in computer passwords. Violations of the CFAA include intrusions into government, financial, medical, and "federal interest" computers.

The Computer Abuse Amendments Act of 1994 expanded the 1986 CFAA to address the transmission of viruses and other harmful code. The measures provided by this act were further tightened on 26 October 2001 by the USA PATRIOT anti-terrorism legislation.[4] Violations of the CFAA are investigated by the National Computer Crimes Squad at the FBI and supported by its Computer Analysis and Response Team (CART), a specialized unit for computer forensics.[5]

### 5.3 Homeland Security Act 2002

Much of the federal legislation concerning CIP/CIIP was written before the emergence of "cyber-threats". Thus, it is questionable whether a timely and efficient response would be possible under the existing legal frameworks at both federal and state/local levels [66].

While the overall act established the Department of Homeland Security (DHS), Title II of the Homeland Security Act (of 2002) specifically addresses information analysis and infrastructure protection. It transferred the various agencies (like CIAO, NIPC, and others mentioned above) into the DHS, and established the categories of information to which the secretary of homeland defense has access. In order to adequately protect the nation,

[2]Information provided by a US expert involved.

[3]"Federal interest computers" are defined as two or more computers involved in a criminal offense, if they are located in different states.

[4]"Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act". For the full-text version, see: http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf. Privacy and civil liberty advocacy groups have expressed concern over the USA PATRIOT Act and a number of other legislative developments.

[5]http://www.fbi.gov/hq/lab/org/cart.htm. Of further importance is also the recent enactment of the Gramm-Leach-Bliley (GLB) Act and the regulations for implementing it, which address privacy concerns by setting forth a range of requirements to protect customer information. For the text of the GLB Act, see: http://www.ftc.gov/privacy/privacyinitiatives/glbact.html.

the secretary has access to certain intelligence analysis, infrastructure vulnerabilities, and any "raw" data that the president discloses to the secretary.

### 5.4 Freedom of Information Act (FOIA)

CIIP is an important issue in the US, primarily because many of the critical sectors are regulated by the government, but controlled by private entities. As part of the regulation, the private entities must regularly file reports and disclose sensitive information to the government. This could place such information in jeopardy, since under the Freedom of Information Act (FOIA), the public can request such information from the government. However, a FOIA exemption was included in the Homeland Security Act of 2002. Any information regarding critical infrastructures (including security systems, warnings, or interdependency studies) is exempt from disclosure.

After the attacks of 11 September 2001, the Federal Energy Regulatory Commission (FERC) removed certain information from its website and its public reading room. This included detailed maps and other information about electric power facilities and natural gas pipelines. Although exempt from FOIA procedures, this information had traditionally been open and available to anyone who requested it. In February 2003, the FERC ruled that individuals wanting access to this information would have to apply for it. The application requirements include identification information, and take into account the necessity or purpose of accessing the information. Access is granted on a case-by-case basis, and only to individual applicants.

***5.4.1 Critical Infrastructure Information Act: Procedures for Handling Critical Infrastructure Information.*** The Homeland Security Act of 2002 contained a provision called the Critical Infrastructure Information Act, which was designed to encourage the private sector to share information voluntarily with the DHS. In April 2003, the DHS released regulations for the implementation of this program, which the DHS has named the Protected Critical Infrastructure Information Program (PCIIP) [67]. These regulations, which were authorized in the Homeland Security Act of 2002, provide rules for the receipt, care, and storage of critical infrastructure information, the maintenance of security and confidentiality, and methods for dealing with proprietary or business-sensitive information. The basic concept of the regulations again underscores the fundamental principles of public-private partnership. Their goal is to encourage the private sector to share sensitive security information with the DHS without fear that the information will be made public. It stipulates that business-sensitive information that businesses voluntarily submit to the DHS may be labeled CII and exempted from disclosure under the FOIA. Under this program, CII that the DHS shares with state and local governments would be protected from state laws pursuant to the Freedom of Information Act. The final rules implementing this program have not yet been issued. This change in the law has potentially broad effects and requires a change of culture, as disclosure of information held by the government has traditionally been favored in the US.

### 5.5 Terrorism Risk Insurance Act 2002

The Terrorism Risk Insurance Act of 2002 is a new law that creates a federal program for public and private compensation for insured losses resulting from acts of terrorism. All commercial insurance providers must offer terrorism risk insurance, and the federal

government agrees to underwrite some of the losses in the event that a terrorist event takes place. Under this law, an act of terrorism includes any act of violence against elements of the infrastructure [68]. This could include catastrophic network assaults as well as physical attacks.

## ACKNOWLEDGMENT

We acknowledge the contribution of the expert, Scott C. Algeier of IT-ISAC, who validated the content of this chapter.

## REFERENCES

1. http://www.epic.org/privacy/terrorism/hr3162.html, 2008.
2. Department of Homeland Security. (2006). *National Infrastructure Protection Plan*, Washington, DC, p. 3, http://cipp.gmu.edu/archive/NIPP_Plan6-06.pdf.
3. The White House. (2007). *National Strategy for Homeland Security*, Washington, DC, p.27, http://www.whitehouse.gov/infocus/homeland/nshs/NSHS.pdf.
4. The White House. (2003). *Homeland Security Presidential Directive/HSPD-7*, Washington, DC, 17th December 2003, Section 15, http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html.
5. *National Strategy for Homeland Security*, op. cit. p. 28.
6. *National Strategy for Homeland Security*, p. 4f.
7. The President's Commission on Critical Infrastructure Protection (PCCIP). (1997). *Critical Foundations: Protecting America's Infrastructures*, Washington, DC, October 1997.
8. William, J. C. (1998). *Protecting America's Critical Infrastructures: Presidential Decision Directive 63*, Washington, DC, 22 May 1998, http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.
9. William, J. C. (2000). *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0*, An Invitation to a Dialogue,Washington, DC.
10. George, W. B. (2001). *"Executive Order 13228", Establishing the Office of Homeland Security and the Homeland Security Council*, Washington, DC, 8th October 2001, http://www.fas.org/irp/offdocs/eo/eo-13228.htm.
11. George, W. B. (2001). *"Executive Order 13231", Critical Infrastructure Protection in the Information Age*, Washington, DC, 16th October 2001, http://www.fas.org/irp/offdocs/eo/eo-13231.htm.
12. http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html, 2008.
13. Office of Homeland Security. (2002). *National Strategy for Homeland Security*, Washington, DC, July 2002, http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf.
14. National Strategy for Homeland Security. (2007). op. cit.
15. The White House. (2003). *National Strategy to Secure Cyberspace*, Washington, DC, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.
16. The White House. (2003). *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Washington, DC.
17. *National Infrastructure Protection Plan*, op. cit.
18. Department of Homeland Security. (2007). *Information Technology: Critical Infrastructure and Key Resources Sector - Specific Plan as Input to the National Infrastructure Protection Plan*, Washington, DC.

19. The White House. (2007). *National Strategy for Information Sharing*, Washington, DC, http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf.
20. The White House. (2007). *National Strategy for Information Sharing*, Washington, DC, http://www.whitehouse.gov/nsc/infosharing/NSIS_book.pdf, p. 1.
21. *National Infrastructure Protection Plan*, op. cit., p. 92.
22. http://www.dhs.gov/xabout/history/editorial_0133.shtm, 2008.
23. http://www.dhs.gov/xabout/structure/index.shtm, 2008.
24. http://www.dhs.gov/xabout/structure/editorial_0794.shtm, 2008.
25. http://www.dhs.gov/xabout/structure/gc_1185203138955.shtm, 2008.
26. http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm, 2008.
27. http://www.ncs.gov/about.html, 2008.
28. http://www.dhs.gov/xabout/structure/editorial_0839.shtm, 2008.
29. http://www.dhs.gov/xabout/structure/gc_1189774174005.shtm, 2008.
30. http://www.state.gov/t/pm/ppa/icipt, 2008.
31. http://homeland.house.gov/about/index.asp, 2008.
32. http://judiciary.senate.gov, 2008.
33. http://judiciary.senate.gov/subcommittees/110/technology110.cfm, 2008.
34. http://oversight.house.gov, 2008.
35. http://hsgac.senate.gov/public, 2008.
36. http://www.gao.gov/about/index.html, 2008.
37. United States Government Accountability Office (GAO). (2004). *Critical Infrastructure Protection and Improving Information Sharing with Infrastructure Sectors*, GAO-04-780, July 2004, http://www.gao.gov/new.items/d04780.pdf.
38. United States Government Accountability Office (GAO). (2005). *Report to the Congressional Requesters, Information Security. Emerging Cybersecurity Issues Threaten Federal Information Systems*, GAO-05-231, May 2005, http://www.gao.gov/new.items/d05231.pdf.
39. United States Government Accountability Office (GAO). (2005). *Critical Infrastructure Protection. Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434, May 2005, http://www.gao.gov/new.items/d05434.pdf.
40. United States Government Accountability Office (GAO). (2005). *Information Security: Federal Agencies Need to Improve Controls Over Wireless Networks*, GAO-05-383, May 2005, http://www.gao.gov/new.items/d05383.pdf.
41. http://www.dhs.gov/xlibrary/assets/nipp-ssp-defense-industrial-base.pdf, 2008.
42. http://www.defenselink.mil/cio-nii/index.shtml, 2008.
43. http://www.usdoj.gov/criminal/cybercrime/index.html, 2008.
44. The President's Commission on Critical Infrastructure Protection (PCCIP), op. cit, p. 35.
45. http://www.dhs.gov/xlibrary/assets/niac/NIAC_Brochure.pdf, 2008.
46. http://www.dhs.gov/xprevprot/committees/editorial_0843.shtm, 2008.
47. http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm, 2008.
48. https://www.it-isac.org, 2008.
49. http://www.ncs.gov/ncc, 2008.
50. http://www.nerc.com, *Energy Information Sharing and Analysis Center*, http://www.esisac.com/, 2008.
51. http://www.nerc.com/cip.html, 2008.
52. http://www.fsisac.com, 2008.
53. http://www.isaccouncil.org/about, 2008.

54. http://www.infragard.net, 2008.
55. http://www.staysafeonline.info, 2008.
56. http://www.pcis.org/index.htm, 2008.
57. http://www.cyberpartnership.org, 2008.
58. http://www.thei3p.org, 2008.
59. http://www.cert.org, 2008.
60. http://www.uscert.gov, 2008.
61. President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations, op. cit.
62. Presidential Decision Directive 63, op. cit.
63. http://onguardonline.gov/index.html, 2008.
64. http://www.gsa.gov/Portal/gsa/ep/channelView.do?pageTypeId=8203&channelPage=/ep/channel/gsaOverview.jsp&channelId=-13170, 2008.
65. http://www4.law.cornell.edu/uscode/18/1001.html, 2008.
66. President's Commission on Critical Infrastructure Protection (PCCIP), Critical Foundations, op. cit., p. 81.
67. Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18,524 (2003) (to be codified at 6 C.F.R. § 29).
68. Terrorism Risk Insurance Act of 2002, Pub. L. No. 107–297, 116 Stat. 2322.

# EUROPEAN UNION (EU)

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 INTRODUCTION

The European Union is a key player at the international level concerning information assurance. CIIP, the Information Society, and information security are considered key issues. Therefore, the EU has launched initiatives and research programs to study various

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

aspects of the information revolution and its impact on education, business, health, and communications.

The terrorist attacks in Madrid in 2004 and London in 2005 have highlighted the risk of terrorist attacks against European infrastructures in a broader sense. The damage or loss of a piece of infrastructure in one state may have negative effects on several others, and on the European economy as a whole. The following chapter gives a short overview of important steps taken by the EU in the field of CIP and CIIP [1].

## 2 CRITICAL SECTORS

The Communication of the Commission of the European Communities (EU Commission) on Critical Infrastructure Protection in the Fight Against Terrorism, adopted on 20 October 2004, provides a definition of critical infrastructures (CI), enumerates the critical sectors identified, and discusses the criteria for determining potential CI. In the Communication, CI are defined as follows: "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy and key government services"[2].

In the follow-up publication of the EU Commission, the Green Paper on a European Program for Critical Infrastructure Protection (Green Paper on EPCIP) [3], CIIP is defined as: "The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of CII in case of failures, attacks or accidents above a defined minimum level of services and aim at minimizing the recovery and damage. CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with CIP from a holistic perspective" [3].

The Green Paper on EPCIP identifies the following critical sectors and their products and services:

- Energy (Oil and Gas Production, Refining, Treatment and Storage, including Pipelines; Electricity Generation; Transmission of Electricity, Gas, and Oil; Distribution of Electricity, Gas, and Oil),
- Information and Communication Technologies (ICT) (Information System and Network Protection; Internet; Provision of Fixed Telecommunications; Provision of Mobile Telecommunications; Radio Communication and Navigation; Satellite Communication; Broadcasting),
- Water (Provision of Drinking Water; Control of Water Quality; Stemming and Control of Water Quantity),
- Food (Provision of Food and Safeguarding Food Safety and Security),
- Health (Medical and Hospital Care; Medicines, Serums, Vaccines, and Pharmaceuticals; Bio-Laboratories and Bio-Agents),
- Financial System (Payment Services/Payment Structures (private); Government Financial Assignment),
- Public and Legal Order and Safety (Maintaining Public and Legal Order, Safety and Security; Administration of Justice and Detention),

- Civil Administration (Government Functions; Armed Forces; Civil Administration Services; Emergency Services; Postal and Courier Services),
- Transport (Road Transport; Rail Transport; Air Traffic; Inland Waterways Transport; Ocean and Short-Sea Shipping),
- Chemical and Nuclear Industry (Production and Storage/Processing of Chemical and Nuclear Substances; Pipelines of Dangerous Goods (Chemical Substances),
- Space and Research [4].

Although most infrastructures are owned and operated by the private sector, the EU Commission declared in its Communication 574/2001 of 10 October 2001: "The reinforcement of certain security measures by the public authorities in the wake of attacks directed against society as a whole and not at the industry players must be borne by the State. The public sector has therefore a fundamental role to play too" [5].

To determine the criticality of an infrastructure is a complex task. The EU Commission suggests that the following three factors be taken into consideration when identifying potential critical infrastructures:

- *Scope.* the loss of a critical infrastructure element is rated by the extent of the geographic area (international, national, provincial/territorial, or local) that could be affected by its loss or unavailability;
- *Magnitude.* the degree of the impact or loss can be categorized as "none", "minimal", "moderate", or "major". Among the criteria for assessing the potential magnitude of an incident are: public impact (number of citizens affected, loss of life, medical illness, serious injury, evacuation); economic impact (GDP effect, significance of economic loss and/or degradation of products or services); environmental impact (effect on the public and the environment); interdependency (with other critical infrastructure elements); and finally, political impact (confidence in the ability of the government to cope);
- *Effects of time.* this criterion ascertains at what point the loss of an element could have a serious impact (e.g., immediately, within 24 to 48 hours, within one week).

However, in most cases, psychological effects also need to be taken into consideration [6].

## 3 INITIATIVES AND POLICIES

The European Commission plans to launch a policy initiative on Critical Communication and Information Infrastructure Protection (CIIP) in 2008 [7]. The aim is to ensure an adequate and consistent level of protective security and the resilience of critical information infrastructure throughout the European Union. This initiative will be part of the broader framework of the European Programme for Critical Infrastructure Protection (EPCIP) [8] and managed independently by the Information and Media Directorate-General (DG INFSO) [9]. This initiative is the latest development since the European Council recognized the vulnerability and interdependency of underlying infrastructures in June 2004 and asked the Commission and the member states to prepare an overall strategy on critical infrastructure protection.

In response to this request, the Commission issued a Green Paper on the EPCIP in November 2005 [8]. It was followed, in December 2006, by a proposal for a directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection [10].

In parallel, the Commission's strategy [11] for a secure information society stressed that critical infrastructures are also becoming increasingly dependent on the security of their respective information systems. The strategy was acknowledged by a Council Resolution [12], and the creation of an environment enhancing the reliability, resilience, and robustness of communication networks and information systems was promoted by the Council. The main activities undertaken so far by the European Union are addressed below.

### 3.1 Study for the Commission on the Availability and Robustness of Electronic Communication Infrastructures (ARECI)

In preparation for this new action area, Lucent Technologies carried out a study for the Commission on the Availability and Robustness of Electronic Communication Infrastructures (ARECI). The study makes ten recommendations for key actions to be taken by the European Commission, member states, and the private sector to improve the reliability, resilience, and robustness of the underlying infrastructures. These recommendations include the areas of emergency preparedness, priority communications on public networks, formal mutual aid agreements, critical infrastructure information-sharing, inter-infrastructure dependencies, integrity and trusted operation of the supply chain, unified European voice standards, interoperability testing, vigorous ownership and partnering deals, and discretionary European expert best practices. The report was presented in January 2007. Stakeholders were invited to comment on its findings, and contributions were discussed in June 2007 [13].

### 3.2 Green Paper on a European Programme for CIP (EPCIP)

The EC Communication on CIP in the Fight Against Terrorism mentioned above discusses the EU Commission's efforts in the field of CIP and proposes additional measures to strengthen existing instruments, mainly by the establishment of a European Programme for Critical Infrastructure Protection (EPCIP). On 24 November 2005, the EU Commission published a "Green Paper on a European Programme for Critical Infrastructure Protection" [14], which outlines options to enhance prevention, preparedness, and responses in protecting the EU's critical infrastructure. The Green Paper provides options on how the EU Commission may respond to the EU Council's request to establish an EPCIP and a Critical Infrastructure Warning Information Network (CIWIN), and constitutes the second phase of the consultation process that began with the Commission Communication on CIP that was adopted in October 2004.

The Green Paper addresses such key issues as:

- EPCIP's protection aim;
- Key principles;
- The type of framework needed;
- Definitions and a comprehensive list of EU Critical Infrastructures (ECI);
- ECI versus National Critical Infrastructures (NCI);

- The role of CI owners, operators, and users;
- The role of CIWIN, and the evaluation and monitoring of critical infrastructure (interdependencies).

The options presented by the Green Paper on EPCIP are a combination of measures and should be seen as complementary measures to current national efforts.

### 3.3 Critical Infrastructure Warning Information Network (CIWIN)

In order to facilitate the exchange of information on shared threats and vulnerabilities within the EU, the EU Commission is setting up the Critical Infrastructure Warning Information Network (CIWIN). This EU network aims at helping member states, EU institutions, and owners and operators of critical infrastructure to exchange information on shared threats, vulnerabilities, and appropriate measures and strategies to mitigate risk in support of critical infrastructure protection.[1] The precise determination of the nodes of this network is still an open issue and will most likely include authorities at various levels.[2]

The EU Commission suggested the following three possible options for the development of the CIWIN in its Green Paper:

- The CIWIN could take the shape of a forum limited to the exchange of CIP ideas and best practices in support of CI owners and operators;
- The CIWIN could be a rapid alert system (RAS) linking member states with the EC;
- CIWIN could be a multi-level communication and alert system with two distinct functions: a rapid alert system (RAS) linking member states with the EU Commission, and a forum for the exchange of CIP ideas and best practices.

Regardless of the option finally chosen, the CIWIN will complement existing networks and not duplicate them [16].

### 3.4 European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) [17] was created on 14 March 2004. By deciding on 5 June 2003 to set up ENISA as a legal entity, the EU reinforced its efforts to enhance European coordination on information security.

ENISA aims at ensuring a high level of network and information security within the community. Thus, the agency contributes to the development of network and information security for the benefit of the citizens, consumers, enterprises, and public-sector organizations of the EU. This work also contributes to the smooth functioning of the Internal Market.

The agency assists the EU Commission, the member states, and, consequently, the business community in meeting the requirements of network and information security, including present and future EU legislation. ENISA ultimately serves as a center of

[1]The US has a similar system, known as the Critical Infrastructure Warning Information Network (CWIN), which has been operational since 2003. http://www.gao.gov/new.items/d05434.pdf [15].
[2]Information provided by an expert.

expertise both for member states and for EU institutions to seek advice on matters related to network and information security.

ENISA's work programs included several deliverables. It has created a Who is Who Directory on Network and Information Security [18] with contact information for authorities acting in the field of network and information security in the member states. ENISA has also published an Inventory of CERT Activities in Europe [19] and issues a quarterly newsletter. In addition, ENISA organizes workshops for outreach and dissemination of good practices in the member states. Moreover, ENISA defines customized information packages, including good practices for specific target groups (e.g., SMEs and home users). Finally, ENISA has created a network of liaison officers that helps ENISA to exchange information and cooperate on a day-to-day basis with member states [17].

ENISA's latest work program for 2008 is entitled Build on Synergies—Achieve Impact [20], and was released in November 2007. It focuses on increasing the agency's impact in network and information security based on cooperation with relevant stakeholders. The Work Programme has been developed in a new approach of setting priorities in closer cooperation with all stakeholders. It also introduces three new key elements by defining so-called Multi-annual Thematic Programmes (MTP). The current three MTPs cover the following topics [21]:

- Improving resilience in European e-Communication networks;
- Developing and maintaining cooperation models;
- Identifying emerging risks for creating trust and confidence.

It offers an overview of ENISA's activities, including awareness-raising and promotion of best practices, and enhancing cooperation. ENISA is aware of the importance of its role and supports the strategy of the European Commission. In an effort to maximize the impact of its activities, the agency strives to leverage existing synergies and initiatives at the national and European levels and will follow a more focused impact-oriented approach [22].

## 4 RESEARCH AND DEVELOPMENT

### 4.1 Information Society Technologies (IST) FP6 and FP7

The overall objective of the IST (Information Society Technologies) efforts within the EU's Sixth Framework Program (FP6) was to contribute directly to realizing European policies for the information society as agreed at the Lisbon European Council of 2000, the Stockholm European Council of 2001, and the Seville European Council of 2002, and as reflected in the eEurope Action Plan. The IST component of FP6, which ran from 2002 to 2006, aimed at ensuring European leadership in the generic and applied technologies at the heart of the knowledge economy. The IST research efforts within FP6 reinforced and complemented the eEurope 2005 objectives. In this EU research program, IST had the first priority in terms of funding [23]. Among the strategic objectives of IST FP6 were: A global dependability and security framework; semantics-based knowledge systems; networked business and government; e-Safety for road and air transport; e-Health; cognitive systems; embedded systems; improving risk management; and e-Inclusion. As in the preceding FP5, the focus of these projects was mainly on technical issues, whereas

policy aspects (such as organizational aspects, ethical questions, etc.) concerning CIIP were hardly discussed and somewhat undervalued in the strategic objectives.

Under FP7, which began in 2007 and runs until 2013, the EU Commission wishes to identify topical areas of interest that are continued after the end of FP6, as well as new and emerging topics, including space and security [24]. While the EU has been funding research into ICTs since 1986, the Seventh Research Framework Programme is the largest yet [25]. This is due to the commitment that Europe must master both the development and use of ICTs to generate economic growth required to fund its social model and protect its environment and quality of life [23]. More specifically, the objective of ICT research under the EU's FP7 is to improve Europe's competitiveness at all levels by focusing on the following three key areas of ICT [26]:

- Productivity and innovation, by facilitating creativity and management;
- Modernization of public services, such as health, education and transport;
- Advances in science and technology, by supporting cooperation and access to information.

CORDIS is the official portal for participating in FP7 and subsequent related developments in European science and technology [27].

### 4.2 European Security Research Programme (ESRP)

The goal of European security research is to make Europe more secure for its citizens while increasing its industrial competitiveness. By co-operating and coordinating efforts on a European scale, the EU can better understand and respond to risks in a constantly changing world [28]. For projects in the field of security research, the following priority missions were identified:

- Optimizing the security and protection of networked systems;
- Protecting CI against terrorism (including bio-terrorism and incidents involving biological, chemical, and other substances);
- Enhancing crisis management (including evacuation, search and rescue operations, control, and remediation);
- Achieving interoperability and integration of systems for information and communication;
- Improving situation awareness (e.g., in crisis management, anti-terrorism activities, or border control) [29].

Furthermore, the EU Commission set up the European Security Research Advisory Board (ESRAB) on 1 July 2005. ESRAB was attached to the EU Commission and could be consulted on any questions related to the content and implementation of the European Security Research Program. ESRAB carried out its work in full awareness of the European policy context, in particular of the research and development activities carried out at the national level and in support of European research policy initiatives [30]. ESRAB published its final report on 22 September 2006 and ceased its activities on 31 December 2006 [31]. In this report, it recommended the creation of the European Security Research and Innovation Forum (ESRIF) to foster greater dialog and a shared

view of European security needs [32]. In the following, the creation of ESRIF was announced at the 2nd European Conference on Security Research in March 2007, and the forum was established as a public-private dialog in security research in September of the same year.

The main objective of ESRIF is the development of a mid- and long-term Joint Security and Research Agenda that will link security research with security policy-making and its implementation [33]. Based on the understanding that research and public-private partnerships have a role to play in protecting critical infrastructures, the aims of the ESRIF program are [34]:

- To bring together all the relevant stakeholders in order to discuss issues of cross-cutting and common concern;
- To identify proposals for forming a strategic security research and innovation agenda, involving national and European stakeholders, laying out a shared and clear view of European security research needs and priorities; and
- To share ideas, views, and best practices in order to make better use of existing capabilities and to enhance the use of technology in security-related domains.

One main focus of ESRIF is critical information protection. ESRIF is supposed to present a Joint Research Agenda towards the end of 2009, when the forum will be terminated.

### 4.3 Critical Information Infrastructure Research Co-ordination (CI2RCO)

The EU has set up a task force[3] to explore the measures taken by its 25 member states to combat (cyber-) threats against critical infrastructure. As part of the EU's CI2RCO (Critical Information Infrastructure Research Coordination) project, announced in April 2005, the task force aims to identify research groups and programs focusing on IT security in critical infrastructures, such as telecommunications networks and power grids. The scope of the cooperation goes beyond the EU; the task force also wants to include the US, Canada, Australia, and Russia. The CI2RCO project was a Co-ordination Action co-funded under the IST FP6. The main objectives of the CI2RCO project are [35]:

- To encourage a coordinated Europe-wide approach for research and development on CIIP;
- To establish a European Research Area (ERA) on CIIP as part of the larger IST strategic objective of integrating and strengthening the ERA in terms of dependability and security.

CI2RCO focuses on activities and actions across the EU-25 and associate candidate countries. Among other information, the CI2RCO website features the European CIIP Newsletter and upcoming events in the area of CIIP [36].

[3]The European task force includes the Fraunhofer Institute for Secure Information Technology (FhG-SIT); the German Aerospace Center (DLR); the Industrieanlagen-Betriebsgesellschaft (IABG) company; the Italian National Agency for New Technologies, Energy and the Environment (ENEA); the Netherlands Organization for Applied Scientific Research (TNO); the Ecole Nationale Supérieure des Télécommunications; and consulting firm Ernst Basler+Partner.

### 4.4 Service and Software Architectures, Infrastructures, and Engineering

In its Research Framework Programme 7, the European Commission will also provide substantial funding for research into service and software architecture, infrastructure, and engineering. This objective integrates research activities in the areas of services, software, grid, and virtualization technologies [37]. The challenge in achieving pervasive and trusted network and service infrastructures is to look at the converged communication and service infrastructure that will gradually replace the current internet, mobile, fixed, and audiovisual networks. The objective of this research project integrates and builds on the achievements of related work from the IST Programme in FP6. The integrated research effort aims at bringing in world-class participants including European industry, small- and medium-size enterprises, universities, and research institutes, each of which are to contribute their specific skills to ensure success [38].

## 5 LAW AND LEGISLATION

In its legislation on CIIP, the EU went back to the basic principles already enshrined in European law, particularly with regard to the confidentiality of communications and the legal conditions for interception, traffic data retention, legality of content, or intellectual property [39].

### 5.1 Data Protection Directive 1995

The Data Protection Directive (95/46/EC) [40] provides a regulatory framework to guarantee the secure and free movement of personal information across the national borders of EU member countries, and also establishes a baseline of security controls protecting this information [41]. The Data Protection Directive requires that any third country to which data is transferred provide "adequate" data protection.[4]

### 5.2 Directive on Electronic Signature 1999

In to the area of e-Commerce, the Directive on Electronic Signatures (1999/93/CE) [42] has been duly incorporated into the national legislation of member states. This directive outlines requirements for certificates, certification service providers, and secure signature-creation devices, and provides recommendations for secure signature verification. The directive recognizes the potential variety of technologies used to generate signatures, but does not establish detailed technical standards or propose best practices. It also lays the groundwork for the international recognition of certificates.

### 5.3 Directive on Privacy Protection in the Electronic Communications Sector 2002

Directive 95/46/EC has been complemented by Directive 97/66 [43] on the protection of personal data in the field of telecommunications and, of even greater relevance, by the EU Directive on Privacy Protection in the Electronic Communications Sector (2002/58/CE) [44].

[4]Cf. the US Safe Harbor Arrangement as a streamlined process for US companies to comply with the directive, developed by the US Department of Commerce in consultation with the EU. http://www.export.gov/safeharbor/.

The directive clarifies policies on spamming, electronic data collection, and retention by requiring the member countries to adopt legislation providing data confidentiality, limiting the traffic data storage, and providing exceptions for reasons of national security. Moreover, the directive specifies that traffic data is to be deleted or depersonalized as soon as it is no longer needed for sending or preparing invoices, but nonetheless allows member states the possibility "of adopting legislative measures providing for the retention of data for a limited period" [45]. These measures must be "appropriate or proportionate, within a democratic society, to safeguard national security, defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of electronic communication systems" [45].

### 5.4 Framework Directive 2002

The objective of the Framework Directive (2002/21/EC) [46] is to establish a harmonized framework for the regulation of electronic communications networks and services. It lays the foundation in the form of horizontal provisions serving the other measures: the scope and general principles, basic definitions, general provisions on the national regulatory authorities, the new concept of significant market power, and rules for granting certain indispensable resources such as radio frequencies or rights of way.

### 5.5 Council Framework Decision on Attacks Against Information Systems 2005

The European Council Framework Decision on attacks against information systems (2005/222/JHA) [47] of February 2005 aims to strengthen criminal judicial cooperation on attacks against information systems by developing effective tools and procedures. The criminal offences punishable under the framework decision are: illegal access to information systems, illegal system interference (the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, degrading, altering, suppressing, or rendering inaccessible computer data) and illegal data interference. The member states will have to make provisions for such offences to be punished by effective, proportionate, and dissuasive criminal penalties. To enhance cooperation, the member states must establish operational points of contact that are available 24 hours a day and seven days a week.

### 5.6 Directive on Data Retention 2006

In March 2006, the European Parliament and the Council enacted the Directive on the Retention of Data processed in connection with the provision of public electronic communication services or of public communications networks (2006/24/EC, following Commission proposal COM(2005)0438).[5] The directive is designed to harmonize

[5]This directive amends Directive 2002/58/EC: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. Member states had to transpose the requirements of the Directive into national laws by 16 September 2007; however, a grace period of 18 additional months is available. Until 15 March 2009, each member state may postpone application of the Directive to the retention of communications data relating to internet access, internet telephony, and e-mail. Any member state that intends to make use of this provision must notify the Council and the Commission to that effect by way of a declaration. The following member states have made such a declaration postponing application for differing lengths of time: the Netherlands, Austria, the United Kingdom, Estonia, Cyprus, Greece, Luxembourg, Slovenia, Sweden, Lithuania, Latvia, the Czech Republic, Belgium, Poland, Finland, and Germany.

member states' national legislation on the retention of telephone and e-mail data for investigating, detecting, and prosecuting serious crime, as defined by each member state in its national law. The directive applies to traffic and location data on both legal entities and natural persons and to the related data necessary to identify the subscriber or registered user. It does not apply to the content of electronic communications, including information consulted using an electronic communications network. Member states must ensure that communications providers retain communication data for periods of not less than six months and not more than two years from the date of the communication. The measures, drafted by the United Kingdom after the London terrorist bombings in July 2005, require companies to keep a wide range of data, including incoming and outgoing phone numbers; the duration of phone calls; data that can be used to trace fixed or mobile telephone calls; information about text messages; IP addresses, which identify a computer's coordinates on the internet; login and logoff times; and details of e-mail traffic—but not the actual content of communications.[6] Details of connected calls that are unanswered, which can be used to send signals to accomplices or to detonate bombs, will also be archived where that data exists. Independent authorities will be designated to monitor the use of the data, which will have to be deleted at the end of the period unless it is kept for anti-terror investigation purposes.[7]

No later than 15 September 2010, the European Commission is required to submit an evaluation of the application of the Directive and its impact on economic operators and consumers, taking into account further developments in electronic communications technology and the statistics provided to the Commission with a view to determining whether it is necessary to amend the provisions of this Directive, in particular with regard to the list of data and the periods of retention.

### 5.7 Treaty of Lisbon 2007

The Treaty of Lisbon, signed by the heads of state or government of the 27 member states in Lisbon on 13 December 2007, which was scheduled to enter into force on 1 January 2009 in order to reform the EU's constitutional framework, includes provisions for the protection of personal data.[8] The treaty reaffirms the "right to the protection of personal data" (Art. 16 B of the Treaty of Lisbon). Moreover, it states that the European Parliament and the Council shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices, and agencies, and by the member states when carrying out activities that fall within the scope of EU law, and the rules relating to the free movement of such data. Compliance with these rules

[6]The following categories of data must be retained with regard to fixed network telephony and mobile telephony, as well as internet access, e-mail, and internet telephony (see Article 5 of the Directive): (a) data necessary to trace and identify the source of a communication; (b) data necessary to trace and identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication; (d) data necessary to identify the type of communication; (e) data necessary to identify the communication device; (f) data necessary to identify the location of mobile communication equipment.

[7]Each member state must designate a supervisory authority to be responsible for monitoring the application within its territory of the provisions adopted by the member states regarding the security of the stored data (see Article 9 of the Directive). Those authorities may be the same authorities as those referred to in Article 28 of Directive 95/46/EC. The supervisory authority must act with complete independence.

[8]Full text of the Treaty of Lisbon (also known as "the Reform Treaty"): http://europa.eu/lisbon_treaty/full_text/index_en.htm.

shall be subject to the control of independent authorities. As an annex, the Declaration on Article 16 B of the Treaty on the Functioning of the European Union (No. 20) states that whenever rules on the protection of personal data could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. The Declaration on the Protection of Personal Data in the Fields of Judicial Cooperation in Criminal Matters and Police Cooperation (No. 21) acknowledges that specific rules on the protection of personal data and the free movement of such data in the fields of judicial cooperation in criminal matters and police cooperation may be necessary because of the specific nature of these fields.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Marcelo Masera of the Institute for the Protection and Security of the Citizen Joint Research Centre and Martin Wählisch of Humboldt University Berlin, who validated the content of this chapter.

## REFERENCES

1. http://ec.europa.eu/information_society/index_en.htm, 2008.
2. Commission of the European Communities (2004). *Critical Infrastructure Protection in the Fight against Terrorism*, (20 October 2004), COM(2004)702 final, p. 3, Brussels, http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.
3. Commission of the European Communities (2005). *Green Paper on a European Programme for Critical Infrastructure Protection*, (17 November 2005), COM(2005) 576 final, p. 19, Brussels, http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf.
4. *Green Paper on CIP*, op. cit., p. 24.
5. *CIP in the Fight against Terrorism*, op. cit., p. 4.
6. Commission of the European Communities (2004). *Critical Infrastructure Protection in the Fight against Terrorism*, Brussels, (20 October), COM(2004)702 final, pp. 3–5, http://europa.eu.int/comm/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf.
7. http://ec.europa.eu/dgs/information_society/index_en.htm, and: http://ec.europa.eu/information_society/index_en.htm, 2008.
8. http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm, 2008.
9. http://ec.europa.eu/dgs/information_society/index_en.htm, 2008.
10. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006PC0787:EN:NOT, 2008.
11. http://ec.europa.eu/information_society/policy/nis/strategy/index_en.htm, 2008.
12. http://eur-lex.europa.eu/LexUriServ/site/en/oj/2007/c_068/c_06820070324en00010004.pdf, 2008.
13. Both the study and the discussions reports are available here: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/areci_study/index_en.htm, 2008.
14. *Green Paper on CIP*, op. cit.
15. *CIP in the Fight Against Terrorism*, op. cit., p. 10.
16. *Green Paper on CIP*, op. cit.
17. http://www.enisa.europa.eu/index.htm, 2008.

18. European Network and Information Security Agency (ENISA) (2006). *Who is Who Directory on Network and Information Security*, (Version 2.0, December 2006). http://www.enisa.europa.eu/doc/pdf/deliverables/wiw_v2_2006.pdf.
19. European Network and Information Security Agency (ENISA) (2007). *ENISA Inventory of CERT Activities in Europe*, (Version 1.5, September 2007). http://www.enisa.europa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf.
20. European Network and Information Security Agency (ENISA) (2008). *Work Programme 2008: Build on Synergies—Achieve Impact*, http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_2008.pdf.
21. http://www.enisa.europa.eu/pages/02_01_press_2007_11_21_wp_2008.html, 2008.
22. ENISA (2008). *Work Programme 2008*, op. cit., p. 3.
23. http://ec.europa.eu/information_society/research/index_en.htm, 2008.
24. http://ec.europa.eu/research/future/themes/index_en.cfm, 2008.
25. http://ec.europa.eu/information_society/research/eu_research/index_en.htm, 2008.
26. http://cordis.europa.eu/fp7/ict, 2008.
27. http://cordis.europa.eu/ for general overview and http://cordis.europa.eu/ist/ for IST and http://cordis.europa.eu/fp7/ict/ for ICT, respectively, 2008.
28. http://ec.europa.eu/enterprise/security/index_en.htm, 2008.
29. http://cordis.europa.eu/fetch?CALLER=NEWS_SECURITY&ACTION=D&RCN=23324&DOC=6&CAT=NEWS&QUERY=1, 2008.
30. Official Journal of the European Union (2005). *Commission Decision of 22 April 2005 establishing the European Research Advisory Board*, (2005/516/EC).
31. http://ec.europa.eu/enterprise/security/articles/article_2006-04-06_en.htm, 2008.
32. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/346&format=HTML&aged=0&language=EN&guiLanguage=en, 2008.
33. http://www.esrif.eu/objectives.html, 2008.
34. http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/346&format=HTML&aged=0&language=EN&guiLanguage=en, 2008.
35. http://www.attrition.org/pipermail/isn/2005-April/001454.html, 2008.
36. http://www.ci2rco.org/index.asp, 2008.
37. http://cordis.europa.eu/fp7/ict/ssai/home_en.html, 2008.
38. http://cordis.europa.eu/fp7/ict/ssai/overview_en.html, 2008.
39. Alain, E., Hanno, R., and Burkard, S. (2005). *Information security. A new challenge for the EU* , Paris, Chaillot Paper no. 76 (March 2005). http://www.iss.europa.eu/uploads/media/cp076.pdf. Overview of all legislative documents on EU data protection: http://ec.europa.eu/information_society/policy/ecomm/info_centre/documentation/legislation/index_en.htm, and http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm. Website of the EU Commission on Data Protection: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm.
40. http://europa.eu/scadplus/leg/en/lvb/l14012.htm. Status of implementation of Directive 95/46: http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm, 2008.
41. Report on the Economic Evaluation of the Data Protection Directive 95/46/EC: http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/economic_evaluation_en.pdf, 2008.
42. http://ec.europa.eu/information_society/eeurope/2002/action_plan/pdf/esignatures_en.pdf, 2008.
43. http://www.spamlaws.com/f/docs/97-66-ec.pdf, 2008.
44. http://www.jura.uniaugsburg.de/prof/moellers/materialien/materialdateien/010_europaeische_gesetze/eu_richtlinien/ril_2002_058_eg_datenschutz_en/, 2008.

45. http://www.jura.uniaugsburg.de/prof/moellers/materialien/materialdateien/010_europaeische_gesetze/eu_richtlinien/ril_2002_058_eg_datenschutz_en/, Article 15, 2008.
46. http://www.bipt.be/ShowDoc.aspx?objectID=1020&lang=en, 2008.
47. http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_069/l_06920050316en00670071.pdf, 2008.

# THE FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST)

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 INTRODUCTION

FIRST is the global Forum for Incident Response and Security Teams. The organization is widely recognized as a global leader in incident response and brings together a variety of Computer Security Incident Response Teams (CSIRTs) from government, commercial, and education organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information-sharing among members and the community at large. FIRST's vision is that membership should enable incident response teams to respond more effectively to security incidents by providing best practices, tools, and trusted communication with member teams. FIRST's mission statement, which was originally adopted in 1995 and reissued in an updated version in June 2003, holds that FIRST is an international confederation of trusted CSIRTs that cooperatively handle programs to prevent computer security incidents. Moreover,

- FIRST members develop and share technical information, tools, methodologies, processes, and best practices;
- FIRST encourages and promotes the development of quality security products, policies, and services;
- FIRST develops and promulgates best computer and security practices;
- FIRST promotes the creation and expansion of incident response teams and membership from organizations around the world;

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

- FIRST members use their combined knowledge, skills, and experience to promote a safer and more secure global electronic environment [1].

## 2 FIRST HISTORY

FIRST was formed in 1990 in response to the occurrence of major incidents—a computer security incident known as the "internet worm", which brought the internet to its knees in 1988, and the "WANK worm", which highlighted the need for better communication and coordination in 1989. Since that time, it has continued to grow and evolve in response to the changing needs of incident response and security teams and their constituencies. By now, most companies rely on the internet in their daily business transactions. Incident response and security teams continue to form around the globe, covering the growing range of constituencies and member teams of FIRST, including entire countries as well as multi-national organizations and teams from educational and commercial establishments, vendors, the government, and the military [2].

## 3 ORGANIZATION

FIRST consists of a network of individual CSIRTs that work together voluntarily to deal with computer security problems and their prevention. It operates under a formal Operational Framework that describes the governing principles and operating rules for the organization [3]. FIRST exercises no authority over the organization and operation of individual member teams. The general coordination of FIRST activities is provided by the Steering Committee, the Board of Directors, and the Secretariat. Every year, FIRST holds general meetings where members are expected to be represented and the Steering Committee members are elected. In order to address specific topics, special meetings can be called by the chair of the Steering Committee.

There are two types of participants in FIRST. The full members represent organizations that assist an information technology community or another defined constituency in preventing and handling computer-related incidents. Liaison members are individuals or representatives of organizations other than incident response or security teams that have a legitimate interest in and value to FIRST [4].

## 4 GLOBAL INITIATIVES

FIRST is the only worldwide global CSIRT forum, and its members are experts from across the field and from all over the world. With its global scope and its heterogeneous character, FIRST supports and collaborates with existing initiatives to communicate with CSIRT members. As a global umbrella organization, it strives to bring together a wide variety of collaborative and cooperative approaches of the multiple disciplines involved in computer and network security incident response [5].

Mainly, FIRST's global initiatives are introduced in Special Interest Groups (SIG) and in the Corporate Executive Programme (CEP). SIGs exist to provide a forum where FIRST members can discuss topics of common interest to the incident response community. A SIG is a group of individuals composed of FIRST members and invited parties, typically coming together to explore an area of interest or specific technology

area, with the goal of collaborating and sharing expertise and experiences to address common challenges. SIGs generate papers and publications for the industry covering their area of interest. While these papers and publications are distributed by FIRST, they do not represent the official position of the FIRST members, or of FIRST itself [6].

In June 2005, the board and membership of FIRST agreed to fund and establish a unique Corporate Executive Programme (CEP). The aim of the CEP is to bring together cross-functional senior executives with responsibility for decision-making in their organizations. The program caters for heads of departments in HR, finance, operations, technology, security, sales and marketing, research, logistics, legal affairs, and other key business disciplines in all sectors—public and private—across all global regions. The program aims to provide an environment where business leaders can fully appreciate the nature of future threats and risks that global organizations will be facing in the years ahead [7].

## REFERENCES

1. http://www.first.org/about/mission/mission.html, 2008.
2. http://www.first.org/about/history, 2008.
3. http://www.first.org/about/policies/index.html, 2008.
4. http://www.first.org/members/index.html. For a comprehensive membership list, see: http://www.first.org/members/teams/index.html, 2008.
5. http://www.first.org/global, 2008.
6. http://www.first.org/global/sigs, 2008.
7. http://www.first.org/global/cep/index.html/ and http://www.globalcep.com, 2008.

# GROUP OF EIGHT (G8)*

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 INTRODUCTION

Since 1995, the Group of Eight (G8) has become increasingly involved in issues relating to cyber-crime, the Information Society, and Critical Infrastructure Protection. At the

*The Group of Eight Survey of 2006 was reviewed by Harry Hoverd, Home Office, UK. For this edition, the authors have thoroughly updated the Group of Eight survey by referring to open-source material.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

Halifax summit in 1995, a group of senior experts was set up with the task of reviewing and assessing existing international agreements and mechanisms to fight organized crime. This G8 Senior Experts Group took stock extensively and critically before drawing up a catalog of 40 operative recommendations. These recommendations were approved at the G8 summit in Lyon in 1996. The G8 Senior Expert Group, known since then as the Lyon Group, was the first international political forum to fully recognize the significance of high-tech crime. The Lyon Group has since developed into a permanent multi-disciplinary body with numerous specialized sub-working groups. Since October 2001, the Lyon Group meetings have been held together with the Roma Group dealing with combating terrorism (Lyon/Roma Group) [1].

A further important stage for the G8 and CIP/CIIP came in spring 2000. On 15–17 May 2000, government officials and industry participants from G8 countries and other interested parties attended the G8 Paris Conference on Dialogue Between the Public Authorities and Private Sector on Security and Trust in Cyberspace [2]. The aim was to discuss common problems and to find solutions associated with high-tech crime and the exploitation of the internet for criminal purposes. The G8 member states were convinced that a dialog between governments and the private sector was essential in the fight against the illegal or prejudicial use of ICT, and they agreed on defining a clear and transparent framework for addressing cyber-crime [2].

## 2 OKINAWA CHARTER ON GLOBAL INFORMATION SOCIETY

The Okinawa Charter on Global Information Society was published in July 2000 [3]. The charter states that ICT is one of the most potent forces shaping the 21st century, enabling many communities to address social and economic challenges with greater efficiency. One of the key principles and approaches of the charter is that international efforts to develop a global Information Society must be accompanied by coordinated action to foster a crime-free and secure cyberspace. In this respect, the Okinawa charter refers to the OECD Guidelines for Security of Information Systems.[1] Moreover, in the Okinawa Charter, the G8 asked both the public and private sectors to make efforts to bridge the international information and knowledge gap.

## 3 G8 PRINCIPLES FOR PROTECTING CRITICAL INFORMATION INFRASTRUCTURES

G8 members met in Paris in March 2003 for the first multilateral meeting devoted to CIP/CIIP. Top-level experts from G8 member states, together with the major CIP/CIIP operators (e.g., France Telecom for France) came together to define common principles for the protection of vital CI/CII [4]. The 11 clearly defined CIIP principles were adopted on 5 May 2003 by the G8 justice and interior ministers. They cover the following topics [5]:

- Countries should have emergency warning networks regarding cyber-vulnerabilities, threats, and incidents;
- Countries should raise awareness to facilitate stakeholders' understanding of the nature and extent of their CII, and the role each must play in protecting them;

[1] See the survey on the OECD in this volume.

- Countries should examine their infrastructures and identify interdependencies among them, thereby enhancing protection of such infrastructures;
- Countries should promote partnerships among stakeholders, both public and private, to share and analyze information on their critical infrastructure in order to prevent, investigate, and respond to damage to or attacks on such infrastructures;
- Countries should create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations;
- Countries should ensure that data availability policies take into account the need to protect critical information infrastructures;
- Countries should trace attacks on critical information infrastructures and, where appropriate, disclose the results to other countries;
- Countries should conduct training and exercises to enhance their response capabilities and to test continuity and contingency plans in the event of an attack on the information infrastructure, and should encourage stakeholders to engage in similar activities;
- Countries should ensure that they have adequate substantive and procedural laws, such as those outlined in the Council of Europe Cybercrime Convention of 23 November 2001, and trained personnel to enable them to investigate and prosecute attacks on critical information infrastructures, and to coordinate such investigations with other countries as appropriate;
- Countries should engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, by sharing and analyzing information regarding vulnerabilities, threats, and incidents, and by coordinating investigations of attacks on such infrastructures in accordance with domestic laws;
- Countries should promote national and international research and development and encourage the application of security technologies that are certified according to international standards.

With the adoption of these principles, the G8 member states suggested that the emergence of a new "security culture" should encourage them to strengthen international co-operation, to implement the best professional practices in the field of computerized surveillance and alert, to conduct common exercises to test the reaction capabilities in case of incidents, to make other countries aware of the problems, and to invite them to adopt the same main courses of action [6]. The 11 principles are intended to guide national responses to CIIP. However, to this end, it is crucial that the principles be communicated to all parties concerned.

The essential elements of the principles of protecting CII were adopted by the 78th United Nations General Assembly [7]. Resolution 58/199 of January 2004, entitled "Creation of a global culture of cyber security and the protection of critical information infrastructures", is complemented by the annex Elements for Protecting CII, which is based on the 11 principles defined by the G8 in 2003 [8].

The G8 justice and home affairs ministers (the ministerial meeting of the Lyon/Roma Group) met in Washington in May 2004 and endorsed Best Practices for Network Security, Incident Response and Reporting to Law Enforcement. This guide assists network operators and system administrators in responding to computer incidents [9].

## 4 HIGH-TECH CRIME SUB-GROUP ACTIVITIES

One of the sub-groups of the Lyon Group, called the High-Tech Crime sub-group, deals with issues concerning CIIP. The sub-group's goal for CIIP work is to find a way to protect the infrastructure that G8 countries are dependent on, and to provide a more unified approach to multinational companies that deal with a number of G8 countries for setting up an international information-sharing mechanism. Furthermore, the High-Tech Crime sub-group is active in a number of areas, including:

- A CIIP handbook of national contact points. This International CIIP Directory is compiled and maintained by CPNI (UK),[2] and its scope is limited to national governmental organizations. The directory is not available publicly, commercially, or to industry (except on government business);
- CIIP conferences;
- A summary of domestic legal frameworks and avenues of co-operation for addressing illegal internet content;
- Best practice for law enforcement in addressing criminal misuse of wireless networks [10];
- A summary of countries' national legislation regarding law enforcement treatment of encrypted evidence and current trends in criminal use of encryption;
- A standard template for making and responding to requests for 24/7 high-tech investigative assistance;
- A work plan for tackling viruses, worms, and other malicious code.

During its presidency of the G8 for the year 2005, the UK defined the improvement of international co-operation in the field of CIIP as a main objective.

From 15–17 June 2005, a meeting of the justice and home affairs ministers was held in Sheffield. On the basis of this meeting, the justice and home affairs ministers published a communiqué on CIIP. The communiqué refers to the Unified Response Tabletop Exercise hosted in New Orleans by the G8 High-Tech Crime sub-group in May 2005, where various experts in law enforcement, watch and warning, and industry met to find solutions to challenges in the field of CIIP. The communiqué also outlines areas where further action is required:

- To continue to enhance communication and information-sharing between watch and warning organizations and law enforcement agencies;
- To ensure that all G8 countries have, and encourage other countries to develop, watch and warning organizations able to detect vulnerabilities and threats;
- To ensure that law enforcement agencies can quickly respond to serious cyber-threats and incidents;
- To continue and strengthen cooperation with the private sector;
- To continue to conduct national and multinational training and exercises.

At the same meeting in Sheffield in June 2005, the High-Tech Crime sub-group released a further paper on Best Practices for Law Enforcement Interaction with Victim-Companies During a Cyber-Crime investigation [11].

[2]See the country survey on the UK in this volume.

## ACKNOWLEDGMENT

We acknowledge the contribution of the expert, Harry Hoverd of the Home Office, United Kingdom, who validated the content of this chapter.

## REFERENCES

1. http://www.auswaertiges-amt.de/diplo/de/Aussenpolitik/Themen/TerrorismusOK/TerrorismusbekaempfungG8.html#t2l, 2008.
2. http://www.g8.utoronto.ca/crime/paris2000.htm, 2008.
3. http://www.g7.utoronto.ca/summit/2000okinawa/gis.htm, 2008.
4. http://www.g7.utoronto.ca/summit/2003evian/press_statement_march24_2003.html, 2008.
5. http://www.usdoj.gov/ag/events/g82004/G8_CIIP_Principles.pdf, 2008.
6. *G8 Principles for Protecting Critical Information Infrastructures*, NISCC Quarterly (April–June 2003), p. 9.
7. http://www.usdoj.gov/ag/events/g82004/Communique_2004_G8_JHA_Ministerial_051204.pdf, 2008.
8. http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf, 2008.
9. http://www.usdoj.gov/ag/events/g82004/G8_Best_Practices_Network_Security.pdf, 2008.
10. http://www.homeoffice.gov.uk/documents/G8-WLANBstPrcNov04.pdf?version=1, 2008.
11. http://www.libertysecurity.org/article396.html, 2008.

# NORTH ATLANTIC TREATY ORGANIZATION (NATO)

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 INTRODUCTION

Critical Infrastructure Protection remains one of the key areas of work of the Civil Emergency Planning in the North Atlantic Treaty Organization (NATO). The Ministerial

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

Guidance for NATO Civil Emergency Planning (CEP) for 2007–2008 includes several references to critical infrastructure protection, while the Updated Civil Emergency Planning Action Plan for the improvement of civil preparedness against possible chemical, biological, radiological, and nuclear (CBRN) attacks includes several action items related to the CIP field of work. In line with the Concept Paper approved in 2003, the Senior Civil Emergency Planning Committee (SCEPC) and its eight Planning Boards and Committees (PB&Cs) will continue to examine critical infrastructure protection from a functional perspective, and to provide integrated contributions from the areas of expertise of all Planning Boards and Committees.

## 2 CIVIL COMMUNICATION PLANNING COMMITTEE (CCPC)

The Civil Communication Planning Committee (CCPC) is responsible for reviewing existing and planned electronic public and non-public communications infrastructures, services, associated facilities, postal services, and any related services with a view to determining their ability to meet the requirements of all vital users (civil and military) during emergencies. Recommendations are made to nations, taking into consideration new and emerging technology, national legislation and arrangements, and the role of international organizations in this field.

The CCPC has published a number of documents and studies on civil communications infrastructures, such as

- Critical telecommunications infrastructure protection;[1]
- CEP consequences of disruption of critical postal infrastructure;[2]
- New risks and threats to civil telecommunications;[3]
- CEP requirements for coordinated national telecommunications regulatory measures;
- New risks and threats to the postal services.[4]

In addition, the CCPC has contributed to the "North Atlantic Council's Action Plan on Cyber Defense", such as:

- CEP consequences of the introduction of the Computer Emergency Response Teams (CERTs)/CEP regarding cyber-attacks and information warfare on critical civil communication infrastructure;
- Identification and assessment of the interdependencies of other critical infrastructures on civil communication networks;
- Impact of Information Society developments and related opportunities for NATO CEP.

[1]NATO document: EAPC(CCPC)D(2002)8.
[2]NATO document: EAPC(CCPC)D(2003)2.
[3]NATO document: EAPC(CCPC)WP(2002)1, REV1.
[4]NATO document: EAPC(CCPC)D(2003)1.

The Bucharest Summit declaration of 2008 in its paragraph 47 states that "NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defence and are developing the structures and authorities to carry it out. Our Policy on Cyber Defence emphasis the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices, and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defence capabilities and strengthening the linkages between NATO and national authorities".[5] On 15 May 2008, at the initiative of Estonia, top military commanders from seven NATO countries and the Allied Command Transformation signed an agreement to create a Cooperative Cyber Defense Center in Tallinn. The cyber-attacks on Estonia in 2007 highlighted for the first time the potential vulnerability of NATO countries, their institutions and societies, an even NATO itself to disruption by penetration of their information and communication systems.[6] The goal of NATO policy and of the center is to assist allied countries as needed in protecting their critical communication and information networks [1].

## 3 CIVIL PROTECTION COMMITTEE (CPC)

The work of the Civil Protection Committee (CPC) in the CIP field started in 2001, when an Ad Hoc Group (AHG) on CIP was established. One of the first tasks of this AHG was to conduct a mapping survey of critical infrastructure. Nations were invited to indicate how they were structurally organized to deal with critical infrastructure protection, and to give indications about their state of readiness in terms of planning and infrastructure mapping.[7] Based on this initial mapping, definitional and conceptual work was undertaken by the AHG on CIP, resulting in a Critical Infrastructure Protection Concept Paper, approved by the SCEPC on 6 November 2003.

The Concept Paper not only proposed a way for work to be carried out by the CPC in this field, but also contained a road map detailing immediate, mid-term, and long-term actions. Also attached were a scenario to further explain the concept and a glossary of frequently-used CIP terms.

In 2005, the CPC conducted a seminar on the theme of Critical Infrastructure Protection (CIP)—Education, which aimed to raise awareness of the importance of CIP. The primary results expected from the seminar were sets of teaching points that could form part of a CIP course curriculum and recommendations for next steps regarding the CIP concept. The AHG is considering ways to develop further training and education activities on the basis of the seminar outcomes.[8]

Among other training activities, the CPC in 2007 organized a table-top exercise attended by representatives of more than 20 NATO, Euro-Atlantic Partnership Council (EAPC), Mediterranean Dialogue (MD), and Istanbul Cooperation Initiative (ICI)

[5]Bucharest Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on 3 April 2008. http://www.summitbucharest.ro/en/doc_201.html.
[6]For more information about these incidents, see the chapter on Estonia.
[7]NATO document: EAPC(CPC)N(2002)6.
[8]Information provided by an expert.

countries and by representatives of NATO Military Authorities. The exercise aimed at increasing the understanding of:

- The vulnerabilities of and interdependencies between various critical infrastructures, including energy-related critical infrastructures;
- The bottlenecks that arise in decision-making at the national and international levels;
- The best practices in disaster response with regard to CIP.

In early 2008, the AHG was reorganized. Its work priorities over the next two years will be to update the Road Map and, if needed, the Concept Paper; to set up an information exchange tool to be used by different civil emergency planning stakeholders and to step up the work on addressing CIP interdependencies.[8]

## 4 INDUSTRIAL PLANNING COMMITTEE (IPC)

In 2003, an Industrial Planning Committee (IPC) seminar in Slovakia was attended by senior officials and representatives from EAPC governments, industry, and trade. The aim of the seminar was to examine industrial interdependencies and resulting vulnerabilities, and to discuss potential preventive and/or consequence-management measures. These issues were introduced by plenary presentations, including two case studies—a Canadian paper on industrial interdependencies and a Slovak case study on aspects of electricity, water, gas, and chemical utilities. Other presentations looked at

- Preventive measures for the protection of critical infrastructure;
- The military experience in infrastructure protection in France;
- Protecting critical infrastructure during disasters.

Following this initial seminar, and based on a questionnaire circulated in April 2003[9] and replies to it,[10] the IPC agreed to develop a guide containing criteria for identifying critical infrastructure in industry and the energy sector, and to compile active and passive methods of critical infrastructure protection. The IPC also established an Ad-Hoc Working Group on Energy CIP (AHWG) for appropriate action. The group agreed that energy-related CI consists of three main infrastructures:

- Systems of electricity generation, transmission, and delivery;
- Systems of natural gas production, transmission, and delivery;and
- Systems of oil production, transportation, refining, and delivery.

The IPC initially concentrated on the protection of critical electricity infrastructure. In 2005, it held a seminar on the topic of Protection of Electricity-Related Critical Infrastructure against Security Related Hazards". Subsequently, in October 2006, the IPC

[9]NATO document: EAPC(IPC)N(2003)6.
[10]NATO document: EAPC(IPC)WP(2003)2.

Vital Resources Seminar on Energy Critical Infrastructure Protection was held. Drawing on the discussions and recommendations of the seminar, the committee has compiled a collection of best practices on the protection of energy CIP as well as on the protection of electricity CIP. In 2007, the IPC seminar addressed the issue of CIP related to gas deliveries. A collection of best practices on protecting critical gas-related infrastructures is currently being drafted.[8]

The Bucharest NATO Summit Declaration states in Paragraph 48: "We have noted a report 'NATO's Role in Energy Security', prepared in response to the tasking of the Riga Summit. Allies have identified principles which will govern NATO's approach in this field, and outlines options and recommendations for further activities. Based on these principles, NATO will engage in the following fields: information and intelligence fusion and sharing; projecting stability; advancing international and regional cooperation; supporting consequence management; and supporting the protection of critical energy infrastructure" [2].

## 5 FOOD AND AGRICULTURE PLANNING COMMITTEE (FAPC)

The Food and Agriculture Planning Committee (FAPC) looks at the impact of CIP on food, agriculture, and water production. In particular, the FAPC looks at threats, risks, and vulnerabilities affecting the water sector. In doing so, the FAPC has chosen a multi-disciplinary training approach, which will make better use of the wealth of knowledge of all NATO experts by bringing them together to work on this subject under exercise conditions. Other planning boards and committees, particularly the Transport and Telecommunications Committees, work jointly with the FAPC.

## 6 CIVIL AVIATION PLANNING COMMITTEE (CAPC)

The Civil Aviation Planning Committee (CAPC) has begun identifying critical infrastructure vulnerabilities and possible protective measures in the area of civil aviation. While the protection of airports, equipment, and resources is primarily a national responsibility, the Civil Aviation Working Group has discussed minimum standards that can help to make national efforts more effective. Any large-scale military deployment would require the transport capabilities of the civil aviation sector and the related infrastructure elements, which together with the air traffic control network, the power grid, fuel supplies, and supporting surface transportation are essential parts of NATO's deployment capability.

## 7 PLANNING BOARD FOR INLAND SURFACE TRANSPORTATION (PBIST)

The Planning Board for Inland Surface Transportation (PBIST) has conducted exploratory and definitional work on problems that may result from attacks on critical inland surface transport infrastructure. A PBIST report emphasizes that the civilian transport infrastructure is considered an attractive target, as global trade depends heavily on transportation.[11]

[11] NATO document: EAPC(PBIST)D(2003)8.

The report aims to reach conclusions on threats to the inland transport infrastructure, characteristics of likely targets, possible protective measures, and the potential role of the PBIST.

## 8 PLANNING BOARD FOR OCEAN SHIPPING (PBOS)

At the behest of the NATO Council and the SCEPC, the Planning Board for Ocean Shipping (PBOS) continues to serve as the NATO focal point for advice and assistance on the protection of civilian maritime assets against acts of terrorism. This work includes: monitoring the work and activities of other international bodies, gathering and exchanging information from international and national sources, and providing advice and assistance as necessary.

## 9 COORDINATION

Overall responsibility for coordinating CIP work lies with the SCEPC. However, on the initiative of the CPC, representatives of the Planning Boards & Committees (PB&Cs) meet on a regular basis to discuss various issues related to CIP. These meetings are an opportunity for all PB&Cs to present work that is under way and/or planned within their respective areas of interest, in addition to fostering closer cooperation and coordination.

## 10 SPECIAL REPORT TO THE NATO PARLIAMENTARY ASSEMBLY 2007

Lord Jopling from the United Kingdom was nominated Special Rapporteur and delivered a report on the protection of critical infrastructures [3] to the NATO Parliamentary Assembly in the 2007 annual session. This report strives to outline the critical infrastructure policies of NATO and also of its individual member countries. It collects the various definitions, highlights their commonalities and differences, and tries to attribute responsibilities by identifying the CIP stakeholders and the sectoral policies including CIIP; energy security, civil aviation security, and port security.

## ACKNOWLEDGMENT

We acknowledge the contribution of the expert, Denisa-Elena Ionete of Civil Emergency Planning, NATO Headquarters, who validated the content of this chapter.

## REFERENCES

1. Vladimir, S. (2008). NATO creates cyber defense center in Estonia. *Eurasia Dly. Monit*. **5**(93)(15 May). http://www.jamestown.org/edm/article.php?article_id=2373060.
2. Heads of State and Government. (2008). Bucharest Summit Declaration. *Meeting of the North Atlantic Council*. Bucharest. http://www.summitbucharest.ro/en/doc201.html.
3. http://www.nato-pa.int/default.asp?SHORTCUT=1165, 2008.

# ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD)*

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 INTRODUCTION

The Organisation for Economic Co-operation and Development (OECD) has a long history and expertise in developing policy guidance for the security of information systems and networks, including critical information infrastructures. The OECD is also committed to the fight against cyber-crime; notably, it fights against the use of malicious software. The OECD produces analytical reports, statistics, and policy guidance (declarations and recommendations) to help governments and businesses develop consistent policies to strengthen information security, to raise public awareness about the importance of information security for the internet economy, and, more broadly, to develop a culture of security across society. There is a consensus among the member countries that secure and reliable (information) infrastructures and services are a necessary requirement for trustworthy e-Commerce, secure transactions, and personal data protection. This is the main reason why the OECD Working Party on Information Security and Privacy (WPISP) promotes a global approach to policy-making in these areas to help build trust online [1]. In addition, the Committee for Information, Computer and Communications Policy (ICCP) analyzes the broad policy framework underlying the e-Economy, information infrastructures, and the Information Society [2].

## 2 OECD GUIDELINES FOR THE SECURITY OF INFORMATION SYSTEMS AND NETWORKS: TOWARDS A CULTURE OF SECURITY

The attacks of 11 September 2001 in the US marked a turning point for the OECD's efforts for information security and CIIP. In order to improve measures against cyber-crime, computer viruses, and hacking, the OECD drew up new guidelines. At its 1037th session on 25 July 2002, the OECD Council adopted the new Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security [3]. The guidelines are not binding. However, they are the result of a consensus between OECD governments

*The OECD Survey of 2008 was reviewed by Anne Carblanc, OECD.

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

and of discussions involving representatives of the information technology industry, business users, and civil society [4]. The OECD invites governments in other countries to adopt a similar approach to CIIP. Furthermore, the private-sector representatives are asked to improve security in their own environment and to provide security information and updates to the users. The individual users are urged to be more aware and responsible, and also to take the best preventive measures possible to decrease the risks to CI/CII. The OECD Guidelines include the following complementary principles at the policy and operational levels [5]:

1. *Awareness.* Participants should be aware of the need for security of information systems and networks and of options to enhance security;
2. *Responsibility.* All participants are responsible for the security of information systems and networks;
3. *Response.* Participants should act in a timely and co-operative manner to prevent, detect, and respond to security incidents;
4. *Ethics.* Participants should respect the legitimate interests of others;
5. *Democracy.* The security of information systems and networks should be compatible with the essential values of a democratic society;
6. *Risk assessment.* Participants should conduct risk assessment;
7. *Security design and implementation.* Participants should incorporate security as an essential element of information systems and networks;
8. *Security management.* Participants should adopt a comprehensive approach to security management;
9. *Reassessment.* Participants should review and reassess the security of information systems and networks and make appropriate modifications to security policies, practices, measures, and procedures.

## 3 OECD GUIDELINES FOR THE PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES

In 2008, the OECD Council plans to adopt a Recommendation on the Protection of Critical Information Infrastructures (CII).[1] This document highlights the relevance of the Security Guidelines to CII. It provides guidance on national policies and proposes ways to improve international cooperation for the protection of CII. The guidance derives from best practices identified in an OECD comparative study of CII policies in seven countries.

The recommendation identifies the need for strengthened international cooperation to address cross-border issues, given the importance of the internet as a global infrastructure. It also identifies the need for a national operational infrastructure security capability, a willingness and ability to share information, close cooperation with the relevant parts of the private sector, and a strong culture of security in the face of rapid technological growth and consequential social changes. The recommendation therefore calls on member

[1]The expression CII used in the OECD recommendation refers to those information networks and systems the failure of which would have a serious impact on the health, safety, security, and economic well-being of citizens, or the effective functioning of government or the economy. The adoption of this document was planned for the OECD Ministerial Meeting on the Future of the Internet Economy in Seoul, Korea, 16–18 June 2008. http://www.biac.org/members/iccp/mtg/2008-06-seoul-min/seoul2008 ministerial documents.asp.

countries to adopt a common approach in a number of areas to enable progress on some of these issues. Further, although the recommendation is addressed to governments, it stresses the need for collaboration with the private sector.

The OECD recommendation is timely. First, critical infrastructures are increasingly interdependent and reliant on the effective functioning of information and communication technologies. For example, the monitoring and control systems of power grids and hydroelectric power plants are often dependent on the functioning of underlying internet protocol-based networks. Further, most industrial control systems that monitor and control critical processes are now increasingly being connected directly or indirectly (through corporate networks) to the internet and therefore face a new set of threats. Also, as shown in the OECD-APEC Analytical Report on Malware [6], there is increasing malicious activity online, which adversely affects all internet users and activities, and unfortunately, critical information systems have not proven immune to this phenomenon.[2]

## 4 CULTURE OF SECURITY WEBSITE

In December 2003, the OECD launched the Culture of Security website as part of the organization's initiative to promote a global culture of security. The site primarily provides member and non-member governments with an international information-exchange tool on initiatives to implement the OECD Security Guidelines. The OECD website provides an overview of [7]:

- OECD work in the area of security of information systems and networks since the adoption of the Security Guidelines in 2002;
- National implementation initiatives: Activities in various countries to apply the OECD Security Guidelines at the national level;
- Selection of practical tools: Countries are developing various useful tools to encourage awareness, education, and individual responsibility;
- International co-operation: Action taken by governments and international organizations at the regional or international levels to co-operate among themselves and/or with other participants.

## 5 OECD FORUMS AND WORKSHOPS

Other OECD efforts concerning CIIP included the OECD-APEC Global Forum on Policy Frameworks for the Digital Economy, held in Honolulu in January 2003, and the OECD Global Forum on Information Systems and Network Security, which was convened in Oslo in October 2003 [8]. The Honolulu Forum emphasized the importance of the security of information systems and networks, as well as the need for the OECD to implement the OECD Security Guidelines. Furthermore, it emphasized the importance of preparing for the World Summit on the Information Society (WSIS) in December 2003 in Geneva (Switzerland). Many Asia-Pacific Economic Cooperation (APEC) member countries were invited to the Oslo conference due to an agreement made in Honolulu

[2]Information provided by an expert.

to increase co-operation between the OECD and APEC. This was another major step towards international and transnational management of CIIP efforts.

Among the main intended policy impacts of the Oslo Forum were:

- Raising awareness of the importance of secure information systems and networks for safeguarding critical infrastructures, as well as business and consumer information;
- Increasing knowledge of the OECD Security Guidelines;
- Encouraging the development and the promotion of security architectures that effectively protect the information systems of organizations;
- Exploring the use of technology and security standards in safeguarding IT infrastructures.

In September 2005, an OECD-APEC Workshop on Security of Information Systems and Networks was held in Seoul (South Korea). Topics discussed included spyware, reaching out to SMEs and individuals, promoting effective global incident response (e.g., the roles of governments and CERTs/CSIRTs), emerging security threats and the technologies being developed to address them, as well as the role of research and development, and finally, a comparison of legislative and policy approaches to improve the management and security of information systems and networks [9].

In March 2006, the OECD together with the US National Science Foundation held a workshop on The Future of the Internet in Paris. The event marked the beginning of the project on the future of the internet by the OECD Committee for Information, Computer and Communications Policy (ICCP) [10]. Following up on this workshop, in 2007, the OECD again co-organized a workshop together with the US National Science Foundation on the Social and Economic Factors Shaping the Future of the Internet. The goal of this second workshop was the discussion of strategic directions for the future of the internet, from both the technological and the policy viewpoints [11].

From 16–18 June 2008, ministers, business leaders, technical experts, academics, and civil society representatives from the 30 OECD countries and more than 15 other economies will meet in Seoul, Korea, to discuss the Future of the Internet Economy and agree new ways to improve global dialog, co-ordination, and co-operation on policies and practices to form an enabling environment for the internet economy.

Strengthening the security of the internet and other information systems and networks, including CII, will be one of the key issues addressed at the ministerial meeting.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts, Anne Carblanc and Peter Lübkert and Laurent Bernat of the Organization for Economic Cooperation and Development, who validated the content of this chapter.

## REFERENCES

1. http://www.oecd.org/document/46/0,3343,en_2649_34255_36862382_1_1_1_1,00.html, 2008.
2. http://www.oecd.org/department/0,2688,en_2649_34223_1_1_1_1_1,00.html, 2008.

3. http://www.oecd.org/document/42/0,2340,es_2649_34255_15582250_1_1_1_1,00.html, 2008.
4. http://www.oecd.org/dataoecd/23/11/31670189.pdf, 2008.
5. OECD (2002). *Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security*, p. 10ff. http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.
6. http://www.oecd.org/dataoecd/37/60/38738890.pdf, 2008.
7. http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase, 2008.
8. http://www.oecd.org/document/38/0,3343,es_2649_34255_16193702_1_1_1_1,00.html, 2008.
9. http://www.oecd.org/document/25/0,2340,en_2649_201185_35481241_1_1_1_1,00.html, 2008.
10. http://www.oecd.org/dataoecd/26/36/37422724.pdf, 2008.
11. http://www.oecd.org/document/4/0,3343,es_2649_34255_39046340_1_1_1_1,00.html, 2008.

# UNITED NATIONS (UN)

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 INTRODUCTION

Issues related to CIIP have been discussed by the United Nations (UN) and its system of organizations since the end of the 1980s. However, formal CIIP efforts are a more recent phenomenon. Several initiatives have since been undertaken towards better work coordination. Among these are initiatives taken by UN institutions, several UN resolutions, and the results of the World Summit on the Information Society (WSIS).

## 2 UN INSTITUTE FOR DISARMAMENT RESEARCH (UNIDIR)

An important first step was the organization of a workshop in July 1999 by the UN Institute for Disarmament Research (UNDIR) in Geneva. The main topic was how to better

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

achieve worldwide information security and assurance in a global digital environment. In this context, a variety of issues, such as the Revolution in Military Affairs (RMA) and the proliferation of offensive tools for attacking information systems and networks, were discussed in Geneva. There was consensus among the participants that the vulnerability of national and international information infrastructures to cyber-attacks was increasing, and that international cooperation had to be improved in order to meet this challenge. One other conclusion was that the issue of CIIP is not only of military or strategic importance, but that it is mainly a political, economic, and social issue [1]. Hence, it is crucial to achieve cooperation between public and private actors as well as between nations.

## 3 UN GENERAL ASSEMBLY RESOLUTIONS

In December 2000 and 2001, the 55th and 56th UN General Assemblies issued Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" [2]. This was another important step in the efforts of the UN concerning CIIP. These resolutions emphasize in particular that the Commission on Crime Prevention and Criminal Justice is intended to make law enforcement more efficient and effective. Furthermore, the importance of cooperation among countries and between the public and private sectors was stressed once again. The resolutions also mention the Convention on Cybercrime of the Council of Europe and the work done by the G8 as crucial milestones in the international field [2].

In December 2002, the 57th UN General Assembly issued Resolution 57/239 on the "Creation of a global culture of cyber-security" [3]. This resolution emphasizes that effective cyber-security not only requires action at the governmental level, but must be supported throughout society. Therefore, it points out the different actors responsible in the field of cyber-security, namely, governments, businesses, and other organizations, as well as individual owners and users of information technologies. The resolution further recognizes once more the importance of international cooperation. The annex outlines nine complementary elements required to create a global culture of cyber-security. They range from awareness of the need for security of information systems and networks, to identifying adequate action in the field of CIIP (taking into account ethical and democratic principles), to security management and reassessment [3].

In December 2003, the 28th UN General Assembly issued Resolution 58/199 on the "Creation of a global culture of cyber-security and the protection of critical information infrastructure" [4]. This resolution points out the increasing links among most countries' critical infrastructure and the growing number and variety of threats facing them. The resolution's annex outlines 11 principles for protecting CII, which are based on those adopted by the G8 Justice and Interior Ministers in Paris in 2003. The UN General Assembly invites member states and international organizations to consider these principles for protecting CII, as well as to share their best practices and measures that could assist other actors in their efforts to achieve cyber-security. Furthermore, the resolution asks that these principles be taken into account in preparations for the second phase of the World Summit on the Information Society (WSIS) in Tunisia in November 2005. Finally, the UN General Assembly outlines the necessity of involving the developing and the least developed countries in CIIP, which means that the transfer of information technology and capacity-building efforts need to be strengthened [4]. In the subsequent years, the UN General Assembly regularly adopted a resolution on the "Developments

in the field of information and telecommunications in the context of international security" [5]. Referring to the earlier resolutions, the member states are repeatedly called upon to promote further the consideration of existing and potential threats in the field of information security, as well as possible measure to limit the threats emerging in the field. Moreover, the secretary-general, with the assistance of a group of experts (to be established by 2009), is requested to continue to study existing and potential threats in the sphere of information security and possible cooperative measures to address them.

In 2005 and 2006, two subsequent resolutions on WSIS were adopted. The first one urges member states to support and actively contribute to the success of the Tunis Summit, as well as its aims and goals. The second one requests that the Economic and Social Council (ECOSOC) oversee the system-wide follow-up of the Geneva and Tunis outcomes of the summit [6]. Furthermore, it proclaims an annual World Information Society Day (17 May) and calls for an overall review of the implementation of the summit outcomes in 2015.

## 4 UN ICT TASK FORCE

The establishment of the UN ICT Task Force in November 2001, in response to a request by the UN ECOSOC, was a further important step. The task force was mandated to mobilize worldwide support for attaining the Millennium Development Goals with the use of ICT. In April 2004, a seminar on "Policy and security issues in information technology" was held at the UN Headquarters. Part of the seminar series was on policy awareness and training in information technology, organized by the ICT Task Force and the UN Institute for Training and Research (UNITAR) [7]. In 2005, the task force published a guide called "Information Insecurity—A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security" [8]. This publication depicts the problem of information insecurity in general, and provides possible solutions for prevention and response to security incidents (including standards and best practices). Moreover, it attempts to create a greater awareness about the growing dangers of cyber-hooliganism, cyber-crime, cyber-terrorism, and cyber-war, which are inherent aspects of the new opportunities (both positive and negative) that have been opened up by new information technologies [8].

## 5 THE WORLD SUMMIT ON THE INFORMATION SOCIETY (WSIS)

Recognizing that confidence and security in the use of information and communication technologies (ICT) are the main pillars of the information society, the first phase of the World Summit on the Information Society (WSIS) in December 2003 urged governments, in cooperation with the private sector, to consider legislation that allows for effective investigation and prosecution of misuse and strengthens institutional support at the international level. As a result, a number of recommendations were made in the WSIS Geneva 2003 first phase Declaration of Principles and Plan of Action [9] that relate to building confidence and security in the use of ICTs and promoting a global culture of cyber-security.

The outcomes of the second phase of the WSIS, held in Tunisia in November 2005, are summarized in the Tunis Agenda and Tunis Commitment. All governments, according to the Tunis Agenda [10], should have an equal role and responsibility in internet governance, but must also ensure the internet's stability, security, and continuity. The

document calls for enhanced cooperation to enable all governments to carry out these responsibilities, including the development of globally applicable principles on public policy issues associated with the coordination and management of critical internet resources.

The Tunis Agenda also recognizes the need for "national action and increased international cooperation to strengthen security while enhancing the protection of personal information, privacy and data." It underlines "the importance of the security, continuity and stability of the Internet, and the need to protect the Internet and other ICT networks from threats and vulnerabilities". It further emphasizes "the need for a common understanding of the issues of Internet security, and for further cooperation to facilitate outreach, the collection and dissemination of security-related information and exchange of good practice among all stakeholders on measures to combat security threats, at national and international levels" [11].

In a resolution passed on 28 July 2008, entitled Follow-up to the World Summit on the Information Society and Review of the Commission on Science and Technology for Development (CSTD) [12], ECOSOC indicated how it would oversee the system-wide follow-up of the summit outcomes, as requested by the Tunis outcomes. To this end, ECOSOC decided that CSTD would assist the council as the focal point in the system-wide follow-up of WSIS. It was agreed that this would entail a strong development orientation and that the Commission would be strengthened in its substantive capacity through the effective and meaningful participation of member states in its work. While preserving the inter-governmental nature of the commission, ECOSOC decided that CSTD should make use of the successful multi-stakeholder approach that was pioneered by WSIS. During the two sessions of 2007 and 2008, the deliberations of CSTD therefore were (and remain) open not only to NGOs in consultative states with ECOSOC, but also to other interested NGOs and civil society entities who were accredited to WSIS [13].

## 6 INTERNATIONAL TELECOMMUNICATION UNION (ITU)

At the WSIS, world leaders entrusted the International Telecommunication Union (ITU) [14] with the leading role in coordinating international efforts on cyber-security. As the sole facilitator for the action line related to Building Confidence and Security in the Use of ICT (WSIS Action Line C5) [15], the ITU launched the Global Cybersecurity Agenda (GCA) in May 2007 to provide a framework within which the international response to the growing challenges to cyber-security can be coordinated and addressed [16]. GCA benefits from the advice of a High-Level Experts Group (HLEG) [17] comprising more than one hundred (100) world-renowned specialists in cyber-security from governments, industry, international organizations, research organizations, and academia. The HLEG was established to advice the ITU secretary-general on concrete measures and strategies to address global challenges in the five work areas of the GCA:

- Legal Measures,
- Technical and Procedural Measures,
- Organizational Structures,
- Capacity-Building,
- International Cooperation.

In 2007 and 2008, the ITU carried out significant standardization work in security architecture, encryption and authentication, and information security management systems:[1]

- Three new recommendations on cyber-security were approved by ITU: Overview of cyber-security; vendor-neutral framework for automatic notification of security related information and dissemination of updates; and guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software.
- Three new recommendations on countering spam were approved by ITU: Technical strategies on countering spam; technologies involved in countering e-mail spam; and a technical framework for countering e-mail spam.
- Two new draft ITU recommendations have been submitted for the approval process: Countering IP multimedia application spam; and requirements for global identity management trust and interoperability.
- Twenty-eight more security recommendations were approved by ITU, as of June 2008, in areas including: directory services, authentication, security architecture, security management, tele-biometrics, peer-to-peer communication security, and secure mobile data communication.
- An ITU Study Group leads the identity management (IdM) work and has made four ongoing draft recommendations, which cover topics such as: data models, interoperable frameworks, interchange frameworks, and entity authentication assurance. In addition to the above-mentioned topics, new issues such as a trusted service provider identifier (T-SPID) were introduced into discussion.
- Significant progress has been made on the security aspects of IPTV. The first IPTV security recommendation is expected to be completed by September 2008.

In addition, the ITU has launched the ICT Security Standards Roadmap [18], an online database that provides information about existing ICT security standards and works in progress in key standards development organizations.

The ITU is also engaged in direct assistance to member states (particularly developing countries) building cyber-security capacities through a number of different activities. To this end, the ITU is developing a national cyber-security framework to coordinate national efforts, provide technical assistance, and organize capacity-building cyber-security forums. The ITU is also working with partners from the public and private sectors on specific cyber-security and Critical Information Infrastructure Protection development initiatives to assist developing countries in awareness and self-assessment, capacity-building, and expanding watch, warning, and incident response capabilities. Some relevant deliverables include the ITU National Cybersecurity/CIIP Self-Assessment Toolkit [19], which aims to assist governments in enhancing their cyber-security and address CIIP requirements; the Botnet Mitigation Toolkit [20]; as well as toolkits on the establishment of CERTs/CSIRTs, and promoting a culture of cyber-security. Other ITU initiatives to assist developing countries include the development of anti-spam legislative surveys, assessment activities of national cyber-crime legislations, and research on the financial aspects of network security, malware, and spam.[1]

[1]Information provided by an expert.

## ACKNOWLEDGMENT

We acknowledge the contribution of the experts of the International Telecommunication Union who validated the content of this chapter.

## REFERENCES

1. Dependability Development Support Initiative (DDSI) (2002). *International Organisations and Dependability-related Activities*, 31 May 2002, p. 66, http://www.ddsi.org/htdocs/DDSI-F/main-fs.htm.
2. UN General Assembly (2002). Resolution 55/63 and 56/121 (23 January 2002). *Combating the Criminal Misuse of Information Technologies*, http://www.un.org/documents/.
3. UN General Assembly Resolution (2003). 57/239 (31 January 2003). *Creation of a Global Culture of Cybersecurity*, http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_57_239.pdf.
4. UN General Assembly (2004). Resolution 58/199 (30 January 2004). *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, http://www.itu.int/osg/spu/cybersecurity/docs/UN_resolution_58_199.pdf.
5. Resolutions 59/61 of 3 December 2004, 60/45 of 8 December 2005; 61/54 of 6 December 2006; 62/17 of 8 January 2008. (2008). http://www.un.org/documents.
6. Resolution 59/220 of 11 February 2005, and Resolution 60/252 of 27 April 2006. (2006). http://www.un.org/documents.
7. http://www.unicttaskforce.org/perl/documents.pl?id=1352, 2008.
8. Eduardo, G., and Ahmad, K. (2002). *Information Insecurity—A Survival Guide to the Uncharted Territories of Cyber-Threats and Cyber-Security*, New York, https://unp.un.org/details.aspx?entry=E04291#.
9. World Summit on the Information Society (WSIS) *"Geneva Declaration of Principles", "Geneva Plan of Action", "Tunis Commitment", and "Tunis Agenda for the Information Society"*, http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160|2266|2267, 2008.
10. World Summit on the Information Society (WSIS) *Tunis Agenda for the Information Society*, http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0, 2008.
11. World Summit on the Information Society (WSIS) *Tunis Agenda for the Information Society*, paragraphs 39 and 45, http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0, 2008.
12. Resolution 2006/46 (28 July 2006). *Follow-up to the World Summit on the Information Society and review of the Commission on Science and Technology for Development*, http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2368|0.
13. http://www.itu.int/wsis/follow-up/index.html, 2008.
14. http://www.itu.int/net/home/index.aspx, 2008.
15. World Summit on the Information Society *Geneva Plan for Action*, http://www.itu.int/wsis/docs/geneva/official/poa.html, 2008.
16. http://www.itu.int/osg/csd/cybersecurity/gca/overview/index.html, 2008.
17. http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html, 2008.
18. http://www.itu.int/ITU-T/studygroups/com17/ict/index.html, 2008.
19. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html, 2008.
20. http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.htmlt, 2008.

# THE WORLD BANK GROUP

MANUEL SUTER AND ELGIN BRUNNER
*Center for Security Studies (CSS), ETH Zurich, Switzerland*

## 1 INTRODUCTION

The growing incidence of computer and cyber-crime has a particularly strong bearing on the financial sector. In view of the growing amount of financial data stored and transmitted online, the ease of computer intrusions has added to the severity of the problem. Therefore, the World Bank Group has taken several steps over the last few years to face the challenges of information security, especially in developing countries [1].

## 2 THE GLOBAL INFORMATION AND COMMUNICATION TECHNOLOGIES DEPARTMENT (GICT)

The Global Information and Communication Technologies Department (GICT) [2] promotes access to information and communication technologies in developing countries. It serves as the World Bank Group's core department for research, policy, investment, and programs related to ICT in developing countries. The GICT's aim is to expand access to a range of information infrastructure networks and support the development and application of information technologies to reduce poverty and improve people's lives. Linked to this mission are three goals aimed at [3]:

- Accelerating the participation of developing countries in the global information economy;
- Spreading the benefits of these technologies through increased competition and private investment in information infrastructure;
- Fostering sustainable economic and social development through innovative technologies, with a special emphasis on the need of the poor in developing countries.

Moreover, the World Bank Group's ICT sector strategy is based on four pillars [3]: The broadening and deepening of sector and institutional reform, the improvement of

Reprinted with permission from Elgin M. Brunner and Manuel Suter. **International CIIP Handbook 2008/2009, Series Editors**: Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, Center for Security Studies, ETH Zurich.

access to information infrastructure, the support of human capacity to exploit ICT, and the support of ICT applications across a broad range of sectors.

The GICT group consists of six teams including [4] the office of the director, the strategy and business development team, the telecom and media division, the portfolio and technology division, the public sector policy and operations division, and the Information for Development (infoDev) Program [5].

## 3 INFORMATION TECHNOLOGY SECURITY HANDBOOK

The Information Technology Security Handbook [6], funded by the infoDev Program, provides technology-independent best practices and recommendations in the field of IT security. The handbook was published in 2003 and, as the technology evolves, the accompanying website [7] provides updates as appropriate. The book addresses private users of IT, small and medium-sized organizations, government, and technical administrators, especially in developing countries. The handbook is based on the premise that use of ICT is on the rise, while the knowledge of IT security practices is lagging behind.

After a general introduction to IT security, the Information Technology Security Handbook deals with topics such as [8]:

- *Security for individuals.* keeping personal computers, data and operating systems, and applications secure; malicious software; securing services over networks; tools to enhance security; and the role of encoding and encryption;
- *Security for organizations.* risk evaluation and mitigation; planning; organizational security policy and personnel security; security outsourcing; mobile risk management; and best practices;
- *Information security and government policies.* various arrangements for protecting government systems; laws and legislation; and government policy in promoting better security in the private sector;
- *IT security for technical administrators.* physical security; information security; identification and authentication; server security; network security; attack and defenses; and detecting and managing break-ins.

## 4 THE WORLD BANK'S E-SECURITY/E-FINANCE EFFORTS

The World Bank published a report on Electronic Security: Risk Mitigation in the Financial Transactions in June 2002, building on previous papers that identified e-security as a key component to the delivery of e-finance benefits. This paper and its technical annexes identify and discuss eight key pillars for a secure electronic environment [9].

In January and May 2004, a follow-up publication was published, entitled Technology Risk Checklist [10]. This World Bank publication describes 13 layers of e-security, covering both hardware and software pertaining to network infrastructures. These layers cover risk management, policy management, cyber-intelligence, access controls and authentication, firewalls, active content filtering, intrusion detection systems (IDS), virus scanners, encryption, vulnerability testing, systems administration, incident response plans (IRP), and wireless security [11]. In 2005, two further documents were published by the World

Bank's e-security/e-finance section on the dangers emanating from BOTs–Cyber Parasites [12] and on the issue of Money Laundering in Cyberspace [13].

## REFERENCES


1. http://info.worldbank.org/ict/index.cfm, 2008.
2. http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:20687829~menuPK:1785618~pagePK:210058~piPK:210062~theSitePK:282823,00.html, 2008.
3. http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:20687836~menuPK:282840~pagePK:210058~piPK:210062~theSitePK:282823,00.html, 2008.
4. http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:20718594~menuPK:1786142~pagePK:210058~piPK:210062~theSitePK:282823,00.html, 2008.
5. http://www.infodev.org/en/index.html, 2008.
6. The International Bank for Reconstruction and Development/The World Bank (infoDev) (2003). *Information Technology Security Handbook*, Washington, DC. http://www.infodev-security.net/handbook.
7. http://www.infodev-security.net, 2008.
8. *Information Technology Security Handbook*, op. cit, 2008.
9. The World Bank (2002). *Electronic Security: Risk Mitigation in the Financial Transactions*, Public Policy Issues (June). http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-security-RiskMitigationInFinancialTransactionsv4/$FILE/E-security-Risk-+Mitigation+In+Financial+Transactions+v+4.0.pdf.
10. The World Bank (2004). *Technology Risk Checklist*, (May, Version 7.3). http://www.infragard.net/library/pdfs/technologyrisklist.pdf.
11. The World Bank (2004). *Technology Risk Checklist*, (May, Version 7.3). http://www.infragard.net/library/pdfs/technologyrisklist.pdf, p. 2ff.
12. http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/Bots/$FILE/Bots.pdf, 2008.
13. http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/MoneyLaunderinginCyberspace/$FILE/MoneyLaunderinginCyberspace.pdf, 2008.

# CYBER SECURITY

# CLASSES OF VULNERABILITIES AND ATTACKS

PASCAL MEUNIER
*Purdue University CERIAS, West Lafayette, Indiana*

## 1 INTRODUCTION

The analysis of the nature of flaws, vulnerabilities, weaknesses, and the attacks they enable has fascinated computer scientists. A better understanding of vulnerabilities and attacks can be achieved by grouping them based on common properties and similarities. Many groups and "types" are commonly discussed in computer security texts and secure programming materials. These popular classifications usually capture a defect or a weak technology that enables attacks or present an appealing, succinct, and useful point of view for discussing vulnerabilities. It is common to refer to the set of vulnerabilities that enable attack scenario X as "X vulnerabilities", for example, "cross-site scripting (XSS) vulnerabilities". Sometimes the name of a technology is used instead of the name of an attack, for example, "format string vulnerabilities". However, the popular vulnerability types suffer from many defects, such as ambiguities and overlapping classifications. A single vulnerability may belong to several popular types simultaneously or at different times, when the analysis is performed from a different point of view or from a different level of abstraction. A systematic grouping can achieve the status of a scientific classification if it meets rigorous criteria, such as reproducibility, objectivity, and lack of ambiguity. First, popular classifications are reviewed and their usefulness discussed. Then, scientific taxonomies and other systematic efforts are discussed. Finally, the advantages of using ontologies instead are presented.

As a side effect of these classifications, there have been various attempts at defining vulnerabilities and flaws. A software vulnerability has been defined as "an instance of an error in the specification, development, or configuration of software such that its execution can violate the security policy" [1]. This definition of vulnerability is close to the definition of a flaw in [2]. For the purposes of this article, a flaw defines or implies what should have been done to prevent policy violations; it is a problem at a higher level of abstraction that may potentially enable several different attacks and create various vulnerabilities. For example, a flaw such as missing input validation may result

in memory management problems such as a buffer overflow vulnerability, an integer overflow vulnerability resulting in a call "malloc(0)", or improper memory access through the indexing of inexistent elements in an array. The same flaw could also cause violations of invariants in the design, such as negative payments or corrupted prices. Because there may be several different ways in which to avoid a vulnerability, flaws can be a vague concept. There have been many attempts to classify vulnerabilities by the flaws that enabled them, so both classes of vulnerabilities and classes of flaws are discussed in the same section.

## 2 POPULAR VULNERABILITY CLASSIFICATIONS

Popular vulnerability classifications fail to meet scientific criteria; yet they can be useful and powerful descriptions of what went wrong. For example, in the book "19 deadly sins", Howard et al. use a mix of several different popular classifications [3]. As a result, the theme of each section is easy to understand and can be effectively and succinctly described. However, it is possible to find examples or contrive vulnerabilities that could fit in more than one section at once, and others that would fit in none.[1] It has also been argued that taxonomies should be judged on whether they are useful, instead of whether they are scientifically correct [2]. In this article, classifications aiming first for usefulness are called *popular classifications* to distinguish them from attempts to meet the rigorous scientific criteria for taxonomies established across disciplines. Popular classifications may have different goals from scientific taxonomies, such as educational, conceptual, and tool use.

### 2.1 Classification by Exploitability

Exploitability can be difficult to establish, therefore including a criterion that is difficult to observe or deduce correctly is not a good idea. Yet the concept is useful and exploitability is often debated, so this section presents the classification of vulnerabilities depending on whether they are latent, potential, or exploitable. A latent vulnerability consists of vulnerable code that is present in a software unit and would usually result in an exploitable vulnerability if the unit was reused in another software artifact. However, it is not currently exploitable due to the circumstances of the unit's use in the software artifact; that is, it is a vulnerability for which there are no known exploit paths. A latent vulnerability can be exposed by adding features or during the maintenance in other units of code, or at any time by the discovery of an exploit path. Coders sometimes attempt to block exploit paths instead of fixing the core vulnerability, and in this manner only downgrade the vulnerability to latent status. This is why the same vulnerability may be found several times in a product or still be present after a patch that supposedly fixed it.

A potential vulnerability is caused by a bad programming practice recognized to lead to the creation of vulnerabilities; however, the specifics of its use do not constitute a vulnerability. A potential vulnerability can become exploitable only if changes are made to the unit containing it. It is not affected by the changes made in other units of code.

[1]This is not a criticism of the book, which meets its goal of providing "a simple list of those security issues that are most important" [3]. It was not intended to provide complete, scientific coverage.

For example, a vulnerability could be contained in the private method of an object. It is not exploitable because all the object's public methods call it safely. As long as the object's code is not changed, this vulnerability will remain a potential vulnerability only.

Vendors often claim that vulnerabilities discovered by researchers are not exploitable in normal use. However, they are often proved wrong by proof-of-concept exploits and automated attack scripts. Exploits can be difficult and expensive to create, even if they are only proof-of-concept exploits. Claiming unexploitability can sometimes be a way for vendors to minimize bad press coverage, delay fixing vulnerabilities, and at the same time discredit and discourage vulnerability reports.

### 2.2 Classification by Software Development Life Cycle (SDLC) Phase

Taxonomies of this kind attempt to categorize vulnerabilities according to when they were introduced in the software life cycle. Classically, six phases are recognized: feasibility study, requirements definition, design, implementation, integration and testing, and operations and maintenance. At a basic level, this classification groups the above phases into three groups: design (first 3 phases), implementation (phases 4 and 5), and operation and maintenance. It was suggested that the timing of reviews could be decided based on the phase in which a vulnerability type could be introduced [4].

The design and implementation distinction is particularly appealing to computer scientists who want to argue the correctness of an algorithm, protocol, or model in theory separately from an implementation that may be subject to unfavorable limitations or mistakes resulting in vulnerabilities. For example, a vulnerability may be due to a bad algorithm being chosen during design phases. Another may be due to a bad implementation of a correctly chosen algorithm, and therefore the vulnerability was introduced at some point during the implementation phases of the program.

It was also suggested to classify vulnerabilities into design, implementation, and configuration vulnerabilities [5]. However, "configuration" vulnerabilities are a narrower category than all the vulnerabilities introduced during operation and maintenance. This difference could be resolved if maintenance is considered as reoccurring design and implementation phases, and if emergent vulnerabilities are considered to be design vulnerabilities at the level of the system.

Even though operation and maintenance are often seen as a single phase from a timeline point of view, they differ in how they can introduce vulnerabilities. Vulnerabilities introduced during operation are usually configuration issues, although some also emerge due to interactions with an unexpected or changed environment, including other installed software and operating system (OS) version, kernel modules and libraries, or unexpected or virtual hardware. Vulnerabilities can be introduced during maintenance to fix bugs or modify functionality. The difference is that maintenance changes the code, whereas operation does not. So, five classes have been proposed: analysis, design, implementation, deployment, and maintenance [6].

The difficulty with the above classifications is that there are usually many levels of abstraction at which to view complex systems, in addition to the choice of the number of phases. What is a design problem may be viewed as an implementation problem or an operation problem at another level, and *vice versa*. This can make some comparisons across projects difficult. Therefore, this classification is subject to an abstraction level that needs to be specified. For the sake of auditing vulnerabilities, reasonable and

useful but fuzzy definitions are provided in [4]. The time of introduction of a vulnerability in the software development life cycle (SDLC) has been used as a taxonomic characteristic [6–8], but was later shown to fail scientific requirements [1, 9]. Some flaws can be introduced at multiple points in the SDLC, so although linking a vulnerability to a specific SDLC phase can be an interesting consideration, it is not always applicable.

This kind of classification may also be useful when reviewing software development processes in a software development firm. The details of the classification are then dependent on the specific software engineering model adopted. Therefore, there can be as many taxonomies of this kind as there are software engineering development models. This makes the comparison and discussion of vulnerabilities across development models difficult.

### 2.3 Classification by Genesis

The premise of this classification is that the reasons and ways flaws are introduced into a system can provide insight into their prevention or detection. This classification differentiates first between intentional and inadvertent flaws. Intentional flaws are further divided into malicious and nonmalicious ones [2, 7]. However, whether the programmer maliciously introduced the vulnerability or not and in general the programmer's intent are in practice impossible to determine after the fact, and therefore the classification is not objective and not specific [1]. Truly, the programmer's intent is irrelevant (and unknowable) to a security researcher analyzing the consequences of released vulnerable code, but that is not the purpose of this classification. The genesis classification helps understand how some flaws could be prevented or caught during development. For example, tools attempting to catch inadvertent flaws were successful [2]. This classification is, therefore, more an aid for strategic thinking and design than something directly applicable to collections of flaws.

### 2.4 Classification by Location in Object Models

These classifications attempt to categorize vulnerabilities according to which model object or "entity" they belong to. Examples are classifying vulnerabilities using the ISO open systems interconnect (OSI) reference model for networking [10]. This model defines seven distinct layers, so a vulnerability could in theory be classified according to which layer it belongs to. In reality, some vulnerabilities depend on the specific interactions between two or more layers or objects, so this kind of taxonomy is not always applicable.

Similarly, attempts to differentiate whether a vulnerability was due to an OS or an application were unsuccessful (CVE-1999-0144). This was because a configuration option of the OS could prevent it from happening, whereas others argued that well-behaved programs should not need that kind of OS configuration. This difficulty can be encountered whenever the vulnerability relates to ill-defined responsibilities. The classification may then change depending on the perception of the responsibilities and is therefore subjective. For example, currently the security of web browser plug-ins and scripting engines is considered their own problem. However, as web browsers mature, the better browsers should limit the security risks posed by vulnerable plug-ins and malicious scripts, in a manner similar to OSs limiting what processes can do.

### 2.5 Classification by Affected Technology

Format string vulnerabilities in the "C" programming language are an example of a vulnerability type identified by the underlying technology. The implementation of polyvariadic functions in "C" is such that called functions have no way of knowing how many arguments were passed. Attacker-controlled format strings can exploit both that limitation and format string functionality, for example, to write data at arbitrary locations in memory by using the "%n" format specifier. Depending on the format string supplied, the result of the attack can be (i) a crash by trying to access inexistent memory or memory allocated to another process (denial of service); (ii) the formatted strings contain unexpected data, possibly exposing confidential data, or adding incorrect or malicious information; or (iii) the process comes under the control of the attacker (compromise).

Metacharacter vulnerabilities happen in technologies where some characters have a special significance, for example, syntactic. Metacharacters are often used to separate data and commands in dynamic query languages. "SQL injection" and "LDAP injection" are examples of subcategories of metacharacter vulnerabilities. Character encoding issues are other examples of a subcategory, inasmuch as special metacharacters indicate special encodings (e.g. URL "percent" encoding).

Resource exhaustion vulnerabilities happen when limited computer resources can be abused maliciously in a way that limits the functionality of the system, possibly resulting in a denial of service. Examples are SYN-flood attacks[2] resulting from the transmission control protocol (TCP) protocol requiring memory for every connection request; memory leaks (specific to languages without garbage collection); and algorithmic complexity issues where an attacker is able to trigger worst-case behaviors in vulnerable algorithms.

Although the name of the affected technology is a useful and descriptive reference, there are many vulnerabilities that do not relate directly to a specific technology. For those that do, the usefulness of the classification is limited in cases where the flaw enabling the vulnerability has a weak or no relationship to the technology; the identification may not always help understand the properties and causes of the vulnerability. Therefore, this classification scheme is not universally useful.

### 2.6 Classification by Errors or Mistakes

Errors known to have led to vulnerabilities have been categorized by their cause, the nature of their impact, and the type of change or fix made to remove the error [11]. A similar type of classification is used often in "19 Deadly Sins", with categories such as "use of weak password-based systems" and "failing to store and protect data securely" [3]. Another example is the "double-free" memory management mistake.

This has educational value, especially when the mistake can be abstracted and applied to new situations. Unfortunately, there are situations in which any of several changes in different code locations, modules, or even different programs altogether can fix a vulnerability or at least block the known exploitation paths. Therefore, as a classification, it can be ambiguous.

### 2.7 Classification by Enabled Attack Scenario

Sometimes the set of vulnerabilities that enable a specific kind of attack is highly descriptive and fairly precise. For example, "XSS" is an attack scenario and "XSS

[2]SYN-flood attacks are remote denial-of-service attacks; see CERT advisory CA-1996-21.

vulnerabilities" are vulnerabilities enabling the injection of scripting code into content served to web browsers. They enable other attacks, but "XSS vulnerabilities" capture a unique common property and is a useful and succinct reference. It should be noted that many XSS vulnerabilities, but not all, are the result of metacharacter handling vulnerabilities.

On the other hand, referring to "denial-of-service vulnerabilities" is not useful because denial of service is the consequence of an attack, and not an attack scenario, and can be achieved in many disparate ways, for example, buffer overflows and format string vulnerabilities.

A classification of vulnerabilities in network protocols proposed by Pothamsetty and Akyol [12] is interesting because it offers simultaneously a "test" or attack taxonomy and countermeasures. Even though the mistakes ("vulnerability classes") are presented first, it is evident that they are defined based on the attacks they enable. This kind of enumeration is likely to be proved incomplete as a new kind of attack may be uncovered in the future. However, it may still be useful in practice. The categories are

1. clear text communication
2. nonrobust protocol message parsing
3. insecure protocol state handling
4. inability to handle abnormal packet rates
5. vulnerability arising from replay (RP) and reuse (RU)
6. protocol field authentication
7. entropy problems.

The "test" or attack techniques are[3]

1. packet sniffing (PS)
2. protocol field fuzzing (PFF)
3. protocol field spoofing (PFS)
4. packet flooding (PF)
5. Replay
6. Reuse
7. packet size variation (PSV)
8. packet number variation (PNV)
9. out-of-sequence packets and out-of-range values
10. special and reserved packets (SRPs)
11. information retrieval[4]
12. communication initiation (CI)
13. communication termination (CT)
14. encryption and random number check (EC).

[3]The attack techniques have been reordered to roughly match the order of the vulnerability types.
[4]This refers to checking the protocol for exposures, not vulnerabilities.

### 2.8 CLASP Classification

CLASP (comprehensive, lightweight application security process) is a set of activities aiming to improve security [13]. It uses a classification focused on enumerating errors, but simultaneously includes conditions resulting from mistakes, as well as events. It has the following categories at the top level:

- *Range and type errors.* This includes the "write-what-where condition" as well as buffer overflows and "format string problems".
- *Environmental problems.* This includes events such as the failure of a random number generator.
- *Synchronization and timing errors.* For some reason this includes statistical attacks. It also includes "capture-replay", the vulnerability to which is usually a protocol flaw.
- *Protocol errors.* This includes using a broken or risky cryptographic algorithm.
- *General logic errors.* This is a catchall that includes things as diverse as using a "noncryptographic" random number generator or too few parameters being passed to a function (e.g. format string issues in "C").

Although the list of things that can go wrong is interesting, this classification has several flaws from a scientific perspective. A vulnerability may simultaneously be classified in several categories at once, for example, if several mistakes are linked to the vulnerability simultaneously, if a mistake results in a condition, or if an event triggers a condition. This classification is inconsistent when used at different abstraction levels. For example, when considered at a low level, a problem may be due to an integer overflow problem. At a higher abstraction level, it may become the failure of a random number generator. Also, similar issues, for example, cryptographic issues, are not grouped together. This may not matter in practice, as the goal of this classification is to discuss which kinds of vulnerabilities may be found during various activities.

### 2.9 Seven Kingdoms

This classification of software security errors has the following eight top levels [14]:

1. input validation and representation
2. API abuse
3. security features
4. time and state
5. error handling
6. code quality
7. encapsulation
8. environment (this category is mostly composed of configuration issues, that is, issues that do not belong in the first seven).

This classification simultaneously includes causes, consequences, and bad practices. Therefore, a vulnerability can belong to several categories simultaneously or be classified differently depending on the abstraction level used. The API abuse category, while

an appealing concept, is especially ambiguous and conflicting with other categories. It harbors issues that could arguably be classified as input validation problems, such as a buffer overflow vulnerability caused by not performing input validation on potentially malicious names returned by a reverse domain name service (DNS) call [14]. Its main strength is that it makes sense when discussing the detection rules used by code scanning software. It can also help educating and conveying to programmers secure programming concepts, such as being aware of the rules involved ("contract") when calling a given API.

### 2.10 Classification by Disclosure Process

Vulnerabilities for which there are written exploits, before they become publicly known, are zero-day (also known as *0-day*) vulnerabilities. Some variations in usage refer to vendor knowledge instead of public knowledge. Before public disclosure, zero-day vulnerabilities may be sellable on black markets or some security companies (e.g. iDefense's "vulnerability challenges"). "Private" 0-days refer to vulnerabilities and exploits shared by small groups. So, 0-day vulnerabilities can be secret, private, or disclosed.

Following the disclosure of a 0-day vulnerability, owners of the vulnerable systems may be able to take actions to mitigate the issue or to detect compromises. Simultaneously, more attackers are informed of new ways to attack systems. Vendors may have to scramble to produce patches that will protect their clients; if the vendor already knew about the vulnerability, they may take less time to produce the patch.

Knowing whether a vulnerability is a 0-day or not has ethical implications, for a security researcher, which will influence the disclosure process. In responsible disclosure, vendors are notified first and given some time to fix the vulnerabilities before they are made public [15]. If a vulnerability is being exploited, that is, it is a 0-day, then there is an ethical justification for giving less or no advance notification at all to the vendor.

### 2.11 Configuration Issues, Exposures, System Vulnerabilities, "Proper" Vulnerabilities

For the purposes of this article, a system is a combination of interacting software and hardware, which may be located on one or several machines, and that performs a set of tasks as a whole. The definition of vulnerabilities with reference to a security policy [1] is especially appropriate for system vulnerabilities. System vulnerabilities may exist even if a system is composed of software artifacts all with correct designs and all perfectly implementing their design. This may be due to misconfigurations (e.g. the presence or execution of software contrarily to policy), designs that are inappropriate for the system, or emergent properties due to the combination and interactions of software artifacts designed separately. Flaws in various subsystems can combine to produce a vulnerability. This is the realm of compositional security. In particular, systems can be vulnerable to emergent abusive behavior attacks, in which legitimate acts can be combined to violate a policy [16].

The analysis of system vulnerabilities cannot proceed simply from the analysis of the code or design of a subsystem in isolation, but should reference the violated security policy and be accompanied by a description of the relevant interactions with other software artifacts. Different security policies that are appropriate given different environments in different organizations may result in two different lists of vulnerabilities for copies of

the very same system. The security policy is defined externally to the system, and is not an intrinsic property; therefore, system vulnerabilities are not intrinsic properties of systems.

Sometimes, the reasonable expectation that there is a relevant policy deployed somewhere is sufficient for the discussion of a system vulnerability, but the generic terms of that policy should be defined explicitly for the discussion. The MITRE common configuration enumeration (CCE) effort aims to identify configuration issues by finding examples of a relevant "reasonable" policies, such as hardening configuration guides for OSs [17].

"Proper" vulnerabilities are apparent when a specific software artifact is compared to its requirements and design (explicit or implied) at the time of its creation. It can be argued that the design and design goals of a software artifact are intrinsic properties of the artifact, because they remain the same regardless of where, how, when, or by whom the software is used. The examination of software artifact vulnerabilities can therefore be performed with less information than needed with system vulnerabilities, while being more objective and reproducible, because it is grounded in technical facts proper to the artifact. However, this can become subjective if some aspects of the design are guessed by the researcher. The MITRE common vulnerabilities and exposures (CVE) effort gives unique identifiers to software artifact vulnerabilities [18].

Understanding the difference between system vulnerabilities and software artifact vulnerabilities is useful when practitioners and academics attempt to communicate. A practitioner may argue that a system is not vulnerable due to a configuration that blocks attacks, while the academic will point out that a vulnerability remains (and could get exposed again). Likewise, a practitioner may consider a system to be vulnerable due to a service running and exposing excess information when it should not, in violation of a policy. In this situation, the academic may lose interest because the violated policy is "arbitrary", that is, orthogonal to the design of all of the software artifacts.

Exposures are information leaks that may aid an attacker, but do not directly violate the design goals of a software artifact. This distinction was at the origin of the name change of the CVE from "common vulnerabilities enumeration" to "common vulnerabilities and exposures" in order to be inclusive of unexpected exposures. As the CVE effort matured and the CCE effort was introduced, the CVE focused on exposures that were not part of the design of a software artifact. Exposures that can be easily prevented without disabling a useful feature are handled by the CCE.

Some vulnerabilities can be examined as both system and software artifact vulnerabilities; consider CVE-1999-0997. This vulnerability arose due to the interactions between the FTP server software "wu-ftpd" with the ftp conversion option enabled and compression programs such as tar. This can be discussed from the point of view of a system vulnerability, because it appears through the combination and interactions of various software artifacts. It can also be considered a software artifact vulnerability because wu-ftp was designed to work with compression programs through the conversion option. A difficulty in creating such programs is that a design can be suddenly invalidated by the introduction of a new feature in an interacting product or by the introduction of a new product that supports unexpected features.

## 3 POPULAR ATTACK CLASSIFICATIONS

Popular attack classifications often use a mix of ambiguous classifiers such as the origin, goal, mechanism, and motivation of an attack, and suffer from a perspective ambiguity.

The purpose of an attack may be clear to the attacker, but can appear as something else to the defender. The DARPA 1999 IDS evaluation program used these five types [19]:

1. *Probe (or surveillance).* This category applies to activity meant to gather information.
2. *Denial of service.* This is really the consequence of an attack.
3. *R2L (remote to local).* Unauthorized access from a remote machine.
4. *U2R (user to root).* Unauthorized transition to root for an unprivileged user.
5. *Data.* This is meant to represent attacks whose goal is to obtain and extract ("exfiltrate") confidential files from a system.

Failed or misunderstood attacks could be put in the probe category by a defender. An attack that may have been meant to be a probe by an attacker may result in a denial of service, accidentally or not. Denial of service can also be the consequence of a failed R2L or U2R attack. Data attacks can also be R2L or U2R attacks, so an attack can be simultaneously classified into two categories [19]. These categories are not complete, as they do not include U2U (user to user) attacks or take into account new attacks, for example, attacks aimed at other users of the system by planting malicious links or scripts (e.g. XSS attacks) or misinformation. Nevertheless, this classification was useful and appropriate for the IDS evaluation, given attacks with known goals.

### 3.1 Web Application Security Consortium Threat Classification

The web application security consortium (WASC)'s threat classification has the following top classes:

1. *Authentication.* This identifies the authentication mechanisms attacked (targets).
2. *Authorization.* This identifies the authorization mechanisms attacked (targets).
3. *Client-side attacks.* This really is a technology type classifier, in this case used to identify a target.
4. *Command execution.* This is a goal.
5. *Information disclosure.* This is a consequence.
6. *Logical attacks.* This contains as a subclass denial-of-service attacks, which is a consequence. Other subclasses describe mistakes or attacks against access control mechanisms (which were covered in class 2).

In conclusion, this classification uses inconsistent types of classification criteria at the same level, which leads to ambiguities, as an attack can be classified in several categories at once.

### 3.2 Classification by Transactional Attack Scenario

A transactional attack scenario describes how the attack operates on the basis of transactions between the participants. Examples are RP attacks, man-in-the-middle, and the strictly defined XSS attacks that involve a third-party host. Eavesdropping is another

transactional attack scenario that simply requires listening and passively gathering information. It can be carried out by listening to incidentally leaked signals (lights of light emitting diodes (LEDs), sounds of typing on keyboards, monitor radiation) or to network or wireless (including Bluetooth) transmissions (also known as "sniffing"). These attack classifications are most useful when studying the security of communication protocols.

### 3.3 Impact

The impact of the attack on the confidentiality, integrity, and availability of targets has been used by the common vulnerability scoring system (CVSS) with levels of "none", "partial", and "complete". These coarse levels indicate the impact of the worst attack enabled by a vulnerability [20]. As the worst attack scenario may not be known yet (perhaps it is enabled only in some circumstances), this classification may be subject to change as more information is found, contrary to the goal of the CVSS to use this as an invariant in the scoring system.

### 3.4 Attack Language

Attack instances can be described as a series of steps to achieve an unauthorized result [5]. This includes the tool used, the vulnerability targeted, events comprised actions and targets, and finally an (at least attempted) unauthorized result. Tool categories are as follows:

- Physical attack.
- Information exchange. This includes social engineering attacks (see below).
- User command.
- Script or program. This includes trojan horses (see below).
- Autonomous agent. This includes viruses and worms (see below).
- Toolkit. This includes rootkits (see below).
- Distributed tool.
- Data tap. This is the monitoring of energy leakage through an external device. This includes light (videos, pictures, blinking LEDs), variations in power consumption, sounds of keys being pressed, radio waves, and so on, which may reveal information.

The events and characteristics of an attack instance provide information useful for identification and comparison. However, the language itself does not define a classification. Although the language is flexible and avoids committing to a specific classification scheme, analyzing and storing detailed information about every instance is expensive and unwieldy.

### 3.5 Classification of Attacks on Human Interactions

Human interactions can be exploited as part of an attack or preattack recon. Human beings may not be the final target of the attack, but are being used by deceptive means. "Social

engineering" is a powerful descriptor of an attack that involves tricking human beings. Subclasses of social engineering attacks include "phishing", which involve exploiting ambiguities in user interfaces (usually in emails pointing to fake websites). "Pretexting" is a form of fraud used to collect password, host, or account information from naïve employees or to instruct them to perform actions that will give the attacker access or weaken systems. Social engineering attacks can also be physical ("in person") by the use of disguises and body language. Some of these attacks are assisted by malicious code (see trojans) in "free" software or "lost" media.

### 3.6 Classification of Malicious Code

The classification of the malicious code used in an attack can be useful to understand the attack. However, for the sake of objectivity, code should be classified from its behavior alone, without needing to know that it was created with malicious intent (maliciousness may be inferred later, however). Indeed, benevolent viruses have been discussed before [21]. An attempt to create a benevolent worm, the Welchia worm, backfired [22], so intent can be largely irrelevant. The classification of viruses as a subclass of Trojan Horse is objectionable [6], since a virus may replicate without needing to deceive users by appearing as another code entity (e.g. boot sector viruses or macroviruses in formats supporting macroscripting). It makes more sense to consider the need to deceive users separately from self-replicating aspects. According to the criteria proposed in [23], it is more useful and desirable to consider "primitive" classifiers that can each be answered by yes or no. Possible definitions of various aspects of malicious code include the ones listed below.

1. *Attack code.* Attack code aims at exploiting vulnerabilities, and is commonly found in the form of attack scripts or proof-of-concept exploits. Worms are another example of attack code. Malicious code is not necessarily an attack code, but its mere presence may imply that the system was compromised by a prior attack. Malicious code resident on a victim computer and performing an undesirable function, such as spyware, rootkits, or backdoors, is to be differentiated from attack code that exploits vulnerabilities.
2. *Parasitic code.* Parasitic code is a code that is attached or included in another document or executable and violates its integrity. Intended or original properties of the document or executable must be identifiable in order to determine the presence, nature, and extent of the parasite. Parasitic code is not necessarily an attack code.
3. *Backdoors (also known as "Trapdoor".* [7]*).* A backdoor is code bypassing policy-approved user authentication mechanisms. Backdoors are usually hidden, hard to discover, and inserted and used for malicious purposes. For example, a remote user may issue commands as root through a previously installed backdoor. Some backdoors are created by programmers for reasons of convenience (e.g. remote maintenance), and so the original intent may not be malicious. However, backdoors that violate security policies must be considered malicious based on their behavior alone as discussed above. Remote access mechanisms operating within policy are not to be confused with backdoors.
4. *Trojans.* Code that gets executed by deceiving a user is a trojan (the deception aspect implies maliciousness, even if it is a mild prank). Trojans can carry and be

the initial entry mechanism for malicious code of another nature (e.g. a backdoor or keylogger).

5. *Self-propagating code.* Self-propagation can occur in two modes:
   (a) Viruses are parasitic and are spread by means of finding new host files (documents or executables) that will presumably also get read and run later. Macro viruses refer to viruses carried by documents which can carry "macros", essentially a scripting capability which blurs the boundary between data and code.
   (b) Worms spread on their own, by duplicating their code to other systems and respawning their processes.
6. *Spyware.* Spyware is a code that reports user activities and system information to "unauthorized" parties (who is "unauthorized" may depend on perspective). An example is an "unauthorized" keylogger. Spyware could also take "interesting" forms such as being a virus and reporting when a certain type of document is opened.
7. *Logic-/time-triggered code.* This is an extraneous code that is not part of the expected function of a software artifact and remains dormant until very specific activation conditions are met. If it can then perform attacks, it is a "bomb" [7]. If not, and it simply exposes humorous (at least to some) content, it is considered an "Easter egg". Some digital rights management ("DRM") codes that violate a security policy, for example, while trying to aggressively enforce a licensing agreement, could be considered triggered code.
8. *Rootkit.* A rootkit is a set of software artifacts that attempts to conceal its existence and execution (and possibly that of other malicious software as well) from the rest of the OS, other processes, or security tools, and consequently from users and administrators. Typically, a rootkit subverts or replaces the utilities included with an OS for the purposes of hiding a compromise and a backdoor. A rootkit may include attack code as one of its components and may resist removal.
9. *Distributed code.* Distributed code has coordinated copies of itself on many hosts. By acting in a coordinated fashion, the distributed code attempts goals that would likely be unreachable for a single copy. The coordination mechanism may be the reception of commands or interactions between copies or with a controller. Blindly following specially crafted rules of conduct may also result in the overall desired behavior. Worms have been known to include a time bomb for attacking a predetermined target at a given time, resulting in a distributed attack.

## 4 SCIENTIFIC CLASSIFICATIONS

Scientifically correct taxonomies of vulnerabilities and attacks are difficult to create due to the requirements that they separate elements of a group into subgroups (taxa) that are mutually exclusive. The crucial problem in designing a taxonomy is to identify and organize appropriate taxonomic characters, also known as features, attributes, or characteristics. The taxonomic characteristics must have the following properties [1]:

1. *Objectivity.* Values must be based on an observable property of the object.

2. *Determinism.* There must be a clear and explicit procedure to follow so that there is no possibility of misclassification.
3. *Repeatability.* Values must be selected reproducibly by different people.
4. *Specificity.* The selected value must be unique and unambiguous.

Finally, the taxonomy must be exhaustive and useful for a broad audience. Many attempts have been made at classifying vulnerabilities and attacks, but most do not meet the above requirements. A typical error seen in the classifications previously discussed is to use different types of taxonomic characteristics at the same level. This leads to ambiguities or nonsensical questions similar to asking "whether something breathes air or has eyes".

Vulnerabilities are conceptual entities, not objects or lines of codes; this is an additional challenge to their understanding and classification, because desirable taxonomic characters should be observable without speculation. They exist at several different conceptual and abstraction levels; many vulnerabilities may exist simultaneouslyat several levels. In addition, the notions of cause or effect suffer from the problem that vulnerabilities may depend on several mishaps in a sequence of events. A "buffer overflow" may have been caused by an "integer overflow" issue. An off-by-one miscalculation resulting in an NUL-termination problem may enable the joining of two string buffers, which then provides sufficient space for a format string attack to be successful (CVE-2001-0609). There is also a possible decoupling of the coding mistake versus the exploit location. An overflow may first occur in a heap buffer, but become (more easily) exploitable when the string is copied to a buffer of the same size on the stack (CVE-2006-0855); in this case, the second copy is justifiably "correct". Information about vulnerabilities is often incomplete and revealed progressively, which may change the "dominant" or primary aspect of the vulnerability or its "cause" as more details are learned.

Taxonomies that use criteria oriented toward defining what programmers, designers, and architects have done incorrectly (implying what they should or could have done) have had fatal flaws [24–27]. The reasons why these taxonomies are incorrect were previously analyzed [1, 9]. Intuitively, this can be understood because there are vulnerabilities whose exploitation could have been prevented or fixed by any of several different ways and mechanisms; therefore, the classification of the vulnerability by the prevention measure or error is ambiguous. Typically, these measures also involve different concepts and levels of abstraction. This situation is even expected when a vulnerability arises from an underspecified API [2].

Taxonomies also have a domain of validity and purpose, or scope and viewpoint, for example, web services [28]. The specific data used to classify vulnerabilities depend upon the specific goals of the classification [23]. However, the scope and the taxonomic criteria should be technical in nature to avoid speculation [23]. The classification of environmental assumptions proposed by Krsul [1] has limited usefulness, because the definition of its scope requires knowing the distinction between a designer misunderstanding the environment and making a simplifying assumption about it. This may be difficult to decide, even in retrospect; it is not objective. So, it is not sufficient that taxonomic characteristics inside the taxonomy have the properties defined above; the scope of the taxonomy should also possess them.

### 4.1 Classification by Violated Program Invariant

Most vulnerabilities can be expressed in the form of an assumption, explicit or implicit, that did not hold [1]. Some assumptions can be expressed as program or unitwide invariants, others specifically as preconditions and postconditions to algorithms, functions. All these properties need to hold true for the program to be correct. Some can be explicitly tested, for example, by using "assert" statements. Some invariants that are not tested or stated can be discovered by dynamic analysis [29].

Buffer overflows are primarily the result of violating the invariant that data should only be read or written to within the space allocated for it. They are very common in "C" because the programming language makes the preservation of that invariant difficult and error-prone. As a result, "buffer overflow" is a common vulnerability type that could belong to a taxonomy where vulnerabilities are classified by violated invariant or assumption. Such taxonomies have the potential to be very powerful and precise. Unfortunately, many assumptions are made unknowingly, and they tend to be unique, which results in a high cardinality of "types". For these reasons, it is not useful to try to express all vulnerabilities as violated assumptions or violated program invariants. However, the explicit specification of invariants in programming languages such as Spark, where they get verified, can be quite useful in avoiding vulnerabilities [30].

## 5 ENUMERATION OF ATTACK AND VULNERABILITY TYPES

As an alternative to producing a rigorous taxonomy from the top down, efforts have tried to tackle the enumeration of all known attack and vulnerability types from a very low level. These enumerations in effect form both test cases and requirements for successful taxonomies. Because of their high cardinality nature, it is impossible to list the enumerated types in this article. The following is merely an introduction to these efforts, pointing out their useful properties.

### 5.1 Plover

The preliminary list of vulnerability examples for researchers was an MITRE effort grouping CVE issues by low-level types of weaknesses [31]. It has been superseded by the common weakness enumeration (CWE) (see below). This was the first attempt to build an "a posteriori" classification, that is, bottom-up ("a priori" classifications are built top down, from a theoretical standpoint).

### 5.2 Common Weakness Enumeration (CWE)

The CWE is an MITRE-driven effort to produce a "standard dictionary of software security weaknesses" [32]. The CWE attempted to be a community effort by enlisting industry, academia, and government. Amongst many benefits, it should allow the verification of coverage claims made by software security tool vendors and service providers [32]. At the top level, the CWE contains "location", "genesis", and "time of introduction" classifiers, which can be used independently, as is applicable and as knowledge permits.

The "genesis" classifier is subject to the limitations and objections noted before. The subcategories for the time of introduction classifier are very detailed, considering events such as bundling and porting. Because the subcategories are flat, a high level of knowledge is required to match the high level of detail in order to make a correct choice. Otherwise, classifications will be biased toward more generic-sounding categories such as "design" or "implementation".

The "location" classifier is subdivided into environment, configuration, and code. Configuration issues are not further expanded upon, and should be the subject of further research (cf. the MITRE CCE effort), especially when configuration options are so complex as to require their own language (is it code then?). The code subcategories are subject to the criticisms appropriate to the classifications borrowed by the CWE. It is, however, very interesting to see how the PLOVER examples were mapped to those classifications.

### 5.3 Common Attack Pattern Enumeration and Classification (CAPEC)

Common attack pattern enumeration and classification (CAPEC) describes attack patterns and relates them to weaknesses in the CWE. It includes "not only weaknesses directly related to the attack but also those whose presence can directly increase the likelihood of the attack succeeding or the impact if it does succeed" [33]. The CAPEC schema description is a work performed under contract for the Department of Homeland Security, and is therefore public.

Attack patterns aim to represent aggregate abstract information about similar attacks: "An attack pattern is a general framework for carrying out a particular type of attack, such as a method for exploiting a buffer overflow or an interposition attack that leverages certain kinds of architectural weaknesses" [34]. As such, they are a form of attack classification.

## 6 ONTOLOGIES AND FUTURE RESEARCH

The definition of a common language for computer security is an important step toward being able to describe and communicate vulnerability and attack knowledge [5]. Seacord and Householder observe that the classical taxonomy approach has not worked well in security and suggest "a structured approach to classifying security vulnerabilities". They do this by describing vulnerabilities and exploits as things with properties [35], which resemble part of an ontological approach to the problem.

Vulnerabilities are concepts, and many taxonomies attempt to link them to more concepts. Ontologies are models of reality in the form of a highly structured system of concepts, including their properties. So, in reality, these "taxonomies" are attempts at creating partial ontologies. They present a reduced ("flattened") or simplified view of the accumulated knowledge, and may be appropriate for limited, specific purposes, as defined by their scope and goals. To completely and accurately represent, transmit knowledge, and discuss vulnerabilities and attacks, proper ontologies are required.

Common ontologies address a clearly defined but restricted domain. The wider the domain, the more difficult the task may be. Upper ontologies are applicable across a wide

range of domain ontologies, but are difficult to create. One reason why an upper ontology may succeed where taxonomies failed is that ontologies can be more flexible and complex. Ontologies may allow an object to belong to several classes at once, because partitions are not necessarily disjoint. Also, through the use of relations (e.g. "part-of") they may allow multiple "memberships" or inheritances to represent complex cases. It is believed that an upper ontology created this way could have simpler "views" (e.g. subsets of the relations and concepts) appropriate to particular domains or applications. In practice, a number of regular ontologies with smaller domains could be created before the task of an upper ontology is addressed. They would also be easier to use. The development of such ontologies is left for future research.

## REFERENCES


1. Krsul, I. V. (1998). *Computer Vulnerability Analysis*, PhD thesis, Purdue University.
2. Weber, S., Karger, P. A., and Paradkar, A. (2005). A software flaw taxonomy: aiming tools at security. *Software Engineering for Secure Systems (SESS'05)* St. Louis, Missouri.
3. Howard, M., LeBlanc, D., and Viega, J. (2005). *19 Deadly Sins of Software Security*. McGraw-Hill/Osborne, Emeryville, CA.
4. Dowd, M., McDonald, J., and Schuh, J. (2006). *The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities*. Addison-Wesley, Boston, MA.
5. Howard, J. D., and Meunier, P. (2002). Using a "common language" for computer incident security information. In *Computer Security Handbook*, Chapter 3, S. Bosworth, and M. E. Kabay, Eds. John Wiley & Sons, New York.
6. Piessens, F. A. (2002). Taxonomy of causes of software vulnerabilities in Internet software. In *Supplementary Proceedings of the 13th International Symposium on Software Reliability Engineering*, M. Vouk, Ed. IEEE Computer Society Press, Los Alamitos, CA. pp. 47–52.
7. Landwehr, C. E., Bull, A. R., McDermott, J. P., and Choi, W. S. (1994). A taxonomy of computer program security flaws. *ACM Comput. Surv.* **26**(3), 211–254.
8. Bishop, M. (1995). *A Taxonomy of Unix System and Network Vulnerabilities*, Technical Report CSE-9510, Department of Computer Science, University of California, Davis.
9. Bishop, M., and Bailey, D. (1996). *A Critical Analysis of Vulnerability Taxonomies*, Technical Report CSE-96-11, Department of Computer Science, University of California, Davis.
10. ISO 7498:1984 Open Systems Interconnection—Basic Reference Model.
11. Du, W., and Mathur, A. P. (1998). Categorization of software errors that led to security breaches. *Proceeding of the 21st National Information Systems Security Conference (NISSC'98)*. Crystal, VA.
12. Pothamsetty, V., and Akyol, B. A. (2004). A vulnerability taxonomy for network protocols: corresponding engineering best practice countermeasures. *Communications, Internet, and Information Technology*. St. Thomas, US Virgin Islands.
13. Secure Software. (acquired by Fortify). (2008). *Comprehensive, Lightweight Application Security Process*. Available at: http://www.owasp.org/index.php/Category:OWASP_CLASP_Project.
14. Tsipenyuk, K., Chess, B., and McGraw, G. (2005). Seven pernicious kingdoms: a taxonomy of software security errors. *IEEE Secur. Priv.* **3**(6), 81–84.
15. Christey, S., and Wysopal, C. (2002). *Responsible Vulnerability Disclosure Process*. The Internet Society, INTERNET-DRAFT "draft-christey-wysopal-vuln-disclosure-00.txt".

16. Wing, J. M. (2003). A call to action. *IEEE Secur. Priv.* **1**(6), 62–67.
17. MITRE Common Configuration Enumeration (CCE). (2008). http://cve.mitre.org/cce/
18. MITRE Common Vulnerability Enumeration (CVE). (2008). http://cve.mitre.org/
19. Lippmann, R., Haines, J. W., Fried, D. J., Korba, J., and Das, K. (2000). The 1999 DARPA off-line intrusion detection evaluation. *Comput. Networks* **34**(4), 579–595.
20. Chambers, J. T., and Thompson, J. W. (2004). *Common Vulnerability Scoring System*, tech. report, US Nat'l Infrastructure Advisory Council. Available at: www.dhs.gov/xlibrary/assets/niac/NIAC_CVSS_FinalRpt_12-2-04.pdf.
21. Cohen, F. B. (1991). *A Case for Benevolent Viruses*. Fred Cohen & Associates, http://www.all.net/books/integ/goodvcase.html.
22. Sophos. (2003). 'W32/Nachi-A', available at: http://www.sophos.com/virusinfo/analyses/w32nachia.html.
23. Bishop, M. (1999). Vulnerabilities analysis. *Web Proceedings of the 2nd International Workshop on Recent Advances in Intrusion Detection (RAID'99)*, West Lafayette, Indiana http://www.raid-symposium.org/raid99.
24. Bisbey II R., and Hollingworth, D. (1978). *Protection Analysis: Final Report*. USC/ISI, Marina Del Rey, CA.
25. Neumann, P. G. (1978). Computer system security evaluation. *1978 National Computer Conference Proceedings (AFIPS Conference Proceedings 47)*, Arlington, VA June 1978, pp. 1087–1095.
26. Abbott, R. P., Chin, J. S., Donnelley, J. E., Konigsford, W. L., Tokubo, S., and Webb, D. A. (1976). *Security Analysis and Enhancements of Computer Operating Systems National Bureau of Standards*. Accession Number: ADA436876.
27. Aslam, T. (1995). *A Taxonomy of Security Faults in the UNIX Operating System*, Master of Science thesis, Department of Computer Sciences, Purdue University, West Lafayette, IN.
28. Vanden Berghe, C., Riordan, J., and Piessens, F. (2005). A vulnerability taxonomy methodology applied to web services. In *Proceedings of the 10th Nordic Workshop on Secure IT Systems (NordSec)*, H. Lipmaa, and D. Gollmann, Eds. Helsinki University of Technology, Espoo. pp. 49–62.
29. Ernsty, M. D., Czeislery, A., Griswoldz, W. G., and Notkiny, D. (2000). Quickly detecting relevant program invariants. *ICSE 2000, Proceedings of the 22nd International Conference on Software Engineering*. Limerick, June 7–9, pp. 449–458.
30. Barnes, J. (2003). *High Integrity Software: The SPARK Approach to Safety and Security*. Addison-Wesley, Boston, MA.
31. Christey, S. *PLOVER: Preliminary List Of Vulnerability Examples for Researchers*. Available at: http://cve.mitre.org/docs/plover/plover.html.
32. Martin, R. A., Christey, S., Jarzombek, J. (2005). The case for common flaw enumeration. *NIST 2005 Workshop on Software Security Assurance Tools, Techniques, and Methods*. Long Beach, CA.
33. Barnum, S. (2006). *Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description* (U.S Department of Defense under Contract HSHQPA-05-A-00035). Cigital, Dulles, VA.
34. Barnum, S., Sethi, A. (2006). *Introduction to Attack Patterns*. Available at: https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/attack/585.html?branch=1&language=1.
35. Seacord, R. C., and Householder, A. D. (2005). *A Structured Approach to Classifying Security Vulnerabilities*, Technical note CMU/SEI-2005-TN-003 Carnegie-Mellon University/Software Engineering Institute, PA.

# AUTHENTICATION, AUTHORIZATION, ACCESS CONTROL, AND PRIVILEGE MANAGEMENT

DAVID FERRAIOLO, RICK KUHN, AND VINCENT HU
*National Institute of Standards and Technology, Gaithersburg, Maryland*

## 1 INTRODUCTION

Homeland security applications present a number of cutting-edge challenges for access control and privilege management because they necessarily entail the integration of physical and information technology (IT) system access controls. Airports, industrial plants, and many other critical infrastructure domains have physical assets that could, in the wrong hands, result in significant loss of life. To get a sense of the problem space, consider the following incidents:

- *Sewage release.* In 2000, an employee of an Australian company that develops industrial control software used a wireless connection to illegally access the control system for a sewage treatment plant, causing eventually the release of 264,000 ga of raw sewage [1].
- *Air traffic control and emergency services.* In 1997, an attacker disabled a critical telephone switch through a dial-up modem, shutting down tower control and air traffic transmission at an airport in Worcester, Massachusetts. Telephone service was disabled for a nearby town also [2].
- *Train derailment.* In January, 2008, a 14 year old in Lodz, Poland took over the control system for city trains, derailing four and injuring several people [3].

None of these incidents would have occurred if access control had worked properly, and the potential for terrorist attacks, beyond the damage described above, should be clear. This article reviews access control models, with their underlying processes of authentication and authorization, and how various models are used in privilege management.

## 2 AUTHENTICATION AND AUTHORIZATION

Authorization and authentication are fundamental to access control. They are distinct concepts but often confused. Part of the confusion stems from the close relationship between the two; proper authorization in fact is dependent on authentication. Authentication can be defined as verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system, whereas authorization is granting or denying access rights to a user, program, or process.

Authentication determines if a user's claimed identity is legitimate. Every computer user is familiar with passwords, the most common form of authentication. Less common forms of authentication include biometrics (e.g. fingerprint readers) and smart cards. Authentication is a process of determining who you are, whereas authorization determines what you are allowed to do. Authorization refers to a yes or no decision as to whether a user is granted access to a system resource.

## 2.1 Authentication Technology

An extensive collection of authentication methods and products is available on the market, ranging from simple and nearly universal approaches, such as passwords, to sophisticated biometric devices. Each method has its own strengths and weaknesses, and the strongest authentication may require more than one approach. A password can be guessed; a key can be lost; and face recognition systems have a significant false positive rate, so using only one of these authentication methods may not provide an acceptable level of security. This is why banks require both cards and personal identification numbers (PINs) to access automatic teller machines (ATMs) rather than only a password, or only a key or card. If the card were lost, a thief would have to guess the PIN in only three tries to beat the authentication system.

Authentication is based on one or more of three factors: (i) something you know, such as the password, PIN, or lock combination; (ii) something you have, such as a smart card, ATM card, or key; (iii) a physical characteristic, "something you are", such as a fingerprint or retinal pattern, or a facial characteristic.

Careful design can provide strong authentication at low cost, as with the ATM example above. Fraudulent ATM transactions have consistently been a fraction of 1% of volume throughout the industry for many years. The problem of authentication continues to be an active field of research as new products and methods appear each year. In this section, we review some of the most significant techniques for human and computer system authentication.

***2.1.1 Personal Authentication.*** Authenticating a user to a computer system requires one or more of the factors given in the introductory section above.

*2.1.1.1 Passwords.* Passwords (something you know) are clearly the most common form of authentication, since they provide adequate security for many applications and are easy to set up. However, it is important to keep in mind that with sufficient time, or a sufficiently large number of accounts, an attacker will inevitably be able to guess a working password if users are able to choose arbitrary passwords. One recent study [4] found the following 10 most commonly used passwords, so an attacker trying words from this list across several thousand accounts would be almost certain to succeed: password, 123456, qwerty, abc123, letmein, monkey, myspace1, password1, blink182, (user's first name). A variety of guidelines for choosing and managing strong passwords can be found at government and industry organizations, such as National Institute of Standards and Technology (NIST)'s Publication 800-114 [5].

*2.1.1.2 Smart Cards and Other Tokens.* Token-based authentication schemes can improve authentication security by requiring the user to possess a physical token (something you have) that the system can recognize as belonging to a particular user.

ATM cards are the most widely used example. Tokens typically contain information that is physically, magnetically, or electrically coded in a form that can be recognized by a host system. More sophisticated tokens, for example, smart cards, contain one or more integrated circuits, which can store and, in some cases, process information. Token-based systems reduce the threat from attackers who attempt to guess or steal passwords, because the attacker must either fabricate a counterfeit token or steal a valid token from a user in addition to knowing the user's password. Even smart cards provide no guarantees however, as several sophisticated systems have been demonstrated to have weaknesses that make them vulnerable to counterfeiting [6, 7].

*2.1.1.3 Biometrics.* Biometric characteristics are being used increasingly for authentication, as technology costs come down. Biometrics includes a variety of human characteristics and can be roughly divided into two clusters: static and dynamic. Static biometrics are relatively fixed: fingerprint, face, handprint, iris, and DNA. Dynamic biometrics include active characteristics of a user: signature, voice, typing speed and rhythm, and others.

- Fingerprints—well known and used since the nineteenth century, fingerprints are often assumed to be a foolproof method of user authentication, and many computers are supplied with built-in fingerprint readers. However, effective means of defeating fingerprint readers, even with live sensing, are well known [8].
- Iris scanners—base authentication on pattern recognition algorithms applied to an image of a user's eyes. Iris recognition is quite accurate, with an average current false match rate of 0.001 and false nonmatch rate of 0.0122–0.03847. In other words, only one in a thousand imposters would fool the system, but roughly 1–4% of legitimate users will be rejected [9]. Some methods of defeating iris recognition under controlled conditions have been demonstrated.
- Facial recognition technology is not as well developed as other biometric methods but has advanced rapidly. The best systems achieve a false acceptance rate of 0.001 and a false reject rate of 0.01 on very high resolution images in controlled conditions [10], but results are much worse in less controlled situations. Different applications may use one or more of the following settings: single still image, multiple still image, uncontrolled conditions, and different types of 3D images.
- Keystroke dynamics attempts to recognize users based on measurements such as time between key presses for various pairs of keys, the length of time the keys are down, and the speed of typing letter combinations. These measurements are used as input to pattern recognition algorithms to distinguish among possible users. Error rates are significantly higher than other biometrics, but keystroke dynamics can be used covertly for user recognition, or combined with other methods to provide relatively high strength authentication [11].
- Other biometric authentication technologies include hand geometry, walking gait, and signature recognition. Commercial implementations of these methods have not developed to the degree of other biometrics.
- The Biometric Consortium has information on a wide range of technologies and biometric standards at: http://www.biometrics.org/. Additional resources are maintained by the US Department of Defense: http://www.biometrics.dod.mil/. Evaluations of commercial and research biometric product accuracy are conducted by NIST: http://biometrics.nist.gov/

***2.1.2 Web Authentication.*** Computer-to-computer authentication is very different from the case where one end of the communication is a human and the authentication methods take full advantage of a machine's storage and computational power. Hypertext transfer protocol (HTTP) basic authentication [12] provides a standard format to send user login ID and password for authentication of users at a website. Because it assumes that transmissions from the user to the website are secure, encryption is not used. Thus, basic authentication should be considered very weak, but for applications with minimal security requirements it may be an acceptable solution.

HTTP digest authentication [12] is a stronger authentication method for web browsers. Digest authentication protects authentication information from packet sniffers and makes it possible to avoid storing a clear-text password. Timestamps can also be used to prevent replay attacks. However, digest authentication relies on an algorithm (MD5) that has never been approved by the US Government because of known weaknesses. Implementation is complicated by the fact that the standard contains options that may allow operation in a reduced security form, either an obsolete variant of digest authentication or the weaker basic authentication.

### 2.2 Authentication Standards

Standards are important in any mature field of IT, but are particularly critical for authentication because of the need for interoperability among products. The primary US standards body dealing with IT standards is the International Committee on Information Technology Standards (INCITS) [13], which operates under the auspices of the American National Standards Institute (ANSI).

Active groups within INCITS that are relevant to authentication include the M1 biometrics group and B10 identification cards and related devices. INCITS M1 includes the following: M1.2, biometric technical interfaces, develops standards for secure transfer of stored data between systems; M1.3, biometric data interchange formats, addresses standardization of content and representation of biometric data exchange formats; M1.4, biometric profiles, deals with profiles for biometric-based verification and identification of transportation workers, border management, and point of sale; M1.5, biometric performance testing and reporting, is standardizing performance metrics, testing, and result reporting for biometrics; M1.6, cross jurisdictional and societal issues, covers standards related to societal aspects of biometric implementations. INCITS B10—identification cards and related devices working group covers standards for international or interorganizational exchange of biometric data.

Security standards and practices are also promulgated by the NIST [14], a consortium that develop industry-specific standards, such as the Payment Card Industry Standards Council [15], and Internet Engineering Task Force (IETF) [16] for internet protocol standards, including web applications.

## 3 ACCESS CONTROL AND PRIVILEGE MANAGEMENT

Authentication and authorization mechanisms are the building blocks that must be integrated into a coherent access control policy. The ability to enforce access control policies is a critical capability of most modern day enterprises. Policies are enterprise requirements that specify how access is managed and who, under what circumstances, may

access what information. Among other issues, security policy enforcement is instrumental in preventing the unauthorized disclosure of sensitive data, protecting the integrity of vital data, mitigating the likelihood of fraud, and ultimately enabling the secure sharing of information. The ability to enforce access control policy can be of great economic and mission importance. Although access control is often specified in terms of limitations or protections, the ability of an organization to enforce access control policy is what ultimately enables the sharing of greater volumes of data and resources to a greater and more diverse user community.

Access control policies are enforced through a mechanism consisting of a fixed system of functions and a collection of access control data (reflecting the configuration of the mechanism) that together map a user's access request to a decision whether to grant or deny access. Included in the access control data is the set of permissions—each indicating a user's potential to perform an operation (e.g. read and write) on object or resource. Regarding a specific mechanism, permissions are not individually specified, but instead permissions are organized in terms of, and mapped (through administrative operations or a predefined set of rules) onto a set of user, subject (processes), and recourse attributes, pertaining to a specific type or class of policy. Also common to access control mechanisms is a requirement to store and authenticate user identities. From an authenticated identity, an access control mechanism is able to establish a security context (activate a specific identity, groups or other attributes) as a basis for granting or denying user and process access requests to resources managed under the control of the mechanism at hand. Operationally access control mechanisms compute a series of decisions based on the specifics of the access control data, and ultimately enforce policy based on those decisions.

To understand management issues and solutions requires a basic understanding of the underlying access control models and approaches that are implemented in today's commercially available products. Although a large number of access control models have been proposed in an attempt to solve real-world access control policy issues, today's operating systems (OSs) are limited to the enforcement of instances of discretionary access control (DAC) and simple variations of role-based access control (RBAC) policies, and to a far lesser extent, instances of mandatory access control (MAC) policies. Each of these models is described below.

### 3.1 Discretionary Access Control (DAC)

DAC [17] is a means of restricting access to objects based on the identity of users or the groups to which they belong, or both. Controls are discretionary in the sense that the object's "owner" has control permission to grant access permission to the object for other subjects. Perhaps the most common approach to representing and administering DAC policies is through the use of access control lists (ACLs). Each object is associated with an ACL that stores the users and the user's approved operations for the object. The list is checked by the access control system to determine if access is granted or denied.

The principal advantage of ACLs is that they make it easy to review the users who have access to an object, as well as the operations that users can apply to the object. In addition, it is easy to revoke access to an object by simply deleting an ACL entry. These advantages make ACLs ideal for implementing policies that are object oriented, such as the policy of DAC. Another advantage is that the lists need not be excessively long, if groups of users with common accesses to the object are attached to the object instead of

the group's individual members. A serious disadvantage of DAC is that it is inherently unsafe because users can give away access to others, and the organization cannot control the propagation of the information beyond the owner.

### 3.2 Mandatory Access Control (MAC)

MAC [17] policies remove the user's ability to give away access rights, by controlling access at an organization level. With regard to this policy, security levels are assigned to users, with subjects acting on behalf of users, and to objects. Security levels have a hierarchical and a nonhierarchical component. For instance, the hierarchical components might include "unclassified" (U), "confidential" (C), "secret" (S), and "top-secret" (TS) whereas the nonhierarchical components may include "NATO" and "NUCLEAR". The security levels are partially ordered under a dominance relation, often written as "$\geq$". For example, TS $\geq$ S $\geq$ C $\geq$ U and S (NATO, NUCLEAR) $\geq$ S (NUCLEAR) $\geq$ S. The security level of the user, often referred to as the *user's clearance level*, reflects the level of trust bestowed to the user and must always dominate the security levels that are assigned to the user's subjects. The security levels that are assigned to objects, often referred to as the *object's classification level*, reflect the sensitivity of the contents of the objects. Access control decisions are made in accordance with the following two properties:

- *Simple security property.* A subject is permitted read access to an object if the subject's security level dominates the security level of the object.
- *Star property.* A subject is permitted write access to an object if the object's security level dominates the security level of the subject.

Satisfaction of these properties prevents users from being able to read information that dominates (i.e. is above) their clearance level. The simple security property directly supports this policy, never allowing a subject to read information that dominates the invoking user's clearance level. The star property supports the MAC policy indirectly, by disallowing subjects from writing information of level $x$ into a container (contents of an object) that could be subsequently read by a subject with a security level that is dominated by $x$. Intuitively, the star property prevents high information from ending up in a low container where a low user could read it.

### 3.3 Role-Based Access Control

In an attempt to streamline authorization management, RBAC models [18, 19] and more recently an RBAC standard [20] have been developed. When deployed, RBAC features offer greater administrative efficiency as well as the ability to intuitively administer and enforce a wide range of commercial access control policies. In RBAC, permissions are associated with roles, and users are made members of roles, thereby acquiring the role's permissions. The implementation of this basic concept has been shown to greatly simplify access control management. Roles are centrally created for the various job functions in an organization, and users are assigned roles based on their responsibilities and qualifications. As such, users can be easily reassigned from one role to another. Users can be granted new permissions as new applications and systems are incorporated, and permissions can be revoked from roles as needed. For example, if a user moves

to a new function within the organization, the user can simply be assigned to the new role and removed from the old one, whereas in the absence of the RBAC, the user's old privileges would have to be individually located, revoked, and new privileges would have to be granted. This includes the specification of duties, responsibilities, and qualifications. For example, the roles that an individual associated with a hospital can assume include doctor, nurse, clinician, and pharmacist. Roles in a bank include teller, loan officer, and accountant. Roles can also apply to military systems; for example, target analyst, situation analyst, and traffic analyst are common roles in tactical systems. An RBAC policy bases access control decisions on the functions a user is allowed to perform within an organization. The users cannot pass access permissions on to other users at their discretion. This is a fundamental difference between RBAC and DAC.

### 3.4 Policy Enforcement Issues

Although DAC and RBAC mechanisms dominate the marketplace, they can be weak in their ability to enforce policy. Consider an RBAC policy where only a user in the role of doctor can read medical records. While reading a medical record, nothing prevents the doctor, or a Trojan horse embedded in the doctor's application, from making a copy of the record to a file that is accessible by a user that is not a doctor. As stated above, today's OSs are limited to the enforcement of instances of DAC, RBAC, and MAC policies. As a consequence, there exist a number of important policies (orphan policies) that lack a commercially viable OS mechanism for their enforcement.

### 3.5 Application-Level Mechanisms

To fill policy voids, policies are routinely accommodated through the implementation of access control mechanisms at the application level, often independent of any underlying OS access control mechanism. Examples include database management systems, enterprise calendars, and time and attendance. Although not normally considered in the realm of access control, e-mail and workflow management systems provide access control services as well. E-mail provides for the reading of messages and attachments, through the discretionary distribution of objects, and workflow provides the reading and writing of specific documents for a prescribed sequence of users. Essentially, any application that requires a user's authentication implements some form of access control. Applications can aggravate identity and privilege management problems, and also undermine policy enforcement objectives. For instance, although a file management system may narrowly restrict access to a specific file, chances are the contents of that file can be attached to or copied to a message and mailed to anyone in the organization or the world.

## 4 INTEROPERABILITY ISSUES

Access control mechanisms come in a wide variety of forms, each with their individual method for authentication, access control data constructs for expressing and managing policy, and functions for making access control decisions and enforcement of policies. Although standardized access control models and specifications may prescribe a strategy for achieving uniform policy support at some level of discourse, they should not be confused with a method for affording interoperability. This is because models and

specifications can and often are implemented in different ways, and thus result in different access control mechanisms. For example, the standard for DAC can be successfully met through the implementation of protection bits, ACLs, or capability lists [21], and consequently each implementation will result in a dramatically different mechanism. Deploying a multitude of heterogeneous systems results in a lack of interoperability. Although this may not be a problem for systems that can adequately operate independently of one another, access control mechanisms clearly do not fall into this category of systems. Users with vastly different credentials have a need to access resources protected under different mechanisms, and resources that are protected under different mechanisms differ vastly in there sensitivity, and therefore accessibility. This lack of interoperability in today's access control paradigm introduces significant privilege and identity management challenges.

In an attempt to enforce global policies, an enterprise has two choices—either procedurally coordinate the administration of access control data among relevant mechanisms or deploy an enterprise security management product. Enterprise security management products attempt to overcome interoperability problems through centralized policy specification and local decision making and enforcement. However, in the end, enterprises are limited to the weak enforcement of fairly simple global policies. This is because the space of enforceable policies is restricted to those policies that can be derived through administrative techniques (manual or automated) alone and are otherwise bound by the decision-making and enforcement functions of the underlying mechanisms. For instance, although simple RBAC policies may be configured and globally enforceable over mechanisms that provide user identity and group structures [18], no administrative technique can be applied over these mechanisms to enable the enforcement of a MAC policy. Even these simple policies cannot be truly globally enforced. For instance, users are now accustomed to being able to copy the content of an object that is protected under one mechanism and paste the content into a second object protected under a different mechanism. In today's paradigm, there does not exist a means to enforce access control policies over such actions. Furthermore, application-level access control mechanisms have the potential to undermine global policies. Although a global policy may restrict user access to information under one policy or another, nothing may stop a user from attaching an otherwise-protected object to an e-mail message and sending the message to an unauthorized user, or prevent a sender from inadvertently routing sensitive data to an unauthorized recipient through a workflow application.

## 5 EMERGING SOLUTIONS

To solve the interoperability and policy enforcement problems of today's access control paradigm, NIST (in part under sponsorship of the Department of Homeland Security) has developed an access control standard, referred to as the *policy machine ( PM )* [22]. Its objective is to provide a unifying framework to support not only current OS and application polices but also a host of orphan polices for which no mechanism yet exists for their viable enforcement. The PM requires changes only in its data configuration in the enforcement of arbitrary and organization-specific, attribute-based access control policies.

A comprehensive reference implementation of PM features has been under development during the past 2 years. Demonstrated benefits now include the following:

- *Policy flexibility.* Virtually any collection of attribute-based access control policies can be configured and enforced (e.g. DAC, multilevel security (MLS), Chinese wall,

user controlled (UCON), and object-based separation of duty (SoD)). In addition, basic application services can be provided through PM configuration to include those services offered by workflow management, e-mail, and database management applications.

- *Policy combinations.* Resources (objects) regardless of their type can be selectively protected under one or more currently configured policies (e.g. DAC only, or DAC and RBAC combined).
- *Comprehensive enforcement.* All user access and subject (process) access requests, and all exchange of data to and from and among applications, between sessions, all exportation of data outside the bounds of the PM can be uniformly controlled under the protection policies of the objects of concern (e.g. "copy and paste", e-mail, workflows, granting access, file management, and writing to devices and ports).
- *Assurance.* Configuration strategies can render malicious application code harmless and prevent unlawful leakage of data, all enforcement could be implemented at the kernel level, and attributes are automatically and minimally assigned to sessions (least privilege) to fit a user's access requests (as opposed to a user's need to select attributes or a user's session provided with all attributes of the user).

The features described above could be provided through a number of PM architectural deployments to include its implementation within a single-OS environment. Our reference implementation provides centralized policy configuration and decision making with local OS enforcement. This PM deployment affords still additional benefits as listed below:

- *Single enterprise-wide scope of protection.* One administrative domain versus policy management on an OS-by-OS and application-by-application basis. Access control policies are uniformly enforced over resources that are physically stored on a multitude of heterogeneous systems.
- *True single sign on.* By virtue of the PM's single scope of control, and a personal object system (POS) that includes the ability to reference and open any resource accessible to a user (e.g. e-mail messages, work items, files, records and fields within records), eliminates the need for a user to authenticate to a multitude of applications and hosts.
- *Logical access.* Any accessible resource could be securely accessed through any PM-compliant OS with access to an application to process the resource.
- *Minimized OS vendor support.* To be PM compliant, all an OS vendor needs to do is implement a standard set of enforcement functions (i.e. PM authentication, user resource presentation, session management and reference mediation), and does not need to be concerned with the management of access control data or the execution of access control decisions.

With the PM's advantages over the existing access control paradigm, coupled with a minimum investment on the part of OS vendors, there exists a strong business argument in favor of the adoption of the PM. Moreover, the features that provide these benefits are native to the PM and as such are afforded without the deployment and expense of less effective privilege management, provisioning, identity management, or synchronization products.

## REFERENCES


1. Stouffer, K., Falco, J., and Scarfone, K. (2008). *Guide to Industrial Control Systems Security*, NIST SP 800-82, citing: www.iti.uiuc.edu/events/2005_09_15_Jeff_Dagle.pdf.
2. Stouffer, K., Falco, J., and Scarfone, K. (2008). *Guide to Industrial Control Systems Security*, NIST SP 800-82, citing: http://www.cnn.com/TECH/computing/9803/18/juvenile.hacker/index.html
3. Leyden, J. (2008). *Polish Teen Derails Tram After Hacking Train Network, The Register*, 11 January, http://www.theregister.co.uk/2008/01/11/tram_hack/.
4. 10 Most Common Passwords, http://www.pcmag.com/article2/0,1759,2113976,00.asp, (2008).
5. Scarfone, K., and Souppaya, M. (2007). *User's Guide to Securing External Devices for Telework and Remote Access*, NIST SP 800-114, November. http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf.
6. Lea, G. (2000). *France Braces for Smart Card Fraud Onslaught, The Register*, 14 March http://www.theregister.co.uk/2000/03/14/france_braces_for_smart_card/.
7. http://www-08.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper04.pdf, (2008).
8. How to Fake Fingerprints, Chaos Computer Club e.V. http://www.ccc.de/biometrie/fingerabdruck_kopieren.xml?language=en, (2008).
9. http://iris.nist.gov/ice/, (2008).
10. http://face.nist.gov/, (2008).
11. de Magalhaes, S. T., Revett, K., and Santos, H. M. D. (2005). Password secured sites—stepping forward with keystroke dynamics. *Next Generation Web Services Practices, 2005. NWeSP 2005. International Conference on*. Issue 22–26 August p. 6.
12. Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Luotonen, A., and Stewart, L. (2008). *RFC 2617. HTTP Authentication: Basic and Digest Access Authentication*, Internet Engineering Task Force, http://www.usfst.com/pastissue/article.asp?art=26023&issue=153.
13. http://www.incits.org, (2008).
14. http://csrc.nist.gov, (2008).
15. http://www.pcisecuritystandards.org/, (2008).
16. http://letf.org/html.charters/wg-dir.html#Security%20Area, (2008).
17. Department of Defense. (1985). *Department of Defense Trusted Computer System Evaluation Criteria*. Department of Defense 5200.28-STD, Washington, DC.
18. Ferraiolo, D. F., and Kuhn, D. R., (1992). Role-based access control. *15th National Computer Security Conference*. National Security Agency/National Institute of Standards and Technology, Baltimore MD, pp. 554–563.
19. Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-based access control models. *IEEE Comput.* **29**(2), 38–47.
20. International Committee for Information Technology Standardization. (2004). *Role Based Access Control*. INCITS 359–2004. Washington, DC.
21. Lampson, B. (1971). Protection, *Proceedings of the 5th Princeton Symposium On Information Science and Systems*. Princeton, NJ, pp. 437–443.
22. Ferraiolo, D. F., Gavrila, S., Hu, V., and Kuhn, D. R. (2005). Composing and combining policies under the policy machine. *ACM Symposium on Access Control Models and Technologies*. Stockholm, pp. 22–20.

# ADVANCED ATTACKER DETECTION AND UNDERSTANDING WITH EMERGING HONEYNET TECHNOLOGIES

RONALD C. DODGE JR.
*United States Military Academy, West Point, New York*
THORSTEN HOLZ
*Aachen University, Aachen, Germany*
ANTON CHUVAKIN
*LogLogic, San Jose, California*

## 1 HONEYPOT ESSENTIALS

Honeypots and honeynets are well known to security processionals. Newly developed honeynet techniques and technologies are a hot topic in information security. However, the amount of technical information available on their setup, configuration, and maintenance is still sparse as are qualified people with the capability to run them, interpret the activity, and make security recommendations. Higher-level guidelines, such as a need and business case determination, are similarly absent. In addition, honeypot risks, such as legal authority and ethical use, need to be fully evaluated prior to honeynet deployments. In this article, we present a brief introduction to honeynet technologies, a short word on ethical and legal considerations, and then describe four of the most productive honeynet technologies.

What is a honeypot? Lance Spitzner, a founder of Honeynet Project [1] defines a honeypot as "a security resource whose value lies in being probed, attacked or compromised". Thus, a goal of such a masochistic system is to be compromised and abused. Hopefully, each time a honeypot goes up in smoke, the researcher learns a new technique. For example, you can use a honeypot to find new rootkits, exploits, or backdoors before they become mainstream.

The term *honeynet*, originated by the Honeynet Project, means a network of honeypots. The configuration of the honeypots is specific to the network and services architecture of the environment you are defending. Further the honeynet is configured so that if a honeypot is compromised, the attacker cannot use that system to attack systems in your production network or external systems. Details of this configuration are described in Section 3.1. In some configurations, the system software of the honeypots is slightly modified (in the same manner as a rootkit works) to help monitor activity and

encrypted communication of attackers. The Honeynet Project defines such honeypots as "high-interaction" honeypots, meaning that attackers interact with a fully functional deception system exactly as they would with a real victim machine. On the other hand, various honeypot and deception daemons are "low interaction", since they only provide an illusion to an attacker. These systems only hold attacker attention for a short time. Examples of low-interaction honeypots include, Honeyd [2], Specter [3], and KFSensor [4]. Such honeypots have value as an early attack indicator collecting statistical data, and collecting malware, but do not yield in-depth information about the attackers.

Honeypots can further be separated into client and server honeypots. Client honeypots or "honeyclients" masquerade not as a legitimate server, but as a legitimate client system, such as a web surfer. A honeyclient might be compromised when trying to connect to a malicious or compromised server. Honeyclients are perfect for collecting web-deployed malware and web exploits.

What are some of the common sense prerequisites for running a honeynet? First, security basics should be covered. If your firewall crashes or your IDS misses attacks, you are clearly not yet ready for a honeypot deployment. Running a honeypot also requires advanced knowledge in computer security, network, platform, and application levels. Obviously, the compromised honeypot systems (whether client or server) should not be allowed to attack other systems.

The Honeynet Project defines guidelines on data control (capability required to control the network traffic flow in and out of the honeynet in order to contain the blackhat actions within the defined policy) and data capture (defines the information that should be captured on the honeypot systems for future analysis, data retention policies, and standardized data formats) for the deployed honeynet. They distill the above ideas and guidelines into a well-written document "Honeynet Definitions, Requirements, and Standards" [5].

The deployment of honeynets must be carefully planned and guidance sought to ensure that legal requirements are followed. Do you have the authority to monitor network traffic? What requirements exist for the data contained within the network packets? What must be done if your honeypots are actually attacked? If the attacker then engages in illegal activity using your honeypots, are you liable?

## 2 HONEYPOT RISK; LEGAL AND ETHICAL ISSUES

Running a honeypot incurs some risks. There are many laws, in virtually all nations that cover a person's expectation of privacy and the culpability incurred when your systems are involved in a cyber crime. Despite the risks, running the honeypot is an exciting and educational experience, which also contributes to a state of the art in information security.

What are some of the legal issues typically associated with running a honeypot?

Liability risk is the most common issue. Can you get sued if an attacker uses your honeynet to attack other, possible sensitive, systems? Given that there is very little case law, it is still too early to decide how significant this is. However, the more freedom is given to the attacker for the sake of creating a realistic "production-like" environment, the more risk of such liability is present.

The privacy and handling of the data captured is also a concern. The data packet may contain communications from unknowing bystanders or sensitive data (such as credit card or other personal information). Proper safeguards must be used to ensure that this type of

data is protected from disclosure. A bizarre issue that is sometimes brought up is whether the honeypots infringe upon the rights (such as the privacy right) of the hackers? While this sounds truly preposterous, the cases where burglars sued the victims who wounded them while defending their property are no less ridiculous—and they actually happened!

Richard Salgado, former senior counsel for the Department of Justice's computer crime unit, investigated some of the legal issues related to honeynet operation. He did confirm that "There are some legal issues here, and they are not necessarily trivial, and they're not necessarily easy." For example, in one of his media interviews [6], Mr Salgato mentioned a case where "an accused kidnapper who was using a cloned cell phone sued for the interception of the cell phone conversations and won."

The discussion of the legalities of deploying honeynets can be a very long one. The specific legal restrictions of the implementer's nation or province must be well understood. As the primary focus of this article is to describe emerging honeynet technologies, the reader should review the material available specifically covering legal issues on the Honeynet Project website [7] as well as other publications [8, 9].

## 3 HONEYNET TECHNOLOGIES

Honeynet technologies have matured over the last 9 years to a collection of sophisticated architectures that enable a relatively safe deployment of honeypots in the traditional high-interaction format to the new Global Distributed Honeynet (GDH) or as a honeyclient. The high-interaction honeypot is the most recognized honeynet technology. The latest version, generation III, brings the latest in ease of deployment, data control and capture, and analysis.

### 3.1 Generation III Honeynet

The generation III honeynet consists of an architecture where the honeypots reside behind a data control and capture device called a *honeywall*. The honeywall is a data link layer (layer 2) proxy. The software for the Honeynet Project honeywall is distributed on a bootable CD and is currently built using a CentOS kernel. This layer 2 proxy intercepts all inbound and outbound packets and uses a variety of mechanisms including rate limiting, selective dropping, and "bit-flipping," to mitigate the risk of a honeynet being used to exploit or scan yours or other's networks.

As shown in Figure 1, the honeywall is placed between the honeynet and the rest of the network. The organizations production systems (for example, e-mail or web services), shown as Production 1 and 2, are placed in front of the honeywall. The honeywall uses a combination of Snort [10] and Snort-inline to log and, where necessary, scrub incoming and outgoing packets. A detailed communication flow for a honeywall is shown in Figure 2.

In most cases, the packets coming into the honeynet through the honeywall are allowed to pass unchallenged to the honeypots. Only packet capture is done on the honeypot facing NIC. Outbound packets are subject to rate limiting (implemented in IP tables) and analysis by the Snort-inline process. The rate limiting of outbound activity is based on protocol and number of packets and can be specified in the scripts that start IP tables.

The task of data control and protecting the production and internet hosts from attacks originating from your honeypots is handled by the Snort-inline process. This process

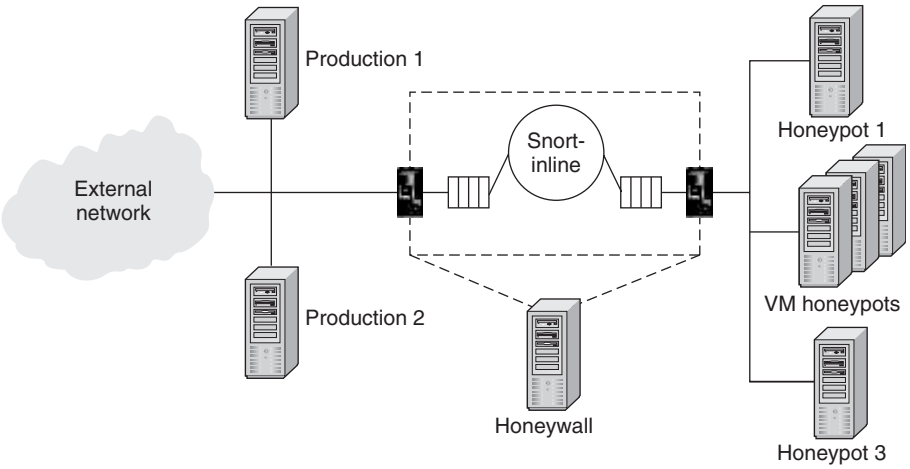



**FIGURE 1** Honeynet architecture.

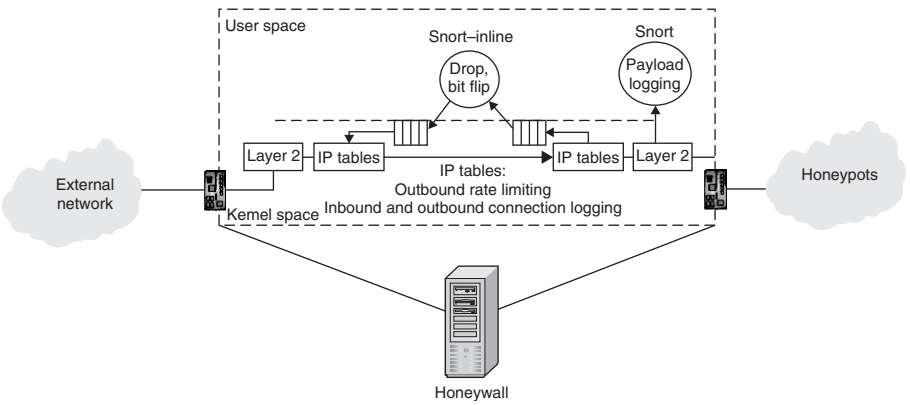



**FIGURE 2** Honeywall connection detail.

receives packets from the IP table queuing feature and matches the packets against a modified Snort rule set. If the packet matches a rule, either the packet could be allowed to continue (not likely) or be simply dropped, or Snort-inline could slightly modify the outbound packet's payload thereby rendering the exploit impotent when it reaches its intended target. Using the last approach, it is less likely that the attacker will become discouraged and move on.

Data Capture is accomplished as described above by the Snort process on the internal interface. Additionally a host-based technology called *Sebek* [11], logs all attacker activity on the honeypot and sends it to the honeywall for capture. The original version of Sebek was based on the Adore rootkit. The current version of Sebek replaces the read() function in the system call table in the 2.4 Linux kernel with a read() that is configured to copy all data that it sees into a packet and sends it to a server that collects Sebek packets as well as the normal processing handled by the read() function. Using this method not only captures all activity by the attacker on the honeypot, but also any data that was

once encrypted between the honeypot and the attacker's SSH server. Sebek also allows data to be sent covertly out of the honeypot without being observed by the attacker. This is accomplished by bypassing the TCP/IP stack (and the corresponding raw socket interface) and sending the Sebek data packets directly to the network device driver using the transport protocol UDP.

While Sebek provides a tremendous opportunity to record everything an attacker does, it is not invisible. Just as we are using attacker techniques by modifying the kernel functions for the purpose of monitoring, an attacker could determine the build of the OS on the honeynet and compare the various kernel functions known to be used by Sebek (most commonly through an MD5 checksum) and determine that he is on a honeypot. While this might be true and the attacker would probably leave, we have still gained a tremendous amount of information about the attacker—including the fact he is *not* a script kiddie. There are other detection mechanisms for honeypots and Sebek that can be found; the first one published is known as *NoSEBrEak* [12].

### 3.2 Global Distributed Honeynet (GDH)

Until last year, the deployment of honeynets was very geographically constrained. The GDH project is an attempt to develop, deploy, operate, and analyze data based on a worldwide network of honeynets. GDH was developed and led by David Watson of the UK Honeynet Project. The idea is to set up at different network locations an identical honeypot sensor system and store all collected information in a central database. Each GDH node consists of different components:

- virtual honeywall for data capture and data control;
- virtual Nepenthes honeypot for automated malware collection;
- one or more high-interaction honeypots running in a virtual machine.

All honeypot components are executed within virtual machines such that the whole honeynet can be deployed on one physical machine. Besides needing only a limited amount of hardware for running a GDH node, this approach has the additional advantage of the administration and system maintenance of the honeypot being easier. Setting up a new node only requires booting from a GDH CD-ROM, which automatically sets up the base platform on the system.

The whole honeynet is structured in a star-based network model with many GDH nodes and one central GDH data server. Each day all collected information, such as raw network data, IDS log files, and binary samples of malware, is transferred from each sensor node to the central data server. This enables a central correlation and analysis mechanism and all reports about malicious activities are generated based on this data.

The full GDH sensor system was operated for a period of 3 months between March and May 2007 with 11 GDH nodes. This GDH phase one was an attempt to test the whole infrastructure in a real-world environment. More than 730 million network packets were captured during this period, resulting in more than 122 GB of raw network data. In total, about 300,000 unique source IP addresses were observed at all honeypot sensors and this shows that such a global network of honeypots can collect quite a lot of information about network-based attacks. Furthermore, about 670,000 brute force attacks against SSH servers could be observed and 1680 malware samples were collected with the virtual Nepenthes honeypots.

Besides these automated attacks, several attacks by blackhats were also observed and lot of information about the typical tools, tactics, and motives of the attackers were collected. The major incidents observed include, for example:

- Polish cyber crime botnet used to attack other system with distributed denial-of-service (DDoS) attacks
- Brazilian group of blackhats who attacked web applications
- Romanian group of blackhats who are specialized in SSH brute force compromises.

The GDH phase one demonstrated the ability to successfully deploy and operate a globally distributed, standardized honeynet with identical sensor nodes at each location. The whole operation has also demonstrated that large scale distributed data collection and analysis are complex and time-consuming efforts, but the collected data compensates the effort since a lot of data about blackhat attacks were collected. In the future, the basic design of a GDH will be refined and adopted to new threats observed in the wild. The goal is to continuously operate a global network of both low- and high-interaction distributed honeynets based on current honeynet technology. Such a system can then be used to study and analyze current events and threats against systems connected to the Internet. The whole infrastructure can also be used as a test bed to study current honeynet technology in a real-world environment.

### 3.3 Honeyclients

One of the new research areas for Honeynet technologies is the honeyclient. Honeyclients, which are sometimes also called *client honeypots*, are the opposite of server honeypots. The main idea is to simulate the behavior of humans and then closely observe whether or not the honeypot is attacked. For example, a honeyclient can actively surf websites to search for malicious web servers that exploit the visitor's web browser and thus gather information of how attackers exploit clients. Another example are honeyclients that automatically process e-mails by clicking on attachments or following links from the e-mail and then closely observing if the honeypot is attacked. The current focus in the area of honeyclients is mostly based on the analysis of web client exploitation, since this attack vector is often used by blackhats in order to compromise a client.

Honeyclients also have another advantage: honeyclients initialize every analysis and thus control the maximum number of possible attacks. It is possible that a server honeypot may not be attacked for weeks or even months, or it is also possible that the honeypot is attacked occasionally by many attackers at the same time. In general, it is not possible to predict how frequently attacks will occur on a honeypot, and therefore the analyses get more complicated.

Honeyclients can also be classified as high-interaction or low-interaction honeyclients. High-interaction honeyclients are usually real, automated web browsers on real operating systems which interact with websites like real humans would do. They log as much data as possible during the attack and allow a fixed time period for an attack. Since they provide detailed information about the attack, high-interaction honeyclients are in general rather slow and not able to scan broad parts of the web. Low-interaction honeyclients, on the other hand, are often emulated web browsers, usually webcrawlers, which have no or only limited abilities for attackers to interact with. Low-interaction honeyclients often

make use of static signature or heuristics-based malware and attack detection tools and thus lack the detection of zero-day exploits and unimplemented attack types.

For all available honeyclients, a common general architecture or process chain, which consists of three serial steps depending on each other, can be observed. At first, a queue is filled with objects to analyze. Second, a honeyclient draws targets from the queued objects. Third, the collected information about the object is analyzed regarding their maliciousness. Several examples of different kinds of honeyclients and first results obtained with these tools are provided in the following paragraphs.

The HoneyMonkey project is a web browser (Internet Explorer) based high-interaction honeyclient developed at Microsoft Research in 2005 [13]. The HoneyMonkey architecture consists of a chain of virtual machines with different flavors of the Windows operating system in various patch levels. Starting with a fully unpatched system, the Monkey Controller initiates a so-called "monkey" program that browses previously scheduled websites. The monkey opens the website and waits for a predefined time. After the time-out, the virtual machine is checked for signs of a successful intrusion. If an attack is detected, the website is revisited with the next machine having a higher patch-level in the pipeline. During their research in May/June 2005, the researchers found that unpatched Windows XP SP1 systems could be exploited by 752 different URLs and a fully patched Windows XP SP2 had no exploits. They also claim to have detected a zero-day exploit in July 2005.

Capture [14] is a high-interaction honeyclient developed at the Victoria University of Wellington, New Zealand. Capture has two functional areas in its design, namely, a Capture client and a Capture server. The clients are hosting the actual high-interaction honeypotclient on a virtual machine, whereas the server coordinates and controls the clients. Capture concentrates on three aspects of high-interaction honeyclients:

- Capture is designed to be fast. State changes on the clients are triggering malicious actions in real time to the server.
- Capture is designed to be scalable. The central Capture server can control numerous clients across a network
- Capture supports different clients. The current version supports the three web browsers Firefox, Opera and Internet Explorer.

The server takes a URL as input and distributes it to one of the honeyclients in a round-robin fashion while controlling the clients in means of starting and stopping them. The clients report back any state changes: each client monitors its own state for changes on the file system, registry, and processes while browsing a website. An exclusion list for known, benign system changes are used to identify a nonmalicious state change; any other operation triggers a malicious classification of the web server and sends this information to the Capture server. Since the state of the client has been changed, the client resets its state to a clean state and retrieves new instructions from the server. If no state change was detected, the client requests new instructions from the server and continues its browsing without resetting. An interesting feature in development is to support nonbrowser clients, such as multimedia players and Microsoft Office applications.

### 3.4 Low-Interaction Malware Collectors

Several low-interaction honeypots were developed in the last few years to automatically capture binary copies of autonomous spreading malware. The basic idea of each of these

honeypots is to emulate an actual vulnerability. If a honeypot thus emulates a vulnerability and behaves like a vulnerable system, the malware will be tricked into thinking that the machine can actually be compromised and attacks the honeypot. By analyzing the received attack data and sending back packets that emulate an actual exploitation phase, the honeypot can collect enough information to acquire a binary copy of the malware.

One of the well-known honeypots from this area is Nepenthes [15]. Nepenthes is a low-interaction honeypot which aims at capturing malicious software artifacts that spread in an automated manner, like for example, worms or bots. The tool is based upon a very flexible and modularized design. The core—the actual daemon—handles the network interface and coordinates the actions of the other modules. The actual work is carried out by several modules, which register themselves in the Nepenthes core, and currently there are several different types of modules:

- Vulnerability modules emulate the vulnerable parts of network services. In total, this honeypot emulates more than 20 different vulnerabilities, corresponding to commonly exploited network services.
- Shellcode parsing modules analyze the payload received by one of the vulnerability modules. These modules analyze the received shellcode, an assembly language program, and extract information about the propagating malware from it.
- Fetch modules use the information extracted by the shellcode parsing modules to download the malware from a remote location.
- Submission modules take care of the downloaded malware, for example, by saving the binary to a hard disc, storing it in a database, or sending it to antivirus vendors.
- Logging modules log information about the emulation process and help in getting an overview of patterns in the collected data.

With the help of Nepenthes, it is possible to collect a large number of malware binaries, which spread autonomously. For example, during an 8-week measurement study between December 2006 and January 2007 a Nepenthes sensor running on about 16,000 IP addresses in parallel was able to collect more than 2500 unique malware samples [16]. The uniqueness is determined by the MD5 hash of each binary: two binaries that have the same MD5 hash are considered to be the same malware. Other operators of low-interaction malware collectors report a similar amount of malware collected with these honeypots [17].

## REFERENCES

1. The Honeynet Project, http://www.honeynet.org last accessed on 20 January 2008.
2. Honeyd, http://www.honeyd.org last accessed on 20 January 2008.
3. Specter, http://www.specter.com last accessed on 20 January 2008.
4. KFsensor, http://www.keyfocus.net/kfsensor/ last accessed on 20 January 2008.
5. Honeynet guideline, http://www.honeynet.org/alliance/requirements.html last accessed on 20 January 2008.
6. http://www.securityfocus.com/news/4004, last accessed on 20 January 2008.
7. http://honeynet.org/book/Chp8.pdf, last accessed 20 January 2008.
8. Spitzner, L. *Honeypots: Are They Illegal?* http://www.securityfocus.com/infocus/1703.

9. Spitzner, L. *The Value of Honeypots, Part Two: Honeypot Solutions and Legal Issues,* http://www.securityfocus.com/infocus/1498.
10. SNORT, last accessed on 20 Jan 2008 at www.snort.org.
11. Balas, E. *Know Your Enemy: Sebek*, http://www.honeynet.org.
12. Dornseif, M., Holz, T., and Klein, C. (2004). NoSEBrEaK—attacking honeynets. *IEEE Information Assurance Workshop*. West Point, NY, June 11, 2004.
13. Wang, Y., Beck, D., Jiang, X., Roussev, R., Verbowski, C., Chen, S., and King, S. (2006). Automated web patrol with strider honeymonkeys: Finding web sites that exploit browser vulnerabilities. *Proceedings of 13th Network and Distributed System Security Symposium (NDSS'06)*.
14. Seifert, C. *Capture High-Interaction Client Honeypot*, Internet:https://www.client-honeynet.org /capture.html.
15. Baecher, P., Koetter, M., Holz, T., Dornseif, M., and Freiling, F. (2006). The Nepenthes platform: an efficient approach to collect malware. In Zamboni, D., and Kruegel, C. Eds. *RAID 2006. LNCS*, Springer, Heidelberg, Vol. 4219, pp. 165–184.
16. Goebel, J., Holz, T., and Willems, C. (2007). Measurement and analysis of autonomous spreading malware in a university environment. *Proceedings of DIMVA*. pp. 109–128.
17. Watson, D. (2007). *Deploying and Operating a Global Distributed Honeynet*, PacSEC 2007, 29-30 November 2007, http://www.honeynet.org/speaking/PacSec07_David_Watson_Global_Distributed_Honeynet.pdf.

# DETECTION OF HIDDEN INFORMATION, COVERT CHANNELS, AND INFORMATION FLOWS

NEIL F. JOHNSON AND PHIL A. SALLEE
*Booz Allen Hamilton, McLean, Virginia*

## 1 INTRODUCTION

The oldest form of protecting information is to conceal its existence—hide it. Numerous methods for hiding information have been developed through the years, ranging from physical concealment of objects which are "hidden in plain sight" to high-tech methods for covert communications in digital media. Some examples of hiding information include hidden tattoos, covered writing, invisible inks, microdots, grille and null ciphers, code words, digital signatures, covert channels and spread-spectrum communications, to name but a few [1–5].

Steganography is used to conceal the existence of hidden messages within seemingly innocuous carriers. Common techniques in digital steganography usually camouflage the intended message within another object or media, referred to as either the *cover* or *carrier*. By far, the most common steganography tools embed information within image files. However, hidden information can be embedded within nearly any type of digital media or information flow. Research also extends beyond digital media such as DNA [6–8], chemical compounds [9], and circuit boards [10–12]. The focus in this article is on digital steganography: hiding in electronic files and media.

Covert channels, though not necessarily designed for communication, provide a means to communicate through the misuse of another mechanism, typically a shared resource. Such a mechanism can be exploited to convey information from a higher (more secure) environment to a lower (less secure) environment [13]. Human ingenuity and the availability of shared resources provide a variety of resources for communications. For example, convicted spy Robert Hanson would signal to his counterparts that information could be picked up by placing a chalk mark on a park sign: no mark, no information. In a digital world, signaling takes place in 0s and 1s.

Any organization or individual requiring secret communication will employ whatever technology is at their disposal to achieve the perceived secrecy. As a result, there is practically no limit to the variety of steganography implementations that may be developed. Inherent redundancy in many digital media formats provides ample storage space for hidden information. Examples of potential carriers include text [14–16], audio [17–19], image (the majority of steganography research), video [20–22], and hidden file systems [23, 24]. Research and techniques also exist for exploiting network packets and protocols to establish covert channels for communication in information flows [25–38]. Figure 1

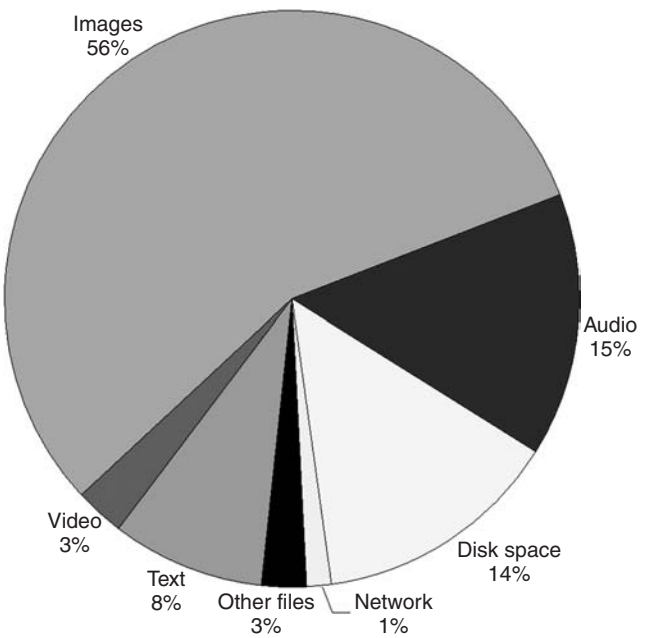



**FIGURE 1** Chart illustrates the observed distribution of media type supported as carriers for hidden information through steganography-related software development from 1992 through 2007.

illustrates the general distribution of media types used as carriers for hidden information by publicly available steganography software.

With the growth of the Internet, the introduction of new digital media formats, and increased concerns over privacy and security, tools and methods for protecting individuals and their information continue to expand. Each year reveals growing interest in steganography as new tools are developed, new research papers are published, and the number of academic research programs and conferences dedicated to the subject of hiding digital information continue to increase. Research efforts on the subject span the globe, and hundreds of new steganography-related software programs are released each year on the Internet. Some of these tools are academic in nature as student projects, others are malicious utilities designed to circumvent security mechanisms, and others are commercially marketed. Some steganographic products are marketed to the public with claims of protecting personal information or encourage the use of steganography where cryptography may be scrutinized.

## 2 SCIENTIFIC OVERVIEW

While many steganography tools and academic papers still focus primarily on the imperceptibility of the hidden information, the most current art in steganography takes into account the potential for statistical steganalysis. Likewise, research efforts in steganalysis quickly respond to new steganography methods and techniques as they are presented. Steganography and steganalysis research efforts form a cat and mouse game that continually advances the state of the art—similar to that of cryptography and cryptanalysis.

Both cryptography and steganography may be used to secure information. However, the two address differing requirements. Cryptography secures information by scrambling it, thus rendering a message unintelligible. Yet, cryptographic data may still be observed in state or in transmission. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message.

Steganographic security is obtained by keeping the very existence of the embedded message from being discovered—essentially camouflaging information so that any observable data or communication does not appear out of the ordinary. The steganography has failed if an observer can determine that a hidden message exists. Like cryptography, however, really good steganography is challenging to design. Detectable signatures can easily be introduced during the embedding process. Consequently, relying solely on "security by obscurity" (concealing the details of the encoding/decoding algorithm) is considered highly inadvisable. Strong steganography, like cryptography, relies on academic peer review to identify potential weaknesses.

### 2.1 Hiding Information

Assume a digital carrier, $C_{\{p,h\}}$. $C_p$ is the perceptual portion of the carrier and any manipulation to this portion will be readily noticeable. $C_h$ is the portion of the carrier that falls below the perceptual threshold and manipulation to this portion will not be readily noticed. If the construct of $a + b$ denotes a composition of $a$ and $b$, then the carrier may be represented as $C_{\{p,h\}} = C_p + C_h$. The size of $C_h$ depends upon the properties of the carrier, complexity of the data hiding process, and the need to balance constraints of imperceptibility versus robustness (survivability of the embedded data to some level of distortion).

If the operation $e \rightarrow f$ represents a process for hiding data $e$ into $f$, then a representation of the embedding process is $m \rightarrow C_h = C'_h$, where the message (m) is hidden in the imperceptible component $C_h$ of the carrier $C$. The resulting modified carrier is in the form of $C'_{\{p,h\}} = C_p + C'_h$ and is perceptually indistinguishable from $C_{\{p,h\}}$. The resulting $C'_{\{p,h\}}$ contains the hidden message and is referred to as the *steganogram* or *stego-media* (images may be referred to as stego-images, audio as stego-audio, etc.).

A common method for hiding data in digital carrier is to manipulate the bits that have the least impact to the observable carrier if changed. In 24-bit images such as bitmap (BMP) or audio files such as PCM WAVs, the *least significant bits* (LSBs) provide an instance of the $C_h$ portion in these carriers. Table 1 illustrates the impact of changing the LSBs of the color cells. Changing three bits of data has no visual impact. In fact, changing the lowest four bits of the color block also has little visible impact to this color. Therefore some bits can be used to embed any data we want without significantly changing the image [39]. Research examining image color reduction based on human vision limitations [40] inspired others to experiment with data hiding techniques and develop steganography tools [41].

A 24-bit image that is 1024 by 768 pixels in size yields 2,359,296 (1024*768*3) bytes of image data from the pixels. Changing only the LSBs permits storage capacity of 294,912 bytes. This article, with the figures and tables would fit with room to spare in such an image—(escaping detection is an altogether different matter). Many steganography tools that embed in BMP images or WAV audio files hide data using this type of technique.

The compressed formats GIF and JPEG are more prevalent on the Internet than BMP files. GIF images have only up to 256 colors and use only one byte to represent an image pixel. This byte is a pointer to a color table (palette) that is used to paint the colors of the image to the screen. Changing the LSB of one of these pointer bytes changes the position being pointed to in the color palette. If neighboring colors are distant, then changing the LSB will have visible difference on the resulting stego-image [39, 42]. To avoid this, steganography developers have investigated ways of arranging image palettes so that near colors are closer [43], or reconstructing new palettes [41] so that LSB manipulation is less visible.

**TABLE 1 Illustrates the Impact of Changing the LSBs of the Color Cells. Changing Three Bits of Data has No Visual Impact. In Fact, Changing the Lowest Four Bits of the Color Block Also has Little Visible Impact to This Color. We Can Clearly See that Some Bits Can be Used to Embed any Data We Want without Significantly Changing the Image**

| | Color | | Color Values |
|---|---|---|---|
| Original | | Red:<br>Blue:<br>Green: | 11000000 (192)<br>11000000 (192)<br>11000000 (192) |
| Only LSBs changed | | Red:<br>Blue:<br>Green: | 1100000*1* (193)<br>1100000*1* (193)<br>1100000*1* (193) |
| HALF the image data changed | | Red:<br>Blue:<br>Green: | 1100*1111* (207)<br>1100*1111* (207)<br>1100*1111* (207) |

Because JPEG images are highly compressed, the pixel data is not as readily available for manipulation. Therefore, manipulation to JPEG images occurs most commonly in the DCT compression coefficients. However, given a process to decode and re-encode coefficients within the JPEG format, the process of hiding data within DCT coefficients can be performed similarly to changing LSBs of pixels in a BMP file.

Early methods for steganography follow the simple LSB embedding technique described. As research progressed and methods for detecting hidden data became published, techniques for hiding became more elaborate. Researchers began combining cryptographic techniques—scrambling and diffusing the hidden messages across the cover media to make the message recovery more difficult if detected. Later techniques consider properties of the cover media and try to mimic the expected statistics of bits that are manipulated within the cover, or attempt modeling other characteristics of the cover media so embedded messages are more difficult to detect [44–52]. Each of these improvements in data hiding prompted related research for detection [42, 50, 53–65].

## 3 COUNTERMEASURES

Countermeasures to hidden communications fall into two general categories: detection and disruption. Steganalysis involves analyzing steganography algorithms, techniques, and their output to devise methods to detect the presence of the hidden data and, if possible, extract the data to reveal the hidden message. Alternatively, one may be more interested in protecting legitimate communications and disrupting potential covert communications by rendering the hidden data unusable.

### 3.1 Countermeasures: Detection

The basis of detecting hidden information involves making observations similar to forensic analysis of files and systems. These observations aid in determining whether applications were used to hide information, or if any media contains hidden data. Such observation includes the examining of media to look for indicators of manipulation by various steganographic tools, and may lead to the development of new *steganalysis* techniques. Two types of signatures emerge when investigating hidden information. *System Signatures* are residual artifacts on computer systems that result from the installation, execution, or removal of tools that hide information [39]. *Steganographic Signatures* are detectable distortions that occur in the carrier media when the carrier is manipulated to conceal the hidden data [39, 42].

The identification of steganographic signatures generally requires extensive experimentation with various products that provide information hiding capabilities. Stego-media is compared with the original carrier media to determine what properties or characteristics change when data is hidden. Such experimentation is also useful in determining the capabilities and limitations of data hiding methods (i.e. the breaking points), as well as discovering signatures that may be leveraged for more rapid detection. Distortions that take the form of repeatable patterns and provide reliable indication that a steganography tool has been used are often referred to as *hard signatures*. The Steganalysis Research Center (SARC) produces forensic and steganalysis tools that look for system signatures and hard signatures in stego-media [66].

Hard signatures do not provide a complete solution to the steganalysis problem, however. Developing a database of signatures requires time, and the growth in the number of steganography applications exceeds the current discovery of steganographic signatures provided in forensic and steganalysis tools. Additionally, not all hiding techniques produce such patterns. In some cases, distortions caused by a steganographic method may simply violate the expected structure of the carrier media to a degree that allows for some uncertainty as to the cause of the distortion. Here, steganalysists must rely on *soft signatures*, based on statistical anomalies in the stego-media to identify potential data hiding.

To address the rapid growth in steganography tools and techniques, other detection methods need to be employed. Research is progressing in the area of *blind detection*, which does not rely on specific knowledge of a steganography technique, and holds the promise of detecting even previously unknown steganography applications. Most academic research in steganalysis is currently pursuing approaches for statistical and blind detection [50, 53–58, 61–65]. Wetstone Technologies produces a steganalysis suite for investigations to perform detection of system signatures (Gargoyle) and assist investigators in discovering stego-media based on statistical analysis [67]. Other researchers have also made attempts at producing steganography detection techniques with mixed results [64].

Both hard and soft signature approaches to detecting stego-media have merit. However, the volume of emerging steganography methods and tools is a hindrance in producing hard signatures for them all. Blind and Statistical detection methods are generally limited in accuracy, due to the intrinsic variability and unpredictability of media content as well as variations due to lossy compression, transcoding, and processing. Even relatively small false alarm rates can overwhelm analysts working with large data sets. Combining features and signatures may help investigators to make better determinations and reduce false alarms.

### 3.2 Countermeasures: Disruption

In some cases, preventing data leakage may be of greater importance than detecting the presence of hidden data. In this case an *active warden* may manipulate suspect media or traffic in an attempt to render any embedded data unusable. Revisiting the steganography system of $C'_{\{p,h\}} = C_p + C'_h$, the warden may also manipulate $C'_h$ to change, overwrite, or remove any embedded data without noticeable distortion to $C'_{\{p,h\}}$. From the warden's view point, as long as the portion or simulation of $C_h$ is below the perceptual level, then a $C_h''$ exists that is of the warden's choosing and prevents the hidden information from being passed [3]. Researchers have investigated using such approaches in multimedia (images, audio, video) [42, 61, 69–73] and as countermeasures to hiding in network traffic and covert channels [31, 38, 74–80].

Some disruption attacks can be defeated. The Stirmark tool was developed to test the robustness of watermarking algorithms by applying various distortions to images [71]. In [81], however, authors described a generalized countermeasure against the distortion attacks executed by Stirmark, demonstrating the ability to recover previously unreadable watermarks from distorted images.

## 4 RESEARCH AND DEVELOPMENT TRENDS

### 4.1 Research Trends

Application development and academic research in digital steganography and steganalysis started gaining momentum during the 1990s and has steadily increased in depth and breadth since. The first academic conference on the subject, the International Information Hiding Workshop, was held in Cambridge, UK, in 1996 [82]. Conferences in information hiding share venues and ideas with research in related areas including anonymity and privacy, cryptology, computer security and forensics. Continued research in information hiding takes inspiration from many other fields as well, including signal detection theory, information theory, signal processing, computer vision, and machine learning. Although having different end goals, digital watermarking is closely related to steganography as a type of information hiding and the two have developed alongside one another with many shared ideas and techniques. Research in both areas has focused on expanding information hiding concepts to address many different types of digital media and signals, and also in the sophistication of the techniques employed and their ability to conceal and reveal information using statistical methods.

The earliest academic research in digital steganography focused primarily on hiding from view, that is, a human observer, in a variety of digital formats. Common techniques of this era included modifying LSBs of a carrier signal, or hiding in specific bit-planes of binary values [39, 83]. Images provided an attractive carrier, with a relatively large capacity for hiding information, and BMPs were an easy target for manipulation due to their simple format. Later, academic research in image steganography shifted to hiding in DCT coefficients in the more popular JPEG format [47, 51, 52], and eventually also in the wavelet transform domain [84]. Hiding in text gained early interest before images were prevalent in e-mail attachments, and while the Internet was still in its infancy. Text embedding techniques included whitespace manipulation, such as line and word spacing [16], and synonym replacement [14, 15]. Other media formats were also exploited, including audio [17, 19] and internet protocols [28, 30, 35].

Early approaches to digital steganalysis included visualization techniques, and histogram tests such as the Chi-squared attack, which demonstrated weaknesses in LSB steganography [42, 65]. In response, steganography algorithms were designed to avoid detection by these specific attacks, and the focus shifted toward resisting statistical detection rather than avoiding human observation. For example, LSB methods were replaced by $\pm 1$ additive embedding [85], and in DCT coefficients by reduction in magnitude [51] and histogram preservation [47]. As steganography improved in sophistication, research in steganalysis quickly responded, focusing primarily on specific attacks to counter known steganography algorithms [59, 60].

Theoretical research has focused on the possibility of provably secure steganography. Taking inspiration from cryptology and information theory, Cachin introduced the concept of epsilon-security for steganography based on the similarity between the true cover and embedded cover distributions in terms of information theoretic divergence measures [86]. A link was recognized between compression and steganography that later served as inspiration for model-based techniques [49, 50, 87]. Some work has also considered the maximum capacity of secure steganographic embedding [49, 88]. Drawing from the

computer vision and natural scenes communities, other research has looked at statistical differences of image steganography as compared to the statistics of natural scenes [89], with obvious implications to steganalysis.

Out of these early starts in digital steganography, some recent trends emerged. Steganography methods began to focus less on avoiding specific attacks and more on preserving the statistical properties of the cover media, and reducing the number of required changes to the media. For example, matrix-embedding techniques provide a means to reduce the number of changes required to hide information, by trading off capacity for a given sized cover. Also, model-based techniques use statistical models of the cover media to preserve the modeled cover statistics more accurately and efficiently [49, 50, 90, 91]. Some more recent steganography techniques dynamically adapt to the characteristics of the cover media. For example, these techniques may identify locations with higher variability that are considered more suitable for embedding data. A significant advancement in this regard is known as informed embedding, which uses side information about the media that is not preserved or passed to the receiver in order to improve the quality and undetectability of the resulting stego-object [44, 92].

Similarly, steganalysis methods began to focus more on modeling the properties of cover media, as well as the results of steganographic embedding. Most notable in this regard is the advancement of general, or universal, steganalysis methods, which use machine learning and classification techniques such as Support Vector Machines (SVMs) to detect steganography based on exemplars rather than specific knowledge of the algorithms being detected. Taking inspiration from computer vision, SVMs were trained using image wavelet statistics [55–57], and later, calibrated features computed in the DCT domain [61, 62]. Future work in this area continues to improve the features that are useful for detecting steganography and explore classification techniques.

### 4.2 Development Trends

Relatively few developers of steganography-related tools appear to incorporate advances published in related academic research. Those that do, introduce methods in an attempt to reduce the detectability of the hidden content. Thus, as research and development in the academic arena continues, the sophistication of available steganography software continues to improve. For example, many applications now incorporate cryptographic methods to encrypt data prior to embedding, or select pseudo-random locations within the digital carriers to hide their data.

Between 1992 and 2004, interest in steganography exploded at a near exponential rate. The most significant jump in software releases that claim to provide steganographic capabilities appear from 2001 to 2002. This growth may be due, in part, to the security and threat frenzy following the 9/11 attacks in 2001. Shortly after the attacks, some authors of steganography tools abandoned their wares while others were driven by curiosity, growing markets, and the desire for privacy protection in a seemingly ever pervasive world. Figure 2 illustrates the trend of steganography-related tools released each year from 1992 through 2007 [93]. Due to the increasing volume of tools being released each year and the fact that some products are released for time, it can be difficult to accurately depict the overall size of this market. As of the writing of this text, over 3000 tools are identified by the authors representing over 1500 software titles. Keeping track of steganography-related tools can be complicated when multiple authors select the same name for their application. For example, over 40 software titles from more

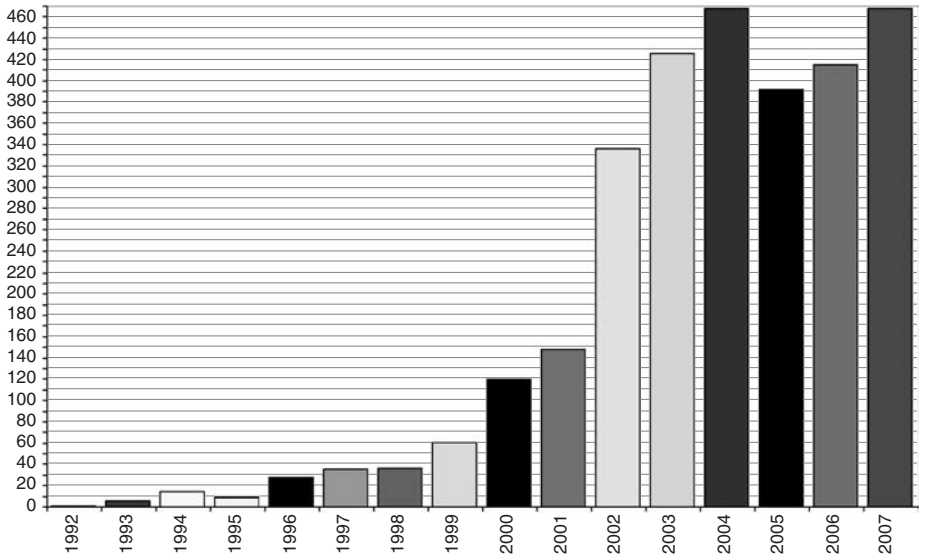



**FIGURE 2** Chart illustrates the overall observed trend of steganography software development from 1992 through 2007 [93].

than 30 authors are variants of the words "steganography" or "steganographie". Other popular steganography tool names include variants of steg, stego, stegano, camouflage, hide, invisible, and stealth.

Steganography research and application development takes place around the globe. Observing research publications and software releases, the top 10 countries with active steganography-related research are (in alpha order) Canada, China, France, Germany, India, Italy, Japan, Russia, United Kingdom, and the United States. A number of steganography applications are multinational, meaning that collaborative software development occurs between individuals from multiple countries. International academic researchers and hacker organizations typically pool talent from multiple countries.

## 5 CRITICAL NEEDS ANALYSIS

Information hiding techniques pose a threat to national security and law enforcement through the potential loss of secrets or intellectual property and as possible distribution and communication channels for coordinating illicit activities. An investigator or analyst must find ways to analyze information that cannot be readily apparent and must seek subtleties that may suggest hidden information. It is not sufficient for investigators to have tools and techniques for handling password-protected files, but must also be involved in locating and recovering data hidden within seemingly innocuous carriers [69, 70].

Traditional perimeter security mechanisms such as firewalls, intrusion detection systems, and virus scanners are ill-equipped to handle media that may contain hidden information. Some tools available to forensic investigators/analysts are useful at examining slack space on storage devices or matching hash sets for known applications. However, many common forensic tools do not specifically detect the presence of steganographic

content in potential carriers. Hash sets are available as part of the National Software Reference Library (NSRL) Project. This project collects and compiles digital signatures of software to produce a reference data set (RDS). The RDS includes signatures of applications including steganography tools and hacking scripts [94].

## 6 RESEARCH DIRECTIONS

The ease in use and abundant availability of steganography tools has authorities concerned about the trafficking of illicit material, or coordination of terrorists' plots via web page images, audio, video, and other transmissions over the Internet. Methods of message detection and understanding the thresholds of current technology are continually under investigation. The success of steganography is dependent upon selecting the proper mechanisms. However, a stego-medium that seems innocent may actually broadcast the existence of embedded information upon further investigation. As long as the need exists for covert communications, development of information hiding techniques will continue. Systems to recover seemingly destroyed information and steganalysis techniques will be useful to authorities in computer forensics, digital traffic analysis, cyber-warfare, and counterterrorism.

Steganographic implementations, through the development of open source or commercial products, are generally behind the ideas and methods published in the research community. Many tools continue to use only basic methods at attempting to hide information. However, research continues to improve and hundreds of applications are released each year. The sheer volume of emerging steganography methods and tools requires innovative and accurate approaches to steganalysis. Being able to detect unforeseen techniques requires continued research. Research efforts continue to push the technological envelope, and staying abreast of such research is increasingly important. Technical publications and conferences provide the best window to the evolution of information hiding techniques from the open source and around the world. For a list of relevant proceedings from the International Information Hiding Workshop see the Further Reading List.

## REFERENCES

1. Kahn, D. (1967, 1996). *The Codebreakers*, The Macmillan Company, New York.
2. Wrixon, F. B. (1998). *Codes, Ciphers and Other Cryptic and Clandestine Communication*, Black Dog & Leventhal Publishers, New York.
3. Johnson, N. F., Duric, Z., and Jajodia, S. (2000). *Information Hiding: Steganography and Watermarking—Attacks, and Countermeasures*, Kluwer Academic Press, Norwell, MA.
4. Katzenbeisser, S., and Petitcolas, F. A. P., Eds. (2000). *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House Books, Norwood, MA.
5. Bender, W., Gruhl, D., Morimoto, N., Lu, A. (1996). Techniques for data hiding. *IBM Syst. J*. **35**(3&4), 313–336. MIT Media Lab.
6. Clelland C. T., Risca, V., and Bancroft, C. (1999). Hiding messages in DNA microdots. *Nature* **399**(6736), 533–534.

7. Saeb, M., El-Abd, E., and El-Zanaty, M. E. (2007). On covert data communication channels employing DNA recombinant and mutagenesis-based steganographic techniques. *WSEAS Trans. Comput. Res*. **2**(1), 50–56. 1991-8755.
8. Shimanovsky, B., Feng, J., and Potkonjak, M. (2003). Hiding data in DNA. In *Proceedings of the 2003 Information Hiding 5th International Workshop*, *Springer Lecture Notes In Computer Science*, Vol. 2578, Springer-Verlag, Berlin/Heidelberg, pp. 373–386.
9. Eggers, J. J., Ihlenfeldt, W., and Girod, B. (2001). Digital watermarking of chemical structure sets. In *Proceedings of the Information Hiding 4th International Workshop*, *Springer Lecture Notes In Computer Science*, Vol. 2137, Springer-Verlag, Berlin/Heidelberg, pp. 200–214.
10. Lach, J., Mangione-Smith, W. H., and Potkonjak, M. (1998). Fingerprinting digital circuits on programmable hardware. In *Proceedings of the Information Hiding Second International Workshop*, *Springer Lecture Notes In Computer Science*, Vol. 1525, Springer-Verlag, Berlin/Heidelberg, pp. 16–31.
11. Lach, J., Mangione-Smith, W. H., and Potkonjak, M. (1999). Enhanced intellectual property protection for digital circuits on programmable hardware, *Proceedings of the Information Hiding: Third International Workshop*, Vol. 1768, Springer-Verlag, Berlin/Heidelberg, pp. 286–301.
12. Jain, A. K., Yuan, L., Pari, P. R., and Qu, G. (2003). Zero overhead watermarking technique for FPGA designs. *Proceedings of the 13th ACM Great Lakes Symposium on VLSI*. 28–29 April, 2003, pp. 147–152.
13. Lampson, B. (1973). A note on the confinement problem. *Commun. ACM* **16**(10), 613–615.
14. Chapman, M., Davida, G. I., and Rennhard, M. (2001). A practical and effective approach to large-scale automated linguistic steganography. In *Proceedings of the 4th International Conference on Information Security*, *Springer Lecture Notes In Computer Science*, Vol. 2200, Springer-Verlag, Berlin/Heidelberg, pp. 156–165.
15. Bolshakov, I. A. (2005). A method of linguistic steganography based on collocationally-verified synonymy. In *Proceedings of the Information Hiding 6th International Workshop*, *Springer Lecture Notes in Computer Science*, Vol. 3200, Springer-Verlag, Berlin/Heidelberg, pp. 180–191.
16. Low, S. H., Maxemchuk, N. F., Brassil, J. T., and O'Gorman, L. (1995). Document marking and identification using both line and wordshifting, *Proceeding of the Fourteenth Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 2, Boston, Massachusetts, pp. 853–860. DOI: 10.1109/INFCOM.1995.515956.
17. Petitcolas, F. A. P. (1998). MP3Stego software. http://www.petitcolas.net/fabien/steganography/mp3stego/.
18. Franz, E., Jerichow, A., Möller, S., Pfitzmann, A., and Stierand, I. (1996). Computer based steganography: how it works and why therefore any restrictions on cryptography are nonsense, at best. In *Proceedings of the Information Hiding First International Workshop*, *Springer-Verlag Lecture Notes in Computer Science*, Vol. 1174, Springer-Verlag, Berlin/Heidelberg, pp. 7–21.
19. Gruhl, D., Bender, W., and Lu, A. (1996). Echo hiding. In *Proceedings of the Information Hiding First International Workshop*, *Springer-Verlag Lecture Notes in Computer Science*, Vol. 1174, Springer-Verlag, Berlin/Heidelberg, pp. 295–315.
20. Westfeld, A., and Wolf, G. (1998). Steganography in a video conferencing system. In *Proceedings of the Information Hiding Second International Workshop, Springer-Verlag Lecture Notes In Computer Science*, Vol. 1525, Springer-Verlag, Berlin/Heidelberg, pp. 32–47.
21. Robie, D. L., and Mersereau, R. M. (2002). Video error correction using steganography. *EURASIP J. Appl. Signal Process*. **2002**(1), 164–173.

22. Xu, C., Ping, X., and Zhang, T. (2006). Steganography in compressed video stream. *Proc. IEEE Comput. Soc. First Int. Conf. Innovative Comput. Inf. Control* **2006**(1), 269–272.

23. Anderson, R. J., Needham, R., and Shamir, A. (1998). The steganographic file system, *Proceedings of the Second International Workshop*, Vol. 1525, Springer-Verlag, Berlin/Heidelberg, pp. 73–82.

24. McDonald, A. D., and Kuhn, M. G. (1999). StegFS: a steganographic file system for Linux, *Proceeding of the Information Hiding: Third International Workshop*, Vol. 1768, Springer-Verlag, Berlin/Heidelberg, pp. 454–468.

25. daemon9 (1997). LOKI2: the implementation. *Phrack Mag*. **7**(51) September 01, 1997, article 06 of 17.

26. Dittmann, J., Vogel, T., and Hillert, R. (2006). Design and evaluation of steganography for voice-over-IP, *Proceedings of the IEEE Circuits and Systems Society (ISCAS)*, Kos, Greece.

27. Giffin, J., Greenstadt, R., Litwack, P., and Tibbetts, R. (2002). Covert messaging through TCP timestamps, *Proceedings of the Privacy Enhancing Technologies Workshop (PET)*, Vol. 2482, Springer-Verlag, Berlin/Heidelberg, pp. 194–208.

28. Handel, T. G., Stanford, M. T. III (1996). Hiding Data in the OSI Network Model. *Proceedings of the Information Hiding: First International Workshop*. Vol. 1174, Springer-Verlag, Berlin/Heidelberg, pp. 23–38.

29. Jones, E., Robert, J., and Moigne, O. L. E. (2005). *IP Time to Live (TTL) Field Used as a Covert Channel 2005*. European Patent No. EP1517517, CIT ALCATEL (FR).

30. Llamas, D., Allison, C., and Miller, A. (2005). Covert channels in internet protocols: a survey, *Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, (PGNET)*.

31. Llamas, D., Miller, A., and Allison, C. (2005). An evaluation framework for the analysis of covert channels in the TCP/IP protocol suite. In *Proceedings of the 4th European Conference on Information Warfare and Security (ECIW 2005)*, University of Glamorgan, Pontypridd, Vol. 4, pp. 205–214.

32. Lucena, N. B., Lewandowski, G., and Chapin, S. J. (2005). Covert channels in IPv6. *Proceedings of the Privacy Enhancing Technologies (PET)*, Vol. 3856, Springer-Verlag, Berlin/Heidelberg, pp. 147–166.

33. Mazurczyk, W., and Kotulski, Z. (2006). Covert channel for improving VoIP security. *Proceedings of the Multiconference on Advanced Computer Systems (ACS)*, Vol. 2006, Miedzyzdroje, Poland, pp. 311–320.

34. Moskowitz, I. S., Newman, R. E., Crepeau, D. P., and Miller, A. R. (2003). Covert channels and anonymizing networks. *Proceedings of the Workshop on Privacy in the Electronic Society (WPES)*, Washington, DC.

35. Rowland, C. H. (1997). Covert channels in the TCP/IP protocol suite (Covert-TCP). *First Monday*, *Peer Reviewed Journal on the Internet*, July 1997.

36. Simple Nomad (2003). Covering your tracks: NCrypt and NCovert. *Proceedings of the Black Hat*, USA.

37. Zander, S., Armitage G., and Branch, P. (2006). Covert channels in the IP time to live field. *Proceedings of the Australian Telecommunication Networks and Applications Conference (ATNAC)*, Melbourne, Australia.

38. Zander, S., Armitage, G., and Branch, P. (2007). A survey of covert channels and countermeasures in computer network protocols. *IEEE Commun. Surv. Tutorials* **9**(3), 44–57.

39. Johnson, N. F., and Jajodia, S. (1998). Exploring steganography: seeing the unseen. *IEEE Comput*. **31**(2), 26–34.

40. Heckbert, P. (1982). Color image quantization for frame buffer display. *Proceedings of the 9th ACM Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH)*. Vol. 1982, Boston, Massachusetts, pp. 297–307.
41. Brown, A. (1998). *S-Tools: Steganography Tools for Windows*.
42. Johnson, N. F., and Jajodia, S. (1998). Steganalysis of images created using current steganography software. *Proceedings of the Information Hiding: Second International Workshop*, Vol. 1525, Springer-Verlag, Berlin/Heidelberg, pp. 32–47.
43. Machado, R. (1996). *Stego and EzStego for Hiding in PICT and GIF Images*.
44. Fridrich, J., Goljan, M., and Soukal, D. (2004). Perturbed quantization steganography with wet paper codes. *Proceedings of the Workshop on Multimedia and Security (MM&Sec)*, pp. 4–15.
45. Fridrich, J., Pevny, T., and Kodovsky, J. (2007). Statistically undetectable JPEG steganography: dead ends, challenges, and opportunities. *Proceedings of the Workshop on Multimedia and Security (MM&Sec)*. Vol. 9, Dallas, TX, pp. 3–14.
46. Gul, G., Dirik, A. E., and Avcibas, S. (2007). Steganalytic features for JPEG compression-based perturbed quantization. *IEEE Signal Process. Lett*. **14**(3), 205–208.
47. Provos, N. (2001). Defending against statistical steganalysis. *Proceedings of the USENIX Security Symposium*. Vol. 10, pp. 323–335.
48. Provos, N. (1998). *OutGuess—Universal Steganography*, http://www.outguess.org/, August 1998.
49. Sallee, P. (2004). Model-based steganography. In *Proceedings of the International Workshop on Digital Watermarking*, *Springer Lecture Notes in Computer Science*, Springer-Verlag, Berlin/Heidelberg, pp. 154–167.
50. Sallee, P. (2005). Model-based methods for steganography and steganalysis. *Int. J. Image Graph. Spec. Issue: Image Data Hiding* **3304**, 167–189.
51. Westfeld, A. (2001). F5-A steganographic algorithm. *Proceedings of the Information Hiding: 4th International Workshop, Proceedings*. Vol. 2135, Springer-Verlag, Berlin/Heidelberg, pp. 289–302.
52. Wong, K., Qi, X., and Tanaka, T. (2007). A DCT-based mod4 steganographic method. *ACM Signal Process*. **87**(6), 1251–1263.
53. Avcibas, I., Memon, N., and Sankur, B. (2003). Steganalysis using image quality metrics. *IEEE Trans. Image Process*. **12**(2), 221–229.
54. Dumitrescu, S., and Wu, X. (2005). LSB steganalysis based on high-order statistics. *Proceedings of the International Multimedia Conference Workshop on Multimedia and Security*. Vol. 7, New York, NY, pp. 25–32.
55. Farid, H. (2002). Detecting hidden messages using higher-order statistical models. *Proceedings of the International Conference on Image Processing*. Vol. 2, Rochester, NY, pp. 905–908.
56. Farid, H., and Lyu, S. (2003). Higher-order wavelet statistics and their application to digital forensics. *Proceedings of the IEEE Workshop on Statistical Analysis in Computer Vision, Conference on Computer Vision and Pattern Recognition Workshop*. Vol. 8, Madison, Wisconsin, pp. 94.
57. Lyu, S., and Farid, H. (2003). Detecting hidden messages using higher-order statistics and support vector machines. *Fifth Proceedings of the Information Hiding: International Workshop*. Vol. 2578, Springer-Verlag, Berlin/Heidelberg, pp. 340–354.
58. Lyu, S., and Farid, H. (2006). Steganalysis using higher-order image statistics. *IEEE Trans. Inf. Forensics Secur*. **1**(1), 111–119.
59. Fridrich, J., Goljan, M., and Hogea, D. (2002). Attacking the outguess. *Proceedings of the ACM Workshop on Multimedia and Security, Juan-les-Pins*, France, December 6, 2002.
60. Fridrich, J., Goljan, M., and Hogea, D. (2003). Steganalysis of JPEG images, breaking the F5 algorithm. In *Proceedings of the Information Hiding 5th International Workshop*,

*Springer-Verlag, Lecture Notes in Computer Science*, Vol. 2578, Springer-Verlag, Berlin/Heidelberg, pp. 310–323.

61. Fridrich, J. (2004). Feature-based steganalysis for JPEG and its implications for future design of steganographic schemes. In *Proceedings of the Information Hiding: 6th International Workshop*, *Springer Lecture Notes in Computer Science*, Vol. 3200, Springer-Verlag, Berlin/Heidelberg, pp. 67–81.
62. Fridrich, J., and Pevny, T. (2006). Multiclass blind steganalysis for JPEG images. In *Proceedings of the SPIE, Electronic Imaging, Photonics West, Security, Steganography, and Watermarking of Multimedia Contents VIII*. Vol. 6072, pp. 257–269.
63. Ji, R., Yao, H., Liu, S., Wang, L., and Sun, J. (2006). A new steganalysis method for adaptive spread spectrum steganography. In *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia*, (December 18–20, 2006). IIH-MSP. IEEE Computer Society, pp. 365–368.
64. Provos, N., and Honeyman, P. (2002). Detecting steganographic content on the internet. In *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS'02)*, Also CITI Technical Report 01-11, 2001. University of Michigan.
65. Westfeld, A., and Pfitzmann, A. (2000). Attacks on steganographic systems. *Proceedings of the Information Hiding: Third International Workshop*. Vol. 1768, Springer-Verlag, Berlin/Heidelberg, pp. 61–76.
66. Steganalysis Reseach Center (SARC)/Backbone Security *Developer of StegAlyzerAS and StegAlyzerSS for Detecting Steganography Applications and Steganographic Data Embedded within Various Carrier Files by Numerous Steganography Applications*.
67. Wetstone Technologies *Developer of Gargoyle and StegWatch for Digital Forensics and Steganography Detection*.
68. Ker, A. D. (2008). A fusion of maximum likelihood and structural steganalysis. *Proceedings of the Information Hiding: 9th International Workshop, IH 2007*. Saint Malo, Vol. 4567, pp. 204–219.
69. Johnson, N. F., Giordano, J., and Jajodia, S. (1999). *Steganography and Computer Forensics: The Investigation of Hidden Information*, Technical Report, CSIS-TR-99-10-NFJ, George Mason University, Center for Secure Information Systems, October 1999.
70. Johnson, N. F., and Kong, E. G. (2002). *Investigating Hidden Information: Steganography and Computer Forensics*, American Academy of Forensic Sciences (AAFS), Atlanta, GA, February 11–16.
71. Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G. (1998). Attacks on copyright marking systems. *Proceedings of the Information Hiding Second International Workshop*. Vol. 1525, Springer-Verlag, Berlin/Heidelberg, pp. 219–239.
72. Petitcolas, F. A. P. (2000). Watermarking schemes evaluation. *IEEE Signal Process*. **17**(5), 58–64.
73. Francia III, G. A., and Gomez, T. S. (2006). Steganography obliterator: an attack on the least significant bits. In *Proceedings of the 3rd Annual Conference on information Security Curriculum Development (InfoSecCD'06)*, ACM, Kennesaw, Georgia, pp. 85–91. DOI: 10.1145/1231047.1231066.
74. Borders, K., and Prakash, A. (2004). Web tap: detecting covert web traffic. *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS)*. Vol. 11, pp. 110–120.
75. Cabuk, S., Brodley, C. E., and Shields, C. (2004). IP covert timing channels: design and detection. *Proceedings of the 11th ACM conference on Computer and Communications Security (CCS)*. Vol. 11, Washington, DC, pp. 178–187.

76. Department of Defense National Computing Security Center (NCSC) (1993). *A Guide to Understanding Covert Channel Analysis of Trusted Systems*, NCSC-TG-030.

77. Fisk, G., Fisk, M., Papadopoulos, P., and Neil, J. (2003). Eliminating steganography in internet traffic with active wardens. In *Proceedings of the Information Hiding 5th International Workshop*, *Springer Lecture Notes in Computer Science*, Vol. 2578, Springer-Verlag, Berlin/Heidelberg, pp. 340–354.

78. Gianvecchio, S., and Wang, H. (2007). Detecting covert timing channels: an entropy-based approach. *Proceedings of the 14th ACM Conference on Computer and Communication Security (CCS)*. Vol. 14, Alexandria, VA, pp. 307–316.

79. Kemmerer, R. (1983). Shared resource matrix methodology: an approach to identifying storage and timing channels. *ACM Trans. Comput. Syst. (TOCS)* **1**(3), 256–277.

80. Sohn, T., Seo, J., and Moon, J. (2003). A study on the covert channel detection of TCP/IP header using support vector machine. *Proceedings of the 5th International Conference on Information and Communications Security*. Vol. 2578, Springer-Verlag, Berlin/Heidelberg, pp. 313–324.

81. Johnson, N. F., Duric, Z., and Jajodia, S. (2000). Recovery of watermarks from distorted images. In *Proceedings of the Third International Workshop on Information Hiding (September 29–October 01, 1999)*, *Lecture Notes In Computer Science*, Vol. 1768, Springer-Verlag, Berlin/Heidelberg, pp. 318–332.

82. Anderson, R. J., ed. (1996). *Information hiding: first international workshop, Cambridge, UK*. *Lecture Notes in Computer Science*, Vol. 1174. Springer-Verlag, Berlin/Heidelberg. DOI: 10.1007/3-540-61996-8.

83. Kawaguchi, E., and Eason, R. O. (1998). Principle and applications of BPCS steganography. *Proceedings of the SPIE International Symposium on Voice, Video, and Data Communications*. Vol. 3528, Boston, Massachusetts, pp. 464–473. DOI: 10.1117/12.337436.

84. Su, P., and Kuo, C. J. (2003). Steganography in JPEG2000 compressed images. *IEEE Trans. Comput. Electron*. **49**(4), 824–832.

85. Sharp, T. (2001). An implementation of key-based digital signal steganography. In *Proceedings of the Information Hiding 4th Internationl Workshop*, *Springer Lecture Notes in Computer Science*, Vol. 2137, Springer-Verlag, Berlin/Heidelberg, pp. 13–26.

86. Cachin, C. (1998). An information-theoretic model for steganography. In *Proceedings of the Information Hiding: 2nd International Workshop*, *Springer Lecture Notes in Computer Science*, Vol. 1525, Springer-Verlag, Berlin/Heidelberg, pp. 306–318.

87. Anderson, R. J., and Petitcolas, F. A. P. (1998). On the limits of steganography. *IEEE J. Sel. Areas Commun.* **16**, 474–481.

88. Cox, I. J., Kalker, T., Pakura, G., and Scheel, M. (2005). Information transmission and steganography. In *Proceedings of the International Workshop on Digital Watermarking*, *Springer Lecture Notes in Computer Science*, Vol. 3710, Springer-Verlag, Berlin/Heidelberg, pp. 15–29.

89. Martín, A., Sapiro, G., and Seroussi, G. (2005). Is image steganography natural? *IEEE Trans. Image Process*. **14**(12), 2040–2050.

90. Eggers, J. J., Bäuml, R., and Girod, B. (2002). A communications approach to image steganography. *Proceedings of the SPIE Electronic Imaging Security and Watermarking of Multimedia Contents IV*. Vol. 4675, San Jose, CA, pp. 26–37.

91. Fridrich, J., and Goljan, M. (2003). Digital image steganography using stochastic modulation. *Proceedings of the SPIE Electronic Imaging, Security, Steganography, and Watermarking of Multimedia Contents V*. Vol. 5020, Santa Clara, CA, pp. 191–202.

92. Fridrich, J., Goljan, M., and Soukal, D. (2005). Efficient wet paper codes. In *Proceedings of Information Hiding 7th International Workshop*, *Springer Lecture Notes in Computer Science*, Vol. 3727, Springer-Verlag, Berlin/Heidelberg, pp. 204–218.

93. Johnson, N. F. (2008). *Observations and Trends in Open Source and Commercial Steganography Tools*, Booz Allen Hamilton Technical Report.

94. National Software Reference Library (NSRL) (2008). http://www.nsrl.nist .gov.

95. Radhakrishnan, R., Kharrazi, M., and Memon, N. (2005). Data masking: a new approach for steganography. *J. VLSI Signal Process. Syst*. **41**(3), 293–303.

## FURTHER READING

Additional Proceedings from the International Information Hiding Workshops/Conferences:

Aucsmith, D., ed. (1998). *Information Hiding: Second International Workshop, IH'98 Portland, Oregon, USA*. *Lecture Notes in Computer Science*, Vol. 1525, Springer-Verlag, Berlin/Heidelberg. DOI: 10.1007/3-540-49380-8.

Barni, M., Herrera-Joancomartí, J., Katzenbeisser, S., and Pérez-González, F., eds. (2005). *Information Hiding: 7th International Workshop, IH 2005, Barcelona, Spain, June 6–8, 2005*, *Lecture Notes in Computer Science*, Vol. 3727, Springer-Verlag, Berlin/Heidelberg. DOI: 10.1007/11558859.

Camenisch, J.L., Collberg, C.S., Johnson, N.F., and Sallee, P., eds. (2006). *Information Hiding: 8th International Workshop, IH 2006, Alexandria, VA, USA, July 10-12, 2006*, *Lecture Notes in Computer Science*, Vol. 4437, Springer, Berlin/Heidelberg. DOI: 10.1007/978-3-540-74124-4.

Fridrich, J., ed. (2004). *Information Hiding: 6th International Workshop, IH 2004, Toronto, Canada, May 23-25, 2004, Revised Selected Papers*, *Lecture Notes in Computer Science*, Vol. 3200, Springer-Verlag, Berlin/Heidelberg. DOI: 10.1007/b104759.

Furon, T., Cayre, F., Doërr, G., and Bas, P., eds. (2007). *Information Hiding: 9th International Workshop, IH 2007, Saint Malo, France, June 11–13, 2007*, *Lecture Notes in Computer Science*, Vol. 4567, Springer, Berlin/Heidelberg. DOI: 10.1007/978-3-540-77370-2.

Moskowitz, I.S., ed. (2001). *Information Hiding: 4th International Workshop, Proceedings, Pittsburgh, Pennsylvania, USA*, April 2001. *Lecture Notes in Computer Science*, Vol. 2135, 2001. Springer-Verlag, Berlin/Heidelberg. DOI: 10.1007/3-540-45496-9.

Petitcolas, F.A.P., ed. (2003). *Information Hiding: 5th International Workshop, Noordwijkerhout, The Netherlands, 7–9 October 2002*, *Lecture Notes in Computer Science*, Vol. 2578, Springer-Verlag, Berlin/Heidelberg. DOI: 10.1007/3-540-36415-3.

Pfitzmann, A., ed. (2000). *Information Hiding: Third International Workshop, Proceedings, Dresden, Germany*, 29 September-1 October 1999, *Lecture Notes in Computer Science*, Vol. 1768, Springer-Verlag, Berlin/Heidelberg. DOI: 10.1007/10719724.

## OTHER SUGGESTED READING

Cole, E. (2003). *Hiding in Plain Sight: Steganography and the Art of Covert Communication.* John Wiley & Sons, Inc., Indianapolis, Indiana.

Cox, I., Miller, M. L., Bloom, J. A., Fridrich, J., and Kalker, T. (2007). *Digital Watermarking and Steganography*, 2nd ed., Morgan Kaufmann Publishers Inc ISBN 0123725852. Burlington, MA.

Wayner, P. (2002). *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*, 2nd ed., Morgan Kaufmann Publishers Inc., San Francisco, CA.

# ATTACK TRACEBACK AND ATTRIBUTION

YONG GUAN AND LINFENG ZHANG
*Iowa State University, Ames, Iowa*

## 1 INTRODUCTION

With the growth of the Internet, cyber attacks happen every day and everywhere. It is very important that we trace back and attribution the real attackers. In this article, we discuss the current techniques in cyber attack traceback. We focus on the present schemes in Internet Protocol (IP) spoofing traceback and stepping stone attack attribution. Furthermore, we introduce the traceback issues in Voice over Internet Protocol (VoIP), botnet, and anonymous systems.

## 2 SCIENTIFIC OVERVIEW

With the phenomenal growth of the Internet, more and more people enjoy and depend on the convenience of its provided services. The Internet has spread rapidly to almost all over the world. Up to December 2006, the Internet has distributed to over 233 countries and world regions, and has more than 1.09 billion users [1]. Unfortunately, the wide use of computer and Internet also has opened doors to cyber attackers. There are different kinds of attacks that an end user of a computer or Internet has to face. For instance, there may be various viruses on the hard disk, there may be several backdoors opened in the operating system, and there may be a lot of phishing e-mails in his/her mailbox, and so on. According to the annual Computer Crime Report of Computer Security Institute (CSI) and the US Federal Bureau of Investigation (FBI) released in 2006 [2], cyber attacks cause a lot of money losses each year.

When we face the cyber attacks, we can detect them and take countermeasures. For instance, an intrusion detection system (IDS) can help detect the attacks; we can update operating systems to close the potential backdoors; we can install antivirus software to defend many known viruses. Although in many cases we can detect attacks and mitigate their damages, it is hard to find who the real attackers are. However, if we cannot trace back to the attackers, they can always conceal in the dark and launch their attacks. If we have the ability to find the attackers and give them desired punishment, we believe this may help reduce the attacks we face every day significantly.

Why is the traceback difficult in computer networks? One reason is that today's Internet is stateless. There are too much data in the Internet to record them. For example, a typical router only forwards the passed packets and does not care where they are from; a typical mail transfer agent (MTA) just relays e-mails to the next agent and never minds who the sender is. Another reason is that today's Internet is almost an unauthorized

environment. Alice can make a VoIP call to Bob and pretends to be Carol; an attacker can send millions of e-mails out using anybody's e-mail address and that individual's mailbox will be bombarded by millions of replies. According to the two main reasons, there are two kinds of attacks that are widely used by attackers and also of interest to researchers all over the world. One is IP spoofing and the other is stepping stone attack. Each IP packet header contains the source IP address. Using IP spoofing, an attacker can change the source IP address in the header to a different machine and thus avoid traceback. Figure 1 shows an example of distributed denial of service (DDoS) attack using IP spoofing. In stepping stone attack, the attack flow may travel through a chain of stepping stones (intermediate hosts) before it reaches the victim. Therefore, it is difficult for the victim to know where the attack comes from except that she or he can see the attack traffic from the last hop of the stepping stone chains. Figure 2 shows an example of stepping stone attack.

In the following section, we first introduce the existing schemes to trace back IP spoofing attacks and then discuss current work on stepping stone attack attribution.

## 2.1 IP Traceback

In this part, we review major existing IP traceback schemes that have been designed to trace back to the origin of IP packets through the Internet. We roughly categorize them into four primary classes:

1. Active probing [3, 4];
2. ICMP traceback [5, 6];
3. Packet marking [7–11];
4. Log-based traceback [12–15].

***2.1.1 Active Probing.*** Stone [4] proposed a traceback scheme called *CenterTrack*, which selectively reroutes packets in question directly from edge routers to some special tracking routers. The tracking routers determine the ingress edge router by observing from which tunnel the packet arrives. This approach requires the cooperation of network administrators, and the management overhead is considerably large.

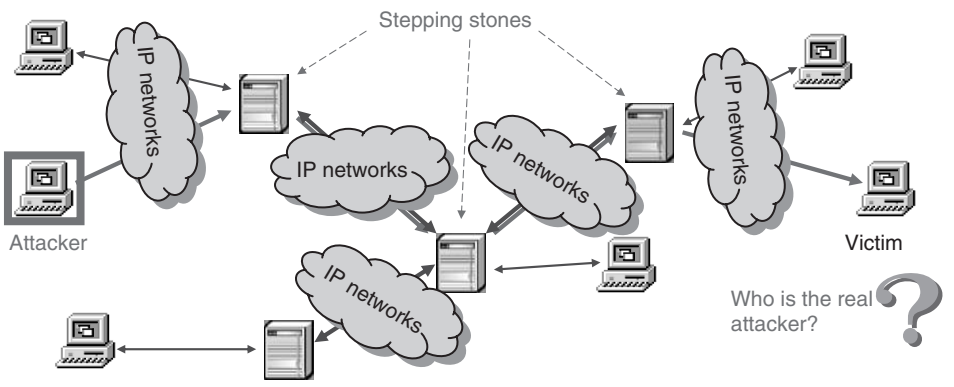



**FIGURE 1** Example of stepping stone attack.

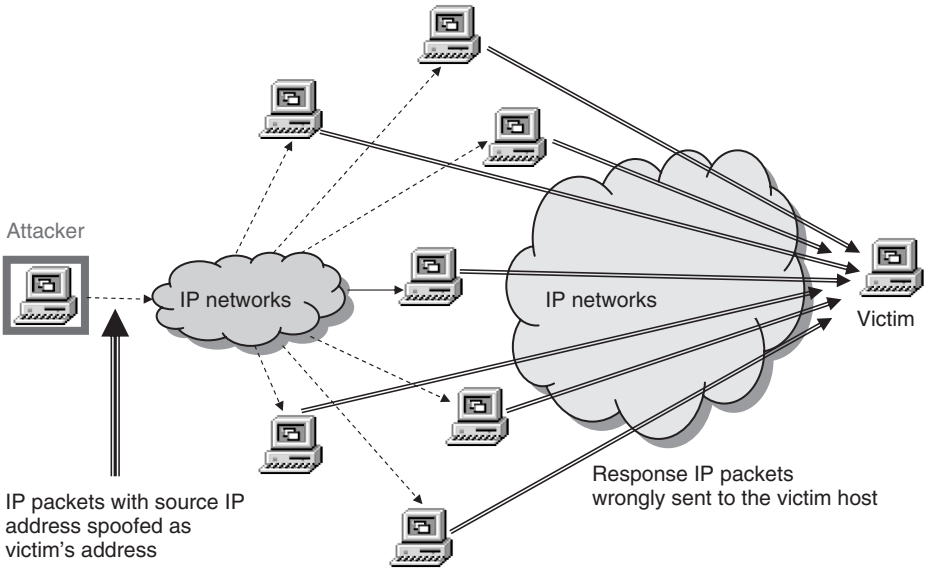



**FIGURE 2** Example of distributed denial of service (DDoS) attack using IP spoofing.

Burch and Cheswick [3] outlined a technique for tracing spoofed packets back to their actual source without relying on the cooperation of intervening internet service providers (ISPs). The victim actively changes the traffic in particular links and observes the influence on attack packets, and thus can determine where the attack comes from. This technique cannot work well on distributed attacks and requires that the attacks remain active during the time period of traceback.

***2.1.2 Internet control message protocol (ICMP) Traceback (iTrace).*** Bellovin [5] proposed a scheme named *iTrace* to traceback using ICMP messages for authenticated IP marking. In this scheme, each router samples (with low probability) the forwarding packets, copies the contents into a special ICMP traceback message, adds its own IP address as well as the IP of the previous and next hop routers, and forwards the packet either to the source or destination address. By combining the information obtained from several of these ICMP messages from different routers, the victim can then reconstruct the path back to the origin of the attacker.

A drawback of this scheme is that it is much more likely that the victim will get ICMP messages from routers nearby than those farther away. This implies that most of the network resources spent on generating and utilizing iTrace messages are wasted. An enhancement of iTrace, called *Intention-Driven iTrace*, was proposed in [6]. By introducing an extra "intention bit", it is possible for the victim to increase the probability of receiving iTrace messages from remote routers.

***2.1.3 Packet Marking.*** Savage et al. [10] proposed a *probabilistic packet marking* (PPM) scheme. Thereafter, several other PPM-based schemes have been developed [8, 9, 11]. The baseline idea of PPM is that routers probabilistically write partial path information into the packets during forwarding. If the attacks are made up of a sufficiently large number of packets, eventually, the victim may get enough information by combining a

modest number of marked packets to reconstruct the entire attack path. This allows victims to locate the approximate source of attack traffic without requiring outside assistance.

*Deterministic packet marking* (DPM) scheme proposed by Belenky and Ansari [7] involves the marking of each individual packet when it enters the network. The packet is marked by the interface closest to the source of the packet on the edge ingress router. The mark remains unchanged as long as the packet traverses the network. However, there is no way to get the whole paths of the attacks.

Dean et al. [8] proposed an *algebraic packet marking* (APM) that reframes the traceback problem as a polynomial reconstruction problem and uses techniques from algebraic coding theory to provide robust methods of transmission and reconstruction. The advantage of this scheme is that it offers more flexibility in design and more powerful techniques that can be used to filter out attacker generated noise and separate multiple paths. However, it shared similarity with PPM in that it requires a sufficiently large number of attack packets.

***2.1.4 Log-based Traceback.*** The basic idea of log-based traceback is that each router stores the information (digests, signature, or even the packet itself) of network traffic through it. Once an attack is detected, the victim queries the upstream routers by checking whether they have logged the attack packet in question or not. If the attack packet's information is found in a given router's memory, then that router is deemed to be part of the attack path. Obviously, the major challenge in log-based traceback schemes is the storage space requirement at the intermediate routers.

Matsuda et al. [13] proposed a hop-by-hop log-based IP traceback method. Its main features are logging *packet feature* that is composed of a portion of the packet for identification purpose, and an algorithm using data-link identifier to identify the routing of a packet. However, for each received packet, about 60 bytes data should be recorded. The resulted large memory space requirement prevents this method from being applied to high-speed networks with heavy traffic.

Although today's high-speed IP networks suggest that classical log-based traceback schemes would be too prohibitive because of the huge memory requirement, log-based traceback becomes attractive after Bloom filter-based (i.e. hash-based) traceback schemes were proposed. *Bloom filters* were presented by Burton H. Bloom [16] in 1970, and have been widely used in many areas, such as database and networking. A Bloom filter is a space-efficient data structure for representing a set of elements to respond membership queries. It is a vector of bits that are all initialized to value 0. Then each element is inserted into the Bloom filter by hashing it using several independent uniform hash functions and setting the corresponding bits in the vector to value 1. Given a query whether an element is present in the Bloom filter, we hash this element using the same hash functions and check if all the corresponding bits are set to 1. If any one of them is 0, then undoubtedly this element is not stored in the filter. Otherwise, we would say that it is present in the filter, although there is a certain probability that the element is determined to be in the filter whereas it is actually not. Such false cases are called *false positives*. The space efficiency of Bloom filters is achieved at the cost of a small acceptable false-positive rate. Bloom filters were first introduced into IP traceback area by Snoeren et al. [15]. They built a system named *source path isolation engine* (SPIE) that can trace the origin of a single IP packet delivered by the network in the recent past. Therefore, SPIE can trace an attack even when it finishes using a single packet. They demonstrated that the system is effective, space-efficient, and

implementable in current or next-generation routing hardware. Bloom filters are used in each SPIE-equipped router to record the digests of all packets it received in the recent past. The digest of a packet is exactly several hash values of its nonmutable IP header fields and the prefix of the payload. However, the inherent false positives of Bloom filters caused by unavoidable collisions restrain the effectiveness of these systems. To reduce the impact of unavoidable collisions in Bloom filters, Zhang and Guan [17] propose a topology-aware single packet IP traceback system, namely TOPO. The router's local topology information, that is, its immediate predecessor information is utilized. The performance analysis shows that TOPO can reduce the number and scope of unnecessary queries and decrease false attributions significantly. When Bloom filters are used, it is difficult to decide their optimal control parameters a priori. They designed a k-adaptive mechanism that can dynamically adjust parameters of Bloom filters to reduce the false-positive rate.

Shanmugasundaram et al. [14] proposed a *payload attribution system* (PAS) based on a *hierarchical Bloom filter* (HBF). HBF is such a Bloom filter that an element is inserted several times using different parts of the same element. Compared with SPIE, which is a packet digesting scheme, PAS uses only the payload excerpt of a packet. It is useful when the packet header is unavailable.

Li et al. [12] proposed a Bloom filter-based IP traceback scheme that requires an order of magnitude processing and storage cost less than that of SPIE, thereby being able to scale to much higher link speed. The baseline idea of their approach is to sample and log a small percentage of packets and 1-bit packet marking is used in their sampling scheme. Therefore, their traceback scheme combines packet marking and packet logging together. Their simulation results showed that the traceback scheme can achieve high accuracy, and scale well to a large number of attackers. However, as the authors also pointed out, because of the low sampling rate, their scheme is no longer capable to trace one attacker with only one packet.

### 2.2 Stepping Stone Attack Attribution

Ever since the problem of detecting stepping stones was first proposed by Staniford-Chen and Heberlein [18], several approaches have been proposed to detect encrypted stepping stone attacks.

The ON/OFF-based approach proposed by Zhang and Paxson [19] is the first timing-based method that can trace stepping stones even if the traffic were to be encrypted. In their approach, they calculated the correlation of different flows by using each flow's OFF periods. A flow is considered to be in an OFF period when there is no data traffic on a flow for more than a time period threshold. Their approach comes from the observation that two flows are in the same connection chain if their OFF periods coincide.

Yoda and Etoh [20] presented a deviation-based approach for detecting stepping stone connections. The deviation is defined as the difference between the average propagation delay and the minimum propagation delay of two connections. This scheme comes from the observation that the deviation for two unrelated connections is large enough to be distinguished from the deviation of connections in the same connection chain.

Wang et al. [21] proposed a correlation scheme using interpacket delay (IPD) characteristics to detect stepping stones. They defined their correlation metric over the IPDs in

a sliding window of packets of the connections to be correlated. They showed that the IPD characteristics may be preserved across many stepping stones.

Wang and Reeves [22] have presented an active watermark scheme, which is designed to be robust against certain delay perturbations. The watermark is introduced into a connection by slightly adjusting the IPDs of selected packets in the flow. If the delay perturbation is not quite large, the watermark information will remain along the connection chain. This is the only active stepping stone attribution approach.

Strayer et al. [23] presented a state-space algorithm that was derived from their work on wireless topology discovery. When a new packet is received, each node is given a weight that decreases as the elapsed time from the last packet from that node increases. Then the connections on the same connection chain will have higher weights than other connections.

However, none of these previous approaches can effectively detect stepping stones when delay and chaff perturbations exist simultaneously. Although no experimental data is available, Donoho et al. [24] have indicated that there are theoretical limits on the ability of attackers to disguise their traffic using evasions for sufficiently long connections. They assumed that the intruder has a maximum delay tolerance and used wavelets and similar multiscale methods to separate the short-term behavior of the flows (delay or chaff) from the long-term behavior of the flows (the remaining correlation). However, this method requires the intrusion connections to remain for long periods and the author never experimented to show the effectiveness against chaff perturbation. These evasions consist of local jittering of packet arrival times and the addition of superfluous packets.

Blum et al. [25] proposed and analyzed algorithms for stepping stone detection using ideas from Computational Learning Theory and the analysis of random walks. They achieved provable (polynomial) upper bounds on the number of packets needed to confidently detect and identify stepping stone flows with proven guarantees on the false positives, and provided lower bounds on the amount of chaff that an attacker would have to send to evade detection. However, their upper bounds on the number of packets required were large, whereas the lower bounds on the amount of chaff needed for attacker to evade detection were very small. They did not discuss how to detect stepping stones without enough packets or with large amounts of chaff, and did not show experimental results.

Zhang et al. [26] proposed and analyzed algorithms which represent that those attackers cannot always evade detection only by adding limited delay and independent chaff perturbations. They provided the upper bounds on the number of packets needed to confidently detect stepping stone connections from nonstepping stone connections with any given probability of false attribution.

Although there have been a lot of stepping stone attack attribution schemes, there is a lack of comprehensive experimental evaluation of these schemes. Therefore, there are no objective, comparable evaluation results on the effectiveness and limitations of these schemes. Xin et al. [27] designed and built a scalable test bed environment that can evaluate all existing stepping stone attack attribution schemes reproducibly, provide a stable platform for further research on this area, and be easily reconfigured, expanded, and operated with user-friendly interface. This test bed environment has been established in a dedicated stepping stone attack attribution research laboratory. An evaluation of proposed stepping stone techniques is currently underway.

## 3 RESEARCH AND FUNDING DATA

From early 2004, Intelligence Advanced Research Projects Activity (IARPA) (formerly, Disruptive Technology Office (DTO)/Advanced Research and Development Activity (ARDA)) supported seven groups from universities and industries on stepping stone attack attribution. Table 1 shows their topics, affiliations, and the names of principal investigators.

The group from North Carolina State University utilizes timing-based watermarking to trace back stepping stone attacks. They proposed schemes to handle repacketization of the attack flow. Wang from George Mason University proposed a "centroid-based" watermarking scheme to detect attack flows with chaff. The group from Iowa State University proposed the first effective detection scheme to detect attack flows with both delay and chaff perturbations. A scheme named *datatick* is proposed, which can handle significant packet merging/splitting and can attribute multiple application layer protocols (e.g. X-windows over secure shell (SSH), Windows Remote Desktop, virtual network computing (VNC), and SSH). A scalable test bed environment is also established, which can evaluate all existing stepping stone attack attribution schemes reproducibly.

The group from Johns Hopkins University demonstrates the feasibility of a "post-mortem" technique for traceback through indirect attacks. The evidence in memory and other sources is collected and characterized to attribute the attacks. The group from Telcordia Technologies proposed a scheme that reroutes the attack traffic from noncooperative networks to cooperative networks, such that the attacks can be attributed. The BBN's group integrates single packet traceback and stepping stone correlation together. A distributed traceback system called *FlyTrap* is developed for uncooperative and hostile networks. A group from Sparta integrates multiple complementary traceback approaches and tests them in Tor anonymous system.

National Science Foundation supports a research project named "Tracing VoIP Calls through the Internet" led by Xinyuan Wang from George Mason University. The objective of this project is to investigate how VoIP calls can be effectively identified and traced

**TABLE 1 DTO/ARDA-Funded Projects on Stepping Stone Attack Attribution**

| Research Topic | Affiliation | Principal Investigator |
|---|---|---|
| Tracing attacks through noncooperative networks and stepping stones with timing-based watermarking | North Carolina State University | Douglas Reeves |
| Advanced watermark tracing through stepping stones and uncooperative networks | George Mason University | Frank Wang |
| Stepping stone attack attribution in noncooperative IP networks | Iowa State University | Yong Guan |
| Johns Hopkins applied physics laboratory presentation | Johns Hopkins University | S. Lee |
| RapidTrace: rapid traceback of cyber attacks | Telcordia | Rajesh Talpade |
| FlyTrap: a practical traceback system for sparse and uncooperative deployment | BBN | Timothy Strayer |
| Tracing attacks through noncooperating networks | Sparta | Richard Edell |

in the Internet and to develop efficient tracing methods with sound scientific foundation. Wang et al. introduced their watermarking technology in stepping stone attack attribution into VoIP attribution and showed VoIP calls still can be attributed [28].

Strayer et al. have been supported by US Army Research Office in their research on how to attribute the attackers using botnets. Their approach for detecting botnets is to examine flow characteristics such as bandwidth, duration, and packet timing looking for evidence of botnet command and control activity [29].

## 4 CRITICAL NEEDS ANALYSIS

Although large scale cyber terrorism seldom happens, some cyber attacks have already showed their power in damaging homeland security. For instance, on October 21, 2002, all the 13 Domain Name System's (DNS) root name servers sustained a Denial of Service attack [30]. Some root name servers were unreachable from many parts of the global Internet due to congestion from the attack traffic. Till now, we do not know who the real attacker is and what his/her intention is.

Besides the Internet itself, many sensitive institutions, such as the US power grid, nuclear power plants, and airports, may also be attacked by terrorists if they are connected to the Internet, although they have been carefully protected physically. If the terrorists want to launch large scale attacks targeting these sensitive institutions through the Internet successfully, probably they have to try several times. If we only sit there and do not fight back, they finally can find our vulnerabilities and achieve their evil purpose. However, if we have the ability that attributes to the source of the attacks, we can detect and arrest them before they succeed.

Although there have been a lot of traceback and attribution schemes on IP spoofing and stepping stone attacks, there still have a lot of open issues in this area. The biggest issue is the deployment of these schemes. Many schemes (e.g. packet marking, log-based traceback) need the change of IP on each intermediate router. Many schemes need a lot of network monitors placed all over the world. These are very difficult to be implemented in current Internet without the supports from government, manufactures, and academics. It is necessary to consider traceback demands when designing and deploying next-generation networks.

## 5 RESEARCH DIRECTIONS

There are still some open problems in attack traceback and attribution.

### 5.1 Vo-IP Attribution

Like the Internet, the VoIP also provides unauthorized services. Therefore, some security issues existing in the Internet may also appear in the VoIP systems. For instance, a phone user may receive a call with a qualified caller ID from his/her credit card company, so he/she would answer the critical questions about social security number and date of birth, and so on. However, this call comes actually from an attacker who fakes the caller ID using a computer. Compared with a public switched telephone network (PSTN) phone or mobile phone, IP phone lacks monitoring. Therefore, it is desirable to provide schemes that can attribute or trace back to the VoIP callers.

### 5.2 Botnet Traceback

A botnet is a network of compromised computers, or bots, commandeered by an adversarial botmaster. Botnets usually spread with virus and communicate through the internet relay chat (IRC) channel. With the army of bots, the bot controllers can launch many attacks, such as spam, phishing, key logging, and denial of service. Now, more and more scientists are interested in how to detect, mitigate, and trace back botnet attacks.

### 5.3 Traceback in Anonymous Systems

Another issue is that a lot of anonymous systems, such as Tor, exist all over the world [31]. Tor is a toolset for anonymizing web browsing and publishing, instant messaging, IRC, SSH, and other applications that use the transmission control protocol (TCP) protocol. It provides anonymity and privacy for legal users, and at the same time, it is a good platform to launch stepping stone attacks. Communications over Tor are relayed through several distributed servers called *onion routers*. There are more than 800 onion routers all over the world so far. Since Tor may be seemed as a special stepping stone attack platform, it is interesting to consider how to trace back attacks over Tor.

## REFERENCES


1. Internet World Stats. (2007). [Online]. Available: http://www.internetworldstats.com.
2. Gordon, L. A., Loeb, M. P., Lucyshyn, W., and Richardson, R. (2006). *CSI/FBI Computer Crime and Security Survey*.
3. Burch, H., and Cheswick, B. (2000).Tracing anonymous packets to their approximate source. *Proceedings of USENIX LISA 2000*. New Orleans, December, pp. 319–327.
4. Stone, R. (2000).Centertrack: An IP overlay network for tracking DoS floods. *Proceedings of the 9th USENIX Security Symposium*. Denver, August, pp. 199–212.
5. Bellovin, S. M. (2000). *ICMP Traceback Messages*, Internet Draft.
6. Wu, S. F., Zhang, L., Massey, D., and Mankin, A. (2001). *Intention-Driven ICMP Trace-back*, Internet Draft.
7. Belenky, A., and Ansari, N. (2003). IP traceback with deterministic packet marking. *IEEE Commun. Lett*. **7**(4), 162–164.
8. Dean, D., Franklin, M., and Stubblefield, A. (2002). An algebraic approach to IP traceback. *Inf. Syst. Secur*. **5**(2), 119–137.
9. Park, K., and Lee, H. (2001).On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack. *Proceedings of IEEE INFOCOM 2001*. Anchorage, April, pp. 338–347.
10. Savage, S., Wetherall, D., Karlin, A., and Anderson, T. (2001). Network support for IP traceback. *IEEE/ACM Trans. Net*. **9**(3), 226–237.
11. Song, D., and Perrig, A. (2001).Advanced and authenticated marking schemes for IP traceback. *Proceedings of IEEE INFOCOM 2001*. Anchorage, April.
12. Li, J., Sung, M., Xu, J., and Li, L. (2004). Large-scale IP traceback in high-speed internet: practical techniques and theoretical foundation. *Proceedings of 2004 IEEE Symposium on Security and Privacy*. Oakland, May.
13. Matsuda, S., Baba, T., Hayakawa, A., and Nakamura, T. (2002). Design and implementation of unauthorized access tracing system. *Proceedings of the 2002 Symposium on Applications and the Internet (SAINT 2002)*. Nara, January.

14. Shanmugasundaram, K., Brönnimann, H., and Memon, N. (2004). Payload attribution via hierarchical Bloom filters. *Proceedings of the 11th ACM Conference on Computer and Communications Security*. Washington, DC, October.
15. Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Schwartz, B., Kent, S. T., and Strayer, W. T. (2002). Single-packet IP traceback. *IEEE/ACM Trans. Network*. **10**(6), 721–734.
16. Bloom, B. H. (1970). Space/time trade-offs in hash coding with allowable errors. *Commun. ACM* **13**(7), 422–426.
17. Zhang, L., and Guan, Y. (2006). TOPO: a topology-aware single packet attack traceback scheme. *Proceedings of the 2nd IEEE Communications Society/CreateNet International Conference on Security and Privacy in Communication Networks (SecureComm 2006)*. Baltimore, August.
18. Staniford-Chen, S., and Heberlein, L. T. (1995). Holding intruders accountable on the internet. *Proceedings of the 1995 IEEE Symposium on Security and Privacy*. Oakland, May.
19. Zhang, Y., and Paxson, V. (2000). Detecting stepping stones. *Proceedings of the 9th USENIX Security Symposium*. Denver, August, pp. 171–184.
20. Yoda, K., and Etoh, H. (2000). Finding a connection chain for tracing intruders. *Proceedings of the 6th European Symposium on Research in Computer Security (ESORICS 2000)*. Toulouse, October.
21. Wang, X., Reeves, D. S., and Wu, S. F. (2002). Inter-packet delay based correlation for tracing encrypted connections through stepping stones. *Proceedings of the 7th European Symposium on Research in Computer Security (ESORICS 2002)*. Zurich, October.
22. Wang, X., and Reeves, D. S. (2003). Robust correlation of encrypted attack traffic through stepping stones by manipulation of interpacket delays. *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 2003)*. Washington, DC, October.
23. Strayer, W. T., Jones, C. E., Castineyra, I., Levin, J. B., and Hain, R. R. (2003). *An Integrated Architecture for Attack Attribution*, BBN Technologies, Tech. Rep. BBN REPORT-8384, December.
24. Donoho, D. L., Flesia, A. G., Shankar, U., Paxson, V., Coit, J., and Staniford, S. (2002). Multiscale stepping-stone detection: detecting pairs of jittered interactive streams by exploiting maximum tolerable delay. *Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID 2002)*. Zurich, October.
25. Blum, A., Song, D., and Venkataraman, S. (2004). Detection of interactive stepping stones: algorithms and confidence bounds. *Proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004)*. Sophia Antipolis, September.
26. Zhang, L., Persaud, A. G., Johnson, A., and Guan, Y. (2006). Detection of stepping stone attack under delay and chaff perturbations. *25th IEEE International Performance Computing and Communications Conference (IPCCC 2006)*. Phoenix, April.
27. Xin, J., Zhang, L., Aswegan, B., Dickerson, J., Dickerson, J., Daniels, T., and Guan, Y. (2006). A testbed for evaluation and analysis of stepping stone attack attribution techniques. *Proceedings of TridentCom 2006*. Barcelona, March.
28. Wang, X., Chen, S., and Jajodia, S. (2005). Tracking anonymous peer-to-peer VoIP calls on the internet. *Proceedings of the 12th ACM Conference on Computer Communications Security (CCS 2005)*. November.
29. Strayer, W. T., Walsh, R., Livadas, C., and Lapsley, D. (2006). Detecting botnets with tight command and control. *Proceedings of the 31st IEEE Conference on Local Computer Networks (LCN)*. November 15–16, Tampa, FL.
30. Vixie, P., Sneeringer, G., and Schleifer, M. (2002). *Events of 21-Oct-2002*, November 24. http://www.isc.org/ops/f-root/october21.txt.
31. Tor system. http://tor.eff.org/, 2007.

# CYBER FORENSICS

MARCUS K. ROGERS
*Purdue University, West Lafayette, Indiana*

## 1 INTRODUCTION

The field of forensics or criminalistics in general has received a great deal of attention over the last few years. The popular media's obsession with anything forensic related has also resulted in increased attention by the scientific and information technology communities. The judiciary has also increased its scrutiny of the field, as judges and lawyers are struggling with the concept of digital or electronic evidence. The very nature of evidence has evolved from being primarily document based to being digital or electronic based. It has been estimated that in the next few years, 80% of all criminal investigations will contain digital evidence (DE). This prediction seems realistic as electronic documents have replaced paper documents in most business environments.

The media attention has also prompted many private sector consulting companies and academia to focus on this area of criminalistics. The introduction of these two communities to the field has resulted in some interesting challenges and uncovered various issues within the field. However, the private sector and academia have also been important factors in the rapid evolution that cyber forensics is currently undergoing.

The current article is divided into three main sections: scientific overview, critical needs analysis, and research directions. More explicitly, the article looks at the development of this new forensic discipline, with specific attention on its historical development, and current state. The discussion will examine the context of digital forensic science (DFS) and cyber forensics/DE, emerging standards and process model(s), current and near term issues and challenges, and finally future directions for the field.

Limitations on the size of the article precludes an in-depth discussion of many of the subtopics, but those interested with specific topics are directed to the further readings section. It is important that it is understood that the deliverablility of this article is to provide a high-level overview of the field.

## 2 SCIENTIFIC OVERVIEW

DFS is the umbrella category to which cyber forensics or DE investigation belongs [1–5]. DFS encompasses what has historically been considered computer forensics (media analysis) as well as multimedia such as audio, video, and imaging technology (IT) [1, 4, 6, 7]. DFS has been defined as follows:

> The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of DE derived from digital sources for the purpose of facilitating or furthering the reconstruction

> of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations [8].

DFS is a forensic science and as such the underlying foundation is no different than other forensic or criminalistics fields. As a forensic science, the admissibility of evidence and the presentation of findings or results in a court of law (e.g. civil, criminal, regulatory, and administrative) is its primary consideration.

In the United States, the American Academy of Forensic Science (AAFS) oversees all forensic sciences, and this governing body is what the courts look to in order to determine the status of a forensic science field. In order to be officially recognized by the AAFS, DFS has been further subdivided into the following [1]:

- digital evidence (DE)
- imaging technology (IT)

The rationale for the subdivision is based on the notion that DE and IT require different and distinct skills sets, knowledge, and abilities. The subdivision has led to the creation of two bodies in the United States to deal with the maturation and acceptance of these new fields of study as follows. The Scientific Working Group on Digital Evidence (SWGDE) and the Scientific Working Group on Imaging Technology (SWGIT). As the name connotes, the SWGDE has the responsibility for DE that encompasses computer forensics (also known as *media analysis*), network/distributed forensics, and code analysis.

The focus of this article is on the DE side of DFS and will not include any discussion related to IT. However, it should be noted that IT and DE are converging and it is expected that in the not too distant future the separation of these two areas/domains will be artificial, as DE will cover both the domains.

### 2.1 Current State

Cyber forensics is defined as follows:

> The scientific examination of electronic data in such a way that the information can be used as evidence in a court of law [9].

This definition is based on the traditional use of the term *forensics*. In the realm of cyber security, cyber forensics is often mistakenly confused of being synonymous with incident response and general investigations such as root cause analysis. Strictly speaking, while incident response, root cause analysis, and cyber forensics are investigative in nature, incident response and root cause analysis have a lower standard of proof. Many organizations will use the cyber forensics process model to aid in general investigations where legal action is not initially anticipated (either civil or criminal). These organizations understand that by using the highest standard of proof as a threshold, this ensures that, if at a later date legal action is desired, there will be fewer issues (e.g. inadmissibility of evidence).

Cyber forensics includes the same processes as DFS and treats a system, network, or storage device as a witness, storage container, or victim/corpse. Cyber forensics is the

marriage of science, technology, and engineering (STEM disciplines) with law and the legal justice system [10–12].

At its most basic level cyber forensics focuses on the three As of acquire, authenticate and analyze DE [13]. *Acquire* refers to acquiring evidence in a manner that does not alter the scene or the potential evidence (or at the very least minimizes the contamination). Authenticate means to prove that the evidence has fidelity and integrity (in the case of a forensic image), and is a true representation of the state and nature of the DE. The most common method of authentication is by using a hashing algorithm (e.g. MD5, SHA 256)—discussed later. *Analyze* refers to examining and interpreting the data/evidence and then drafting a report (either oral or written).

In conjunction with the three As is the concept of chain of custody of evidence. It is vital that the entire life cycle of the DE be documented and accounted for. Chain of custody of evidence is tantamount to the who, what, when, where, how, and why of the evidence, from its initial identification to its ultimate disposition (e.g. destruction or return). If any part of the "chain" is broken or brought into question, the admissibility and/or weight of the evidence becomes questionable and/or significantly diminished [3, 14–16].

According the Digital Forensic Research Workshop (DFRWS) [5, 17, 18], there are at least three different communities that have a vested interest in cyber forensics. These communities consist of Law Enforcement, Military, and Private Sector. Cyber forensics was historically the domain of law enforcement (including military law enforcement). In fact, the term computer forensics came from the law enforcement community in the earlier 1980s.

As society has become more dependent on technology and the Internet, DE and electronic trails have become more commonplace. This has led to the military being interested in cyber forensics for purposes of national security and information warfare. The military soon realized that the same process models and tools used for traditional law enforcement DE investigations could be used for intelligence gathering.

The private sector's interest in cyber forensics stems from the ubiquity of technology in the workplace and/or the fact that electronically stored information (ESI) plays a vital role in various civil litigations (e.g. Intellectual Property (IP) law suits, wrongful terminations, and regulatory investigations). The private sector has also discovered that offering consulting services in the area of DE investigations is lucrative. The reasons for this service line are varied and include the belief that despite law enforcement having the longest history with DE, they are ill prepared and/or trained to conduct complicated investigations. There is also the very real desire to protect organizations from unwanted publicity that can occur if law enforcement is officially involved.

Recently, a fourth community has been added to the model. Educational institutions are starting to play a vital role in education and training, curriculum development, and both applied and basic research in this area. With the public popularity of forensics, academia sees the potential for increased enrollment and funding opportunities. Academy also plays a vital role in basic and applied research in this field—which is discussed in a subsequent section.

Unfortunately, the goals of the four communities are not necessarily congruent. Law enforcement is concerned with the investigation and prosecution of criminals and the military is concerned with protecting national security, gathering intelligence, and attacking the enemy's technology, while protecting its own. The private sector is concerned with

profit, protecting its investors, getting its infrastructure back up and running in the event of an attack or breach. Academia is concerned with education, training, and research. These sometimes mutually exclusive goals have led to conflicts and a lack of uniformity within the scientific discipline.

Cyber forensics is a relatively immature field. The more traditional forensic sciences such as questioned document analysis and latent fingerprint analysis have been around for several hundreds of years. As was stated earlier, cyber forensics can trace its beginnings to the 1980s in North America and to about the same time period in the United Kingdom.

Historically, vendors have dominated the area of cyber forensics. As previously stated, the field originated with law enforcement. Few, if any, law enforcement officers dealing with DE had basic or advanced degrees in computer science or engineering. This resulted in a dependency on vendors to develop tools to allow law enforcement to conduct their investigations [4, 5]. There was little, if any, oversight on the vendors and the investigators were completely dependent on the vendors to ensure that the tools worked correctly. Although this may have been sufficient in the past, this dependency has become very problematic (Section 3). It is now the job/mandate of academia to develop the theoretical framework for tool development and the investigators to articulate the functional requirements of the tools; all the while keeping in mind the fundamental rule of forensics—admissibility of the derived evidence.

At the time of writing, there was no definitive process model for conducting the actual acquisition, authentication, and analysis [5–7, 17, 19, 20]. Several academic papers have been written and organizations, such as SWGDE, National Institute of Justice (NIJ), US Secret Service (USSS), International Association of Computer Investigative Specialists (IACIS), the High Technology Crime Investigators Association (HTCIA), Royal Canadian Mounted Police (RCMP), Canada, and Association of Chief Police Officers (ACPO) United Kingdom, have released white papers, technical reports, and guidelines. However, there are varying degrees of consensus among these groups as to what is the best approach from an investigative, admissibility of evidence, and scientific perspective. The ever-changing nature of technology also makes it extremely difficult to adapt any sort of static approach for gathering DE.

The closest approach to a consensus can be found in the work of the International Organization on Computer Evidence (IOCE) and SWGDE, whom have released a set of six high-level principles for dealing with DE [1]:

1. When dealing with DE, all of the general forensic and procedural principles must be applied.
2. Upon seizing DE, actions taken should not change that evidence.
3. When it is necessary for a person to access original DE, that person should be trained for the purpose.
4. All activity relating to the seizure, access, storage, or transfer of DE must be fully documented, preserved, and available for review.
5. An individual is responsible for all actions taken with respect to DE while the DE is in their possession.
6. Any agency, which is responsible for seizing, accessing, storing, or transferring DE is responsible for compliance with these principles.

Principle 2 is considered one of the most basic axioms, and yet even this is coming under increasing scrutiny and debate given the fact that cyber forensics is moving away from dealing primarily with static systems (turned off) or storage devices, to live systems that are very dynamic. Although it is relatively easy to adhere to the second principle with systems that are static, it is impossible not to change the state and nature of the scene and possible evidence, when gathering evidence from a system that is turned on and running processes.

With a static system, an investigator can use a hardware write blocker to protect the suspect storage device from being written to or changed, while acquiring an image or collecting pieces of evidence. The hardware write blocker is a physical bridge device that sits between the investigators system and the suspect storage device and physically blocks any commands to the suspect device that could modify or change the device. It essentially turns the suspect device into a physical read only device (much like the old write protect tabs on floppy disks). The hardware write blocker is quickly replacing software write blockers that operated at the BIOS and Interrupt level (INT13 or Extended INT13). With modern drives and operating systems, the BIOS is often no longer responsible for managing input output (IO) requests, thus the software write blockers are often bypassed and prone to failure resulting in changes to the suspect device, and possible contamination and/or destruction of evidence (both inculpatory and exculpatory).

Live system and memory analysis present unique problems. With a system turned off, any potential evidence that may have been in the volatile memory is lost, although, depending upon the operating system and the user defined settings, the swapfile or virtual memory (pagefile) is accessible and may contain remnants of important data. With live systems, the memory is intact, any network shares are still mounted, and cache information is available. The conundrum arises from the fact that in order to collect and interpret the data in a meaningful (human readable) way, an application has to be run on the system. This causes a change in the memory as a running application or tool uses the memory, and thus changes the state and nature of the very thing it is trying to collect. Despite this issue, the limitations of the tools, lack of protected memory space, and virtualization of storage devices, makes the examination, collection, and analysis of live systems and memory an investigative reality.

## 2.2 Cyber Forensics Process Model

The exact process of conducting a cyber forensics investigation is dependent upon various factors such as the context of the investigation, the technology in question, type of storage device and file system, technical knowledge of the suspect, and legal considerations. For the sake of simplicity, only a generic process model is discussed.

Once the cyber forensic process has been initiated, the first phase deals with the proper identification of the physical and digital crime scene, and potential evidence or likely containers of potential evidence (e.g. workstations, external peripherals, network storage, and log files).

Once the proper identification has been completed, the evidence must be collected in a manner that minimizes the alteration to both the physical and digital crime scene. This may include photographing the physical scene, obtaining forensic images of the systems,

storage devices, and so on. (A forensic image is a bit stream image that captures all data from the entire physical storage; from sector 0 to the last sector.)

Once the evidence has been collected, it needs to be preserved and its integrity needs to be maintained. This is often accomplished by using protected media (i.e. write once) or read only file image formats (e.g. EnCase E0). A digital hash functional (e.g. MD5 and SHA1) is then calculated from the original and the image copy and compared. If the totals match, it is assumed that the image copy is an exact copy of the original. This calculated and stored hash total can be used to further prove that nothing was changed on the image at a later date.

The collected evidence is then examined and analyzed to determine what has happened (sometimes referred to as *root cause analysis* in incident response situations) and answer the appropriate investigative questions. In most cases, the original evidence is never examined; the investigator works from a copy (investigative copy) of the forensic image (library copy). This further ensures the integrity of the original evidence. Various tools are used to abstract the evidence and assist in the interpretation of what is discovered.

The final phase consists of creating a report that summarizes the process that was followed, the evidence identified and collected, and the investigative findings. This report may include both factual and speculative findings. The report should be written for a nontechnical audience and be free from acronyms and jargon. A glossary is often used to assist readers with technical terms.

## 3 CRITICAL NEEDS AND ISSUES

As a relatively new discipline, cyber forensics has its fair share of issues, hurdles, and critical needs. Some of these are generic and common to all forensic sciences (e.g. changing case law and rules pertaining to admissibility of evidence, scientific expert witness testimony considerations). However, others are unique to cyber forensics and are artifacts of the dynamic nature of technology and scientific advances. For simplicity sake, the issues can be broken down into the following categories: education and training, technology and tools, research and scholarship, policies and processes, and at the center, legal requirements (Figure 1).

### 3.1 Education and Training

The demand for properly educated and trained investigators and scientists has outpaced the supply. Formal education and training in cyber forensics has only come about in the last few years. The tremendous demand for all levels of individuals to deal with DE has resulted in an increased interest by the various education institutions ranging from vocational schools and private colleges (offering associate degrees) to tier 1 doctoral granting universities. Programs of study can be found in criminal justice departments, management, computer science, engineering, and technology departments, as well as in law schools, and law and society departments. This academic plurality has some very serious unanticipated consequences for the discipline. One serious consequence is the lack of standards for curricula development. This has resulted in a situation in which the

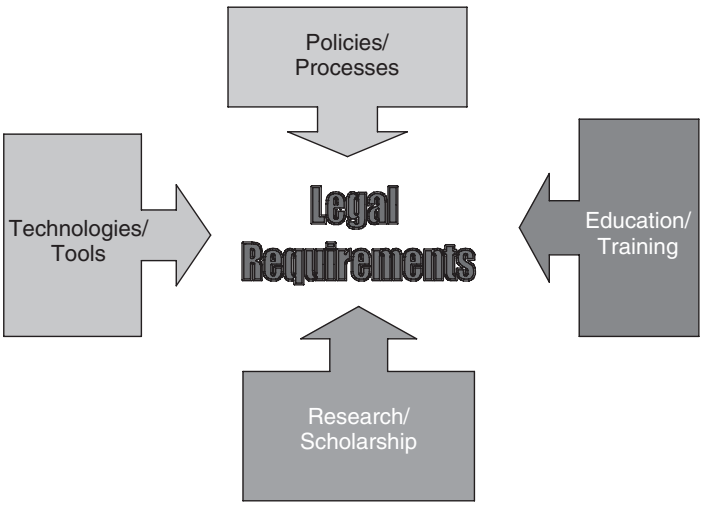



**FIGURE 1** Cyber Forensic Issues.

judiciary is confused as to who has the proper credentials and who is properly qualified in the scientific discipline. The severity of this problem has prompted the AAFSs in conjunction with the Forensic Science Education Program Accreditation Commission (FEPAC) and the NIJ to begin development of a national strategy for accrediting cyber forensic academic programs. The accreditation will be similar to accreditation program that was developed for the traditional forensic sciences (e.g. biology, physics, and chemistry).

While accreditation may address the educational issues, the training issue has still not been addressed. There is no one "gold" standard for practitioners of cyber forensics. At the time of writing, there were approximately eight different professional certifications in cyber forensics, and at least 12 bodies claiming to be the "legitimate" certification and accreditation body. The certifications range from vendor/tool specific to law enforcement only. Some of these bodies grant the credentials based on extensive hands on testing, while others are based solely on the individual's resume and history of cases investigated.

This lack of standards in training is unacceptable and negatively impacts the maturation of the discipline. In an attempt to address this, a national certification body for cyber forensics is being formed. This body will oversee the testing and proficiency requirements and accreditation of training programs. It will not offer any training itself in order to maintain a neutral posture. This model is consistent with the Boards developed by the other forensic sciences, and thus it will allow an individual to effectively be Board Certified in cyber forensics (it is anticipated that the certification will be in a specific specialty such as digital crime scene analysis and small-scale devices).

The emerging requirement in the United States that crime laboratories be accredited by the American Society of Crime Lab Directors/Laboratory Accreditation Board (ASCLD/LAB) in all areas of criminalistics, including DE (ca. 2003), has increased the pressure for educational and training standards. The ASCLD/LAB has specific educational, training, and proficiency requirements for individuals handling DE. These

requirements should form the basis for the development of standards for certification and possibly the development of a recognized common body of knowledge (CBK) or corpus of knowledge for cyber forensics. It should be noted that ASCLD/LAB is being harmonized with the ISO/IEC 17025 General Requirements for the competence of calibration and testing laboratories. This mapping to an ISO will assist in the internationalization of standards.

### 3.2 Technology and Tools

The field of cyber forensics is inextricably tied to technology. Given the fact that technological advances are continuing at an unheralded pace, keeping up with the changes is a major issue for the field [3, 21]. Even the most basic process of identification has been complicated by changes in technology. Currently, digital storage devices come in a plethora of sizes (both in terms of storage capacity and footprint). Storage media ranges from devices the size of dimes to thumb drives, watches, digital media devices, personal digital assistants (PDAs), cell phones, digital video recorders (DVRs), gaming systems, smart refrigerators, and black boxes in automobiles. The unconventional nature of these devices makes the chances of DE being overlooked much higher. These devices have also pushed the very method of storage from magnetic based (e.g. hard drives) to solid state and flash memory. The move from magnetic to solid-state storage also has a large impact on the notion of data permanence and data wiping (solid-state memory has the capacity for true one-button data destruction and/or wiping).

The continual upgrading of operating systems and file systems such as Microsoft Vista and Apple Leopard negatively affects the ability of the current tools to create forensics images, interpret the file system structure, and locate potential evidence. A case in point is Apple's HFS+ file system. Most current cyber forensics tools have problems creating accurate forensic images of HFS+ drives, and cannot interpret the structure in a manner that allows the investigator to visually examine the system. The current process requires the investigator to perform a string or keyword search on the raw data structure; a very time-consuming process.

Other issues include the data carving of multimedia files, dealing with large volumes of data (e.g. plus 1 TB storage, network area storage—NAS), multifile system devices (e.g. Intel Core 2 Duo using Windows NTFS and Apple HFS+), proprietary file systems on unique devices (e.g. cell phones), and virtualization (e.g. virtual computer images, fiber channel drives, cluster computing, and grids). This is obviously not an exhaustive list, but it illustrates the problems of keeping up with such a dynamic entity as technology. The more traditional forensics sciences are somewhat resistant to this problem as the elements they are concerned with are static (e.g. fingerprints, blood, and DNA).

### 3.3 Research and Scholarship

As was stated earlier, it is only recently that there has been formal and widely published research in the area of cyber forensics. If one examines the history and development of the other forensic sciences, it can be seen that their origin was derived from basic scientific research and development efforts. These fields tested the theories, which resulted in a body of research and the discovery that the methods, tests, results, and findings could be

extended to a forensic capacity; the science drove the forensics. This has not been the case with cyber forensics. The dearth of empirically sound research makes it difficult to defend the development of tools and techniques. Most tools currently in use and introduced before the courts are little better than black boxes whose internal structure, error rate, and true functionality are either unknown or if known by the vendor, not released to the community. (In some documented cases, the claims by the vendors were found to be incorrect and/or misleading.) Such glaring areas of uncertainty are unacceptable; especially when people's freedom if not their very lives may be hanging in the balance. The field of cyber forensics needs to reach out to the various scientific disciplines that comprise the field and formally develop a common body of scientific knowledge and basic theory. This corpus must then drive future development, testing and evaluation of hypotheses, processes, and tools.

A corollary to the late arrival of research is the problem of defining the scientific community for cyber forensics. As it currently stands, cyber forensics is an amalgam of various disciplines and is truly eclectic, with no one really owning the field. Adding to the problems is the reality that there are currently only a handful of what can be considered peer reviewed and refereed journals and conferences. In order for the discipline to mature scientifically, oversight by the scientific community is crucial.

As with anything related to research and scholarship, funding is very important. The newness of cyber forensics, coupled with its multidisciplinary nature has resulted in inadequate funding and confusion over which funding entity should have jurisdiction over the area. Is this a computer science problem, a legal justice problem, or a social science problem? It is anticipated that the government funding agencies will recognize that the answer to the preceding question is yes, it is all of these and thus funding needs to come from various sources. It is only through increased funding levels that research, development, and scholarship will continue.

### 3.4 Policies and Process

Tied to the issues of the lack of a unified CBK and changing technology is a lack of consensus on standard processes and procedures to follow. The field as a whole has shied away from checklists or even well-defined process models [5, 6, 17]. Although several models have recently been defined, none have become the "gold standard". In a field that is so dynamic, the development of anything more than principles and/or axioms may not be feasible. This has been readily apparent with the shift from dealing with static systems and devices to live analysis and acquisitions requiring the need for volatile memory examination while minimizing the degree of contamination [22].

Most organizations have yet to appreciate the importance of DE despite its ubiquitous nature in today's business environment. Notwithstanding some movement in recent years toward having standard policies related to information assurance and security, policies focusing on the capacity to conduct DE investigations are rarely found. It is speculated that the recent changes to the US Federal Rules of Civil Procedure specifically targeting ESI and discovery will prompt businesses and organization to be more proactive with their policies. [It is also anticipated that (ESI) discovery will result in systems that have a built-in forensics capability that will be embedded at the operating system or kernel level.]

### 3.5 Legal Requirements

Like other forensic sciences, cyber forensics must satisfy the courts that the procedures, processes, tools, and protocols are sufficient to allow for the admissibility of derived evidence [23].

A further legal hurdle in the United States is the ability of expert witnesses in area of cyber forensics to satisfy the federal and state admissibility requirements for novel scientific evidence. The current Federal Rules of Evidence (FRE) Section 702—*Daubert* considerations require that the tools, techniques, or procedures have been tested are generally accepted by the scientific community, have undergone peer review, and have a known or knowable error rate [24]. Although these four considerations are intended to assist judges (acting as gate keepers) in filtering out testimony based on pseudo or junk science, the field of cyber forensics as it currently stands is unable to satisfy any of the four criteria.

### 3.6 Critical Needs Analysis

Although cyber forensics tends to be discussed solely in the realm of criminal or civil investigations, it also plays a role in counterterrorism, critical infrastructure protection, and information warfare [18, 25]. Terrorist organizations, hostile foreign governments, and organized crime have all embraced technology as a tool to conduct business. Most industrialized countries depend on technology and the Internet for the smooth operation of their critical infrastructures (e.g. telecommunications, healthcare, banking and finance, power—hydroelectric and oil/gas, transportation). The ability to effectively and efficiently investigate and conduct a root cause analysis is paramount not only for law enforcement, but also for counterterrorism efforts. Several countries including the United States have included cyber terrorism and organized attacks against technology in discussions with weapons of mass destruction such as chemical, biological, and nuclear [26, 27]. Others consider attacks of this nature to be more along the lines of weapons of mass disruption and emphasize both direct and indirect impacts (e.g. disruption of first responder communications).

The view that technology will be used simply as a target or victim for terrorists is myopic at best. The terrorists (both foreign and domestic) and organized crime groups rely on technology such as computers and the Internet in order to communicate, gather intelligence, recruit followers, raise money, conduct marketing and propaganda, and conduct day-to-day business operations. The assumed anonymity fits perfectly into the shadow world of both terrorism and organized crime, and can make it difficult for counterterrorism efforts. In some cases, the lines between terrorists (both single cell and traditional organizations) and criminals have become very blurred. Organized crime groups operating in countries that formerly comprised the USSR are a hybrid of highly trained military and intelligence people, criminals, and arguably terrorists. It is artificial and naive to talk in terms of distinct and mutually exclusive categories when it comes to domestic and international deviant/criminal use of technology.

The best counterterrorism weapons include the gathering of timely intelligence and the transformation into meaningful information. The tools, processes, and technologies used for traditional digital investigations come into play here as well. Real-time data taps, the ability to pinpoint trends in large volumes of data, detecting and defeating crypto and steganography, data recovery, and source identification are all prime examples of the

synergy between computer forensics and counterterrorism/intelligence gathering. Open source and commercial developers are now starting to undertake development efforts that will extend the capabilities of their tools from traditional criminal or civil investigations to intelligence gathering, counterespionage, and counterterrorism.

## 4 RESEARCH DIRECTIONS

As was alluded to throughout the various sections, there are many areas that require further research in order to deal with both the current and near term issues and challenges. These are not necessarily relevant to digital investigations alone; solutions to these challenges will also assist in homeland security and counterterrorism efforts.

One of the biggest challenges is the ability to deal with large volumes of data. In the next few years, the storage capacity on servers and workstations is expected to surpass the multiterabyte range and potentially be in the petabyte range. Solutions to the issue of volume will likely be based on the commercial data mining approaches, but this will require more efficient algorithms, multiprocessing, and true multithreading. The use of cluster computing may also factor into the solution.

Closely related to the problem of the volume of data to search is the ability to search or carve data from the physical storage device, independent of the file system itself. Data carving for images (e.g. GIF, ART, JPEG, and BMP) is a common approach for most investigators today, but the current tools are inefficient, have issues with false positive rates, and cannot be extended to other multimedia formats such as MP4, MPEG, and Quicktime. Newer tools need to be developed that can identify files using more sophisticated file signature algorithms (e.g. fuzzy logic based and neural networks) and be more efficient and effective at carving multiple classes of file types, including multimedia.

As operating system developers/vendors are looking at implementing encrypted file systems, defeating encryption (crypt analysis) will be a real challenge. There is not much sense making a forensic image of a storage device, if the original is encrypted at the file system level. Solutions to this problem may need to leverage cluster computing to run brute force attacks against the encryption keys. Other solutions may look for backdoors, trapdoors, or flaws in the implementation of the encryption. (This is the current approach to defeating encrypted file systems.) These newer encrypted devices may also necessitate better methods for conducting live system analysis where the data is live and in clear text (i.e. nonencrypted).

The ability to forensically image and conduct a forensically sound analysis and examination of a live system and live memory is becoming more important today and will be even more critical in the future. This increase in importance is due to the phenomena of virtualizing storage and operating systems themselves. Virtual storage devices and the data they contain can be lost once a system is shutdown (e.g. fiber channel drives, and SAN). The size of random access memory (RAM) capacity on systems is exceeding 16 GB. The old method of pulling the power cord form the wall to turn a system off is now counterproductive as entire operating systems can be run in volatile memory. (To say, nothing of the paged data that is lost when the power is terminated.) Once shared RAM becomes more common, powering a suspect system off will be the exception as opposed to the norm.

Although these are a subset of the challenges facing the field, progress in any of these alone will greatly benefit investigative and homeland security efforts. The dynamic nature of technology will continue to be problematic for cyber forensics, but as long as the field is vigilant in its efforts at keeping an eye on the advances that are on the horizon, the problem is not insurmountable.

## 5 SUMMARY

The field of cyber forensics has become an important part of the general area of information assurance and security. Although cyber forensics is primarily focused on the identification, collection, analysis, and examination of DE, its tools can be extended to assist in counterterrorism and homeland security initiatives.

As our society becomes more and more dependent on technology, the ability to quickly and accurately deal with DE will become increasingly important. Despite the issues and challenges faced by this developing scientific area, cyber forensics is a crucial investigative tool in the fight against crime and terrorism.

## REFERENCES

1. Scientific Working Group on Digital Evidence. (2000). Digital evidence: standards and principles [Electronic Version]. *Forensic Sci. Commun.* **2**. Retrieved June 1, 2007, from http://www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm.
2. Palmer, G. L. (2002). Forensic analysis in the digital World [Electronic Version]. *Int. J. Digit. Evid.* **1**. Retrieved July 7, 2004, from http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action{=}issue&id=1.
3. Pollitt, M., and Shenoi, S. (2006). *Advances in Digital Forensics: IFIP International Conference on Digital Forensics*. National Center for Forensic Science, Orlando, FL, February 13-16, 2005, Springer, New York, [Great Britain].
4. Rogers, M. (2003). Computer forensics: science or fad? *Secur. Wire Dig.* **5**(55), 4–5.
5. Rogers, M. (2005). DCSA: digital crime scene analysis. In *Handbook of Information Security Management*, 5th ed., H. Tipton, and M. Krause, Eds. Auerbach, Dunedin, FL, pp. 601–614.
6. Beebe, N. L., and Clark, J. G. (2004). *A Hierarchical, Objectives-Based Framework for the Digital Investigations Process*. Digital Forensics Research Workshop (DFRWS), Baltimore, MD, p. 17. August 2004.
7. Reith, M., Carr, C., and Gunsch, G. (2002). An examination of digital forensic models. *Int. J. Digit. Evid.* **1**(3), 1–12.
8. Scientific Working Group on Digital Evidence. (2003). *SWGDE Draft Best Practices*. (June 5).
9. Rogers, M. (2006). *Introduction to Cyber Forensics—Lecture*. Purdue University, West Lafayette Indiana, IN.
10. Casey, E. (2000). Criminal profiling, computers, and the internet [Electronic Version]. *J. Behav. Profiling* **1**. Retrieved July 1, 2001, from http://www.law-forensic.com/computers_and_profiler.htm.
11. Icove, D. J., Seger, K. A., and VonStorch, W. R. (1995). *Computer Crime: A Crimefighter's Handbook*, 1st ed., O'Reilly & Associates, Sebastopol, CA.
12. Whitcomb, C. M. (2002). A historical perspective of digital evidence: a forensic scientist's view [Electronic Version]. *Int. J. Digit. Evid.* **1**. Retrieved July 1, 2003, from http://www.utica.

edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

13. Kruse, W. G., and Heiser, J. G. (2001). *Computer Forensics: Incident Response Essentials*. Addison-Wesley, Boston, MA.
14. Kovacich, G., and Boni, W. (2003). *High-Technology Crime Investigators Handbook*. Butterworth Heinemann, New York.
15. Marcella, A. J., and Greenfield, R. (2002). *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Auerbach, Boca Raton, FL.
16. Sommer, P. (1997). *Computer Forensics: An Introduction*, [cited 2003 June 3]; Available from: http://www.virtualcity.co.uk/vcaforensics.htm.
17. Carrier, E. H. S. B. (2003). Getting physical with the digital investigation process. *Int. J. Digit. Evid.* **2**(2), 20.
18. Workshop, D. F. R. (2001). A roadmap for digital forensic research. *First Digital Forensic Research Workshop*. DFRWS, Utica, NY.
19. Casey, E. (2004). *Digital Evidence and Computer Crime Forensic Science, Computers, and the Internet*, 2nd ed., Academic Press, Boston, MA.
20. Prosise, C., and Mandia, K. (2003). *Incident Response and Computer Forensics*, 2nd ed., Osborne, Berkeley, CA.
21. Rogers, M., and Seigfried, K. (2004). The future of computer forensics: a needs analysis survey. *Comput. Secur.* Spring, **23**(1), 12–16.
22. Feldman, J. E. (2005). *Collecting and Preserving Electronic Media [Electronic Version]*. Computer Forensics Retrieved August 1, 2007, from http://www.forensics.com/pdf/Collection.pdf.
23. Meyers, M., and Rogers, M. (2004). Computer forensics: the need standardization and certification [Electronic Version]. *Int. J. Digit. Evid.* **3**(2) Fall 2004, 3. Retrieved December 1, 2003, from http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=iisue&id=10.
24. Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 C.F.R. (1993).
25. Vacca, J. R. *Computer Forensics: Computer Crime Scene Investigation*. Charles River Media, Hingham, MA.
26. National Research Council. (2002). *Making The Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academy Press, Washington, DC.
27. Clinton, B. (1998). *Protecting America's Critical Infrastructures: PPD 63*. Retrieved. from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

## FURTHER READING

Casey, E. (2004). *Digital Evidence and Computer Crime Forensic Science, Computers, and the Internet*, 2nd ed., Elsevier, Boston, MA.

Digital Forensic Research Workshop. (2001). A roadmap for digital forensic research. Paper presented at the *First Digital Forensic Research Workshop*. Utica, NY.

Palmer, G. L. (2002). Forensic analysis in the digital world. [Electronic Version]. *Int. J. Digit. Evid.* **1**(1). Retrieved July 1, 2004 from http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=issue&id=1.

Reith, M., Carr, C., and Gunsch, G. (2002). An examination of digital forensic models. [Electronic Version]. *Int. J. Digit. Evid.* **1(3)**, 1–12. Retrieved July 1, 2004 from http://www.utica.edu/academic/institutes/ecii/ijde/articles.cfm?action=article&id=A04A40DC-A6F6-F2C1-98F94F16AF57232D.

Rogers, M. (2005). DCSA: digital crime scene analysis. In *Handbook of Information Security Management*, 7th ed. , H. Tipton, and M. Krause Eds. Auerbach, Dunedin, FL, pp. 601–614.

# CYBER SECURITY POLICY SPECIFICATION AND MANAGEMENT

SUSAN K. HINRICHS
*University of Illinois at Urbana-Champaign and Network Geographics, Inc., Champaign, Illinois*

## 1 INTRODUCTION

According to the Oxford English Dictionary, policy is defined as "a course or principle of action adopted or proposed by an organization or individual". The policy defines how things should be, but it does not get into the details of how that principle of action should be enforced. Consider an organizational policy that states that employees may not use e-mail for personal correspondence. The policy defines a general goal that will not change frequently, but how that goal gets enforced may change over time. Perhaps initially it is enforced by procedure. The employees are informed that they are not to use e-mail for personal use, and the system administrator periodically spot checks the e-mail queues for personal mail. The system administrator may later deploy a tool to automate the detection of personal mail. By separating policy from enforcing mechanism, the longer term goals and constraints driving the organization are clear. The enforcing mechanisms are then free to evolve over time to best enforce the policy goals. Most organizations today use these high level natural language policies to drive all aspects of their operation from human resources to financial practices to security. If the natural language security policy could be formalized, a computer program could use the policy to directly provision a security architecture and guide or validate its operation. This chapter discusses policy in greater detail and examines how formal policies have been used in several technology domains.

## 2 WHAT IS POLICY?

The term policy has been used in quite a few diverse projects and products over the years, making the term itself somewhat ambiguous. It is applied to both high level natural language policies and very low level statements that could also be seen as device configuration. In reality, policy is a continuum from the broad natural language guiding principles to the device-specific configurations. Morris Sloman's policy group at the Imperial College London has formalized the policy refinement hierarchy [1]. See Figure 1 for an example refinement hierarchy. The policy statements at the top of the hierarchy are very broad and too ill defined to be formally analyzed, but perhaps these policies are intuitively understandable to the executive responsible for setting the organization's policy. At each level of the refinement hierarchy, one formalizes some aspect of the policy, potentially creating multiple versions from the previous level, for example refining the policy for one site versus another or refining the policy for one technology (networking)

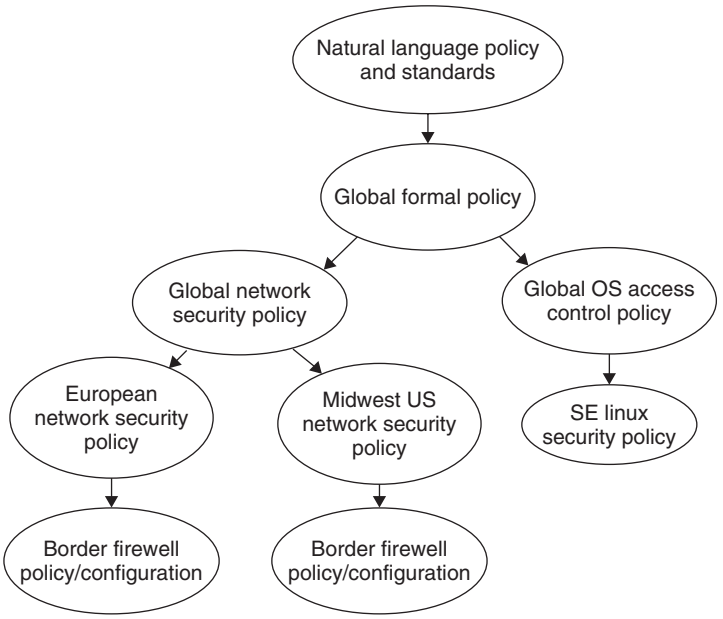



**FIGURE 1** Example of a policy refinement hierarchy. In this case the high level organizational policy is refined by technology area and then site.

versus another (operating system). At the lowest level of the refinement hierarchy is a policy that could be used to directly control enforcing devices. At the higher levels of the hierarchy, there are more general policies that could be used to direct global validation of a security implementation.

With a formal security policy, one can build tools to directly control the way security devices operate. Such a policy-based management tool can generate native configuration for the security device, or newer security devices can be developed that operate on the formal security policy directly. Most policy management tools can be mapped into the policy management architecture defined by the Internet Engineering Task Force (IETF) [2] shown in Figure 2. The policy enforcement point (PEP) is the mechanism that enforces the policy (e.g. a firewall device or an authentication system). The policy decision point (PDP) works on the policy to determine how the PEPs should operate. The PDP will also take input on restrictions specific to the environment like topology or maximum available resources to interpret the policy appropriately for the specific implementation. The PDP may generate the configuration for the PEP from the policy, or using a protocol like COPS [3], the PEP may query the PDP for operational guidance as needed.

By operating on a global policy, the system administrator can be freed from the details of the device-specific view and better keep the higher level goals of the policy in mind. The policy may describe goals that must be enforced by a set of devices, and the policy management tool can control and coordinate the operation of these enforcing devices. Even when operating at a device-specific level, the policy can shield the user from the necessary but infrequently changing vendor-specific details of the enforcing device.

If such a global policy-based management is not feasible, the presence of a formal high level policy can be beneficial for policy validation and compliance checking. The enforcing devices may be configured directly by different administrators, but a validation tool

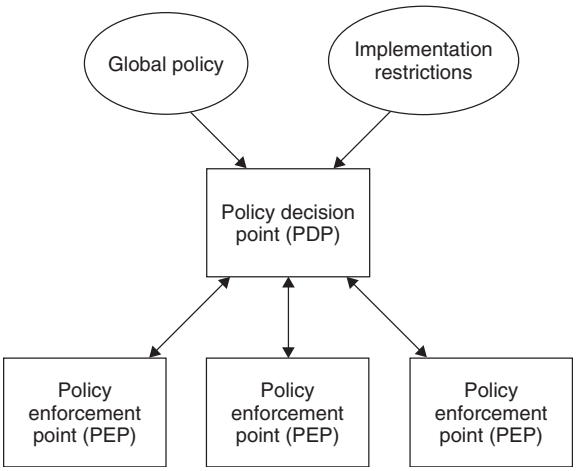



**FIGURE 2** The workflow of the policy management architecture suggested by the IETF. The policy management tool acts as the policy decision point (PDP). It operates on the formal policy and a set of implementation restrictions to create device-specific operational information used by the policy enforcement points (PEPs).

could use the formal high level policy to drive validation of the current implementation. Figure 3 shows the flow of such a policy-based validation tool. The administrator may have a new version of the device configuration. Before deployment the new configuration can be evaluated against sets of policy-based constraints to ensure that the configuration changes do not violate policy. Auditors may also use policy-based constraints to test whether the policy specifications of the client match their deployed configurations.

### 2.1 Conflict Resolution

One issue that appears with all nontrivial formal policy systems is that of conflict resolution. In any real environment, there are conflicting policies that guide operation. An organization may want to provide a easy to use web interface to encourage new customers, but the organization must also ensure that their infrastructure has sufficient authentication and auditing to avoid fraudulent customers. These two goals are necessarily conflicting. At the implementation level, one group may require HTTP communication with a particular server, but another group may need to prohibit all communication with that server to avoid potential conflict of interest contamination.

The policy language could force the user to clarify all conflicts through ordered lists or policy priorities, and this is the approach taken with most currently deployed policy tools. While this approach is straightforward to implement, it pushes complexity back onto the user. Some early firewall devices tried to use "best match" languages to eliminate conflicts between firewall rules, but the meaning of "best match" was either vague or did not always match the user's expectations. More recent work with autonomic network management [4] adds a ratification policy to enable the administrator of a specific system to describe how conflicting policies should be resolved. For example, some aspects of the high level policy may not apply in the particular environment (e.g. Windows policies in a Linux environment). The ratification policies are meta policies that are defined against the operation of other policies rather than the operation of the managed devices.

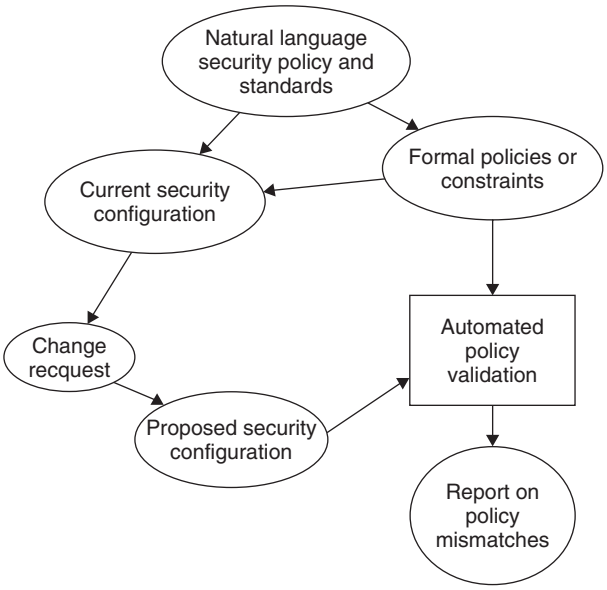



**FIGURE 3** The workflow of a policy validation tool. It takes a formal policy description and a proposed enforcing device configuration. The policy validation tool builds a model of the new configuration and determines whether there are mismatches between the formal policy and the new operational model.

## 2.2 A Policy Example

To make this policy definition discussion more concrete, consider the following broad organizational security policy.

> Partners should only be given access to a specific set of partner servers and only necessary communication protocols should be permitted. Partner traffic must be appropriately authenticated and encrypted.

This policy can be refined into a network security policy that describes where traffic can flow and where it must be encrypted. Ultimately, this formal security policy will direct the provisioning of the appropriate enforcing devices (firewalls, intrusion protection systems, tunnel routers, etc.). The broad organizational security policy can also be refined into a set of policies that define allowable cryptographic algorithms and parameters for the IPSec tunnels. This policy set will be used at run time to negotiate mutually agreeable tunnel parameters for the organization and its partners.

For this example, assume there are more specific natural language policies and standards which enumerate the partner IP networks and internal partner services addresses. The standards also state that the protocols HTTP and secure shell (SSH) are necessary for partner communication and declare that the deep inspection or state-full analysis performed by most of today's enterprise firewalls is sufficient for the broader policy's analysis requirements.

The system administrators can create and maintain configurations for the security enforcing devices directly from the natural language policies and standards. However, as the environment changes, the human mapping between the natural language security

policies and the real configurations may diverge, particularly when dealing with change requests for other policy goals that have unintended consequences. Consider the following scenario.

The system administrator is told to give FTP access to the sensitive document repository machine to machines from network 192.168.1.0/24. Say the configuration writer accidentally mistyped the mask so access was allowed from 192.168.1.0/23. If 192.168.0.0/24 was a partner network, this seemingly unrelated change causes a conflict between the security implementation and the policy on partner communication.

In this scenario the supposedly unrelated changes will affect how the security policy with respect to partner communication will be implemented. It is unlikely in reviewing these unrelated change, the IT personnel will think to check for policy requirements that "should not" be affected by the current change. This error may not be caught until the next audit cycle. In the meantime, some partners have access to a sensitive internal machine that is not indicated by policy.

## 3 PROVISIONING POLICY TOOLS

In the example partner policy, a formal network security policy can be used to provision or validate the network enforcing devices. The formal policy directs a relatively static set of rules for resource allocation or access control. The configuration can be generated from a single policy or a set of policies that can be resolved at configuration or provisioning time. In contrast, other systems can delay policy resolution until runtime via a negotiation protocol. This section discusses tools developed for manipulating provisioning policies.

### 3.1 Network Security Policy Tools

Although the specifics of network security vendor configuration languages differ, they all configure operations on the same basic packet model, which is *"specify a packet and describe what happens to it"*. Thus, it is possible to parse configurations and place the functional configuration information into a common network security model. Guttman [5] first described a technique for parsing router access control lists (ACLs) and building a packet flow model. Others [6, 7] have followed up on this work to parse in network configurations and build higher level packet handling modules. This work provides the basis for a wide variety of network security management and validation tools.

### 3.2 Network Security Policy Management

A number of commercial and research groups have developed network security management tools that present a common security management model and generate the appropriate device-specific configuration to implement the desired model. The architecture of these tools map into the general IETF policy management architecture shown in Figure 2. Cisco Secure Policy Manager [8] and Solsoft [9] both present a global policy model. The user defines the network architecture and identifies the location of the configurable security enforcing devices in that architecture as the implementation restrictions, and he then defines a global policy of desired traffic flows, tunnels, and so on. The management tool acts as the PDP and generates the appropriate configurations for the enforcing points to enforce the global policy.

Some management tools present a rule table interface and use a variety of multi-assignment techniques to share policy rules to multiple enforcing devices, for example Checkpoint, NetScreen Security Manager, Cisco Firewall MC, and Cisco Security Manager. In the research space Bartel et al. [7] created Firmato, a toolkit for creating management tools for different vendors' devices.

Presenting the security implementor with a higher level policy-based management model is a good solution to keep security policy and implementation in sync. By raising the security implementor up a level of abstraction and enabling him to express his requirements globally, he is working at a level closer to the natural language security policies. However, for a variety of technical and social reasons these policy-driven configuration generation solutions have not gained wide acceptance in the network security domain.

In general, the problem with the policy-driven configuration is that it is an all-or-nothing solution. Some aspects of the configuration may map very well to the high level policy, but perhaps other aspects of the configuration are easily done by someone with expertise in the configuration language. Some people in the organization may be comfortable working with the policy language, but others are more comfortable with the command line. In general it is hard to have a configuration that is sometimes configured from policy generation and sometimes through direct human editing [10], because the changes at the lower level may not consistently map into the model at the higher abstraction layer.

### 3.3 Network Security Policy Validation

Today organizations rely on a combination of manual configuration review and network scanning to ensure that configuration changes to the network security implementation are still consistent with the guiding security policy. In many organizations, network security changes are only allowed within a particular change window each week. No configuration change can be deployed until it has been reviewed by the key IT staff with the hope that multiple eyes will catch potential problems.

Many organizations also use network traffic scanners such as *nmap* and *nessus* to probe the newly deployed configuration to ensure that only the expected traffic is passed. Based on the guiding security policy the IT staff can determine what and where to scan and review the scanning logs to see if there are any surprises. Generally, the scanning checks are made after the configuration changes are deployed in the production network. If the changes are extreme or an organization is very security conscious, they may deploy the changes in a similar network in an isolated lab and perform the scans in the lab before deploying the changes on the production network.

Although these solutions catch many potential problems, it is desirable to have a more precise understanding of how the network will behave once the proposed changes deployed without going through the trouble of setting up a separate lab or opening up the organization to a potential vulnerability window on their production network. A number of groups have started to look at configuration validation in addition to direct management. Such validation tools fit into the workflow as shown in Figure 3. Al-Shaer and Hamed [11] and Wool [12] have cataloged sets of possible conflicts that arise in today's common linearly ordered access lists. Al-Shaer and Hamed and a number of commercial products (e.g. Netscreen and Cisco Firewall MC) have tools to perform rule conflict analysis which examines access lists or rule lists and presents conflicts within

the lists. This conflict analysis identifies rules within the same list that could be matched by the same packet. Some conflicts will occur in most ordered access lists, because there are narrow permit rules followed by broader deny rules, but the conflicts are a good place to focus a configuration review. Typos and other development errors will result in unexpected conflicts as indicated in the example error scenario for the partner policy.

Mayer et al. [13] have developed a firewall analyzer that augments the Firmato query engine to generate an exhaustive report of how all possible packets will be handled by a device configured with a specific configuration. This exhaustive report removes any ambiguity from trying to understand how the packets will be processed. This report can be performed without actually configuring the device or passing any traffic. The user can then review the report to understand how any particular packet will be processed.

InfoSecter [14] is another tool that addresses the network security policy validation. In addition to identifying conflicts between rules within the same configuration, it evaluates a configuration against a set of formal policy constraints which are written as conditions that test packet attributes (e.g. source and destination address, and service) and specify desired actions. The condition describes how sets of packets should be treated in the operational environment. The constraint analysis compares the policy constraint against the processing model built from the proposed device configuration and determines if there are sets of packets where the configuration model and the policy constraint differ on the specified action (e.g. permit, encrypt, proxy, or deny). In the case of the FTP configuration change described in the example policy section, the constraint analysis would catch the mismatch with existing policy and alert the IT staff before the proposed configuration is even deployed.

Multiple policy constraints can be defined, and there is no need to specify ordering or other conflict resolution for the policy constraints as would be needed for policy management. This is beneficial when multiple groups of people have policy concerns about the operation of a specific PEP. Consider a firewall that is managed by the IT team. Traffic to the accounting team and the engineering team passes through this device, and each team has its own unique policy concerns. As the firewall configuration evolves, the accounting and engineering teams could independently run their own reviews and scans on each newly deployed change to the firewall, but this would require too much time and expertise on the part of the nonprovisioning teams. Instead, by encoding their concerns in formal policy constraints, the IT team could automatically check their policy constraints on each proposed new configuration.

### 3.4 Operating System Policy Tools

Operating systems that provide mandatory access control (MAC) use policy to define the access rules. The MAC rules are not embedded in the representation of the objects (files) or subjects (processes). The Bell LaPadula MAC policy [15] that is implemented by most multilevel systems does not present a configurable policy. Rather, the administrator can adjust security levels of the subjects and objects to change access control decisions, but the rules or policy against which these levels are evaluated is fixed. However, the type enforcement MAC policy used by SELinux [16] is directly configured by the system administrator. This gives the system administrator a great deal of freedom to implement almost any MAC model, but the policy can grow to be very complex with this increased expressibility.

SEEdit developed by Hitachi provides a graphical interface to edit the SELinux type enforcement policy on a device. It attempts to address the policy creation and management complexity by providing the policy writer with a higher level view of the type enforcement policy. The editor also presents information about common building blocks and macros used to create the policy.

The SELinux type enforcement language provides a basic validation mechanism in the form of the neverallow statement. With this statement, the policy writer can assert that a particular subject (or domain) should never have the specified access to a particular object (or type). For example, the policy writer may want to specify that the guest user should never gain direct access to the objects of type system configuration.

Tresys has created Apol to provide higher level analysis of the type enforcement policy. Apol gives the user the ability to query the policy to determine the allowed information flow, for example which subjects can access which objects. One problem with this and similar higher level SELinux policy analysis tools is that they operate on the raw policy. The policy writer is working with a policy that refers to M4 macros in an attempt to have some form of modularity and reusability. The types that are presented by Apol may have been generated by one of the M4 macros and so are not directly meaningful to the policy writer.

MulVal [17] is a tool that validates access control policy against a formal model built from system configuration. The tool builds a system model from operating system access control information, known system vulnerabilities, and network connectivity. With this formal system model, MulVAL validates whether a formal system policy is accurately enforced. The paper describes results against a network of Red Hat linux devices. The tool was later applied to networks of well-managed Windows devices and revealed numerous exploitable access control flaws. Thus, by defining the system in terms of global access control via policy, the tool was able to take care of the details of validation in a rather complex system.

## 4 CONTRACTUAL OR NEGOTIATING POLICY

Another style of policy has been developed, which does not require configuration time resolution. Rather the infrastructure is aware of the policy and the system entities introduce policies which are resolved at runtime as needed. The policies are like contracts, and the infrastructure provides negotiation protocols to resolve conflicts at run time. The IPSec policy of acceptable cryptographic parameters from the partner example is a very simple example of such a contractual policy.

The Security Assertion Markup Language (SAML) [18] is a more sophisticated example of this type of policy. With SAML statements a user can coordinate between one identify provider and one or more service providers. The service providers can share an identity proof assuming they trust the identify provider. The SAML statements coordinate this sharing. Thus the user can sign on once and pass his validated identity to multiple service providers (that all trust the identity provider).

Similarly the web services security policy (WS-Policy) [19] is a language of assertions which are used to control the run time operation of the web services security infrastructure. For example, a user of a web service may have an associated WS-Policy statement that indicates that he wants to use at least 128 AES encryption with communicating with

a service. The Web Server may have an associated policy that places restrictions on what it needs to be convinced of a user's identity.

In the research space, trust negotiation has been breaking new ground in implementing policy constraints on identity proofs [20]. It is desirable to initiate communication with entities that the user has not previously directly registered with, for example a shopper. The shopper may want some proof that the shopping site is legitimate. Similarly, the shopping site wants to know that the shopper has a good credit rating. The shopper may hold some certificates that show he has a valid credit card and a good credit rating. The shopping site may have certificates that show it is in good standing with the better business bureau. Some of the certificates may be sensitive, and the entities may not want to exchange all certificates up front. Trust negotiation gives a framework for a controlled exchange of information. Policies describe what each entity needs to know to trust the other side. Policies also control how much information an entity is willing to reveal about himself and to whom.

## 5 SUMMARY

Without a strong tie between an organization's high level policy and their operational stance organization is very likely to have a mismatch between policy and operation at some point. This mismatch will expose the organization to insecure states, e.g., too much access, too weak encryption, or too little authentication. By introducing formal policies to fill out the policy refinement hierarchy, one can deploy tools to automatically tie policy to operations via policy management or policy validation. By relying on tools and infrastructures to automatically control devices from policy, an organization has a more direct path from organizational policy to operation. Changes at a more abstract policy level are easier to reconcile with an organization's goals and guiding constraints.

Policy-aware technologies still face many technical hurdles. Accurate and usable conflict resolution will continue to be a difficult problem. The conflict resolution sophistication continues to grow with the evolution of the ratification policies and constraint systems (borrowing technology from artificial intelligence (AI) and type systems). The more dynamic environments of negotiating policies will present even greater problems in reasoning about all possible ways a policy can be enforced.

The benefits of using policy to direct and validate system operation will drive the resolution of these technical hurdles. The computer is well-suited to keeping track of the details in a formal model, and the policy-driven program is less likely to introduce errors (via typos or mismatches between devices) than direct human operation would introduce. As our systems become more complex and control more critical functions, the need for policy driven systems becomes even more important to operate secure and reliable systems.

## REFERENCES

1. Bandara, A., Lupu, E., Russo, A., Dulay, N., Sloman, M. Flegkas, P., Charalambides, M., and Pavlou, G. (2005). Policy Refinement for DiffServ Quality of Service Management. *Proceedings 9th IEEE/IFIP International Symposium on Integrated Network Management (IM 2005). Nice, France, May, pp. 469–482*. DOI 10.1109/INM.2005.1440817.

2. Yavatkar, R., Pendarakis, D., and Guerin, R. (2000). *A Framework for Policy-based Admission Control*. Internet Engineering Task Force RFC 2753. January.
3. Durham, D., Boyle, J., Cohen, R., Herzog, S., Rajan, R., and Sastry, A. (2000). *The COPS (Common Open Policy Service) Protocol*. Internet Engineering Task Force RFC 2748. January.
4. Agrawal, D., Calo, S., Giles, J., Lee, K.-W., and Verma, D. (2005). Policy Management for Networked Systems and Applications. *Proceedings of IFIP/IEEE International Symposium on Integrated Network Management (IM 2005). Nice, France, pp. 455–468*. DOI 10.1109/INM.2005.1440816.
5. Guttman, J. D. (1997). Filtering Postures: local enforcement for global policies. *IEEE Security and Privacy Symposium. Oakland, CA, pp. 120–129*. DOI 10.1109/SECPRI.1997.601327.
6. Al-Shaer, E., Hamed, H., Boutaba, R., and Hasan, M. (2005). Conflict Classification and analysis of distributed firwall policies. *IEEE J. Sel. Areas Commun.* **23**(10), 2069–2084. DOI 10.1109/JSAC.2005.854119.
7. Bartal, Y., Mayer, A., Nissim, K., and Wool, A. (2004). Firmato: A novel firewall management toolkit. *ACM Trans. Comput. Syst.* **22**(4), 381–420.
8. Hinrichs, S. (1999). Policy-Based Management: Bridging the Gap. *Proceedings of the 15th Annual Security Applications Conference, IEEE. Phoenix, AZ, December*, pp. 209–208. DOI 10.1109/CSAC.1999.816030.
9. Advice on Enterprise policy Management for Security and Compliance. http://www.exaprotect.com/globals/gating.php?gateparams=YTo1OntzOjE6InQiO3M6NTc6li9maWxlcy9nYXRIL3dwLWFkdmljZS1vbi1lbnRIcnByaXNILXBvbGIjeS1tYW5hZ2VtZW50LnBkZil7czoxOiJmljtzOjE5OilvcmVzb3VyY2VzL2dhdGUucGhwljtzOjE6lmQiO3M6NjY6lkFkdmljZSBvbiBFbnRIcnByaXNIIFBvbGIjeSBNYW5hZ2VtZW50IGZvciBTZWN1cml0eSBhbmQgQ29tcGxpYW5jZSI7czoxOiJ1IjtzOjEyOiJ1c2VyIGRIZmluZWQiO3M6MToicCI7czoyMzoiL3Jlc291cmNIcy9wb3N0Z2F0ZS5waHAiO30%3D.
10. Hinrichs, S. (2005). Integrating Changes to a Hierarchical Policy Model. *Proceedings of 9th IFIP/IEEE International Symposium on Integrated Network Management, IEEE. Nice, France, May*, pp. 441–454. DOI 10.1109/INM.2005.1440815.
11. Al-Shaer, E., and Hamed, H. (2006). Taxonomy of Conflicts in Network Security Policies. *IEEE Commun. Mag.* **44**(3), 134–141. DOI 10.1109/MCOM.2006.1607877.
12. Wool, A. (2004). A quantitative study of firewall configuration errors. *IEEE Comput.* **37**(6), 62–67. DOI 10.1109/MC.2004.2.
13. Mayer, A., Wool, A., and Ziskind, E. (2006). Offline firewall analysis. *Int. J. Inf. Secur.* **5**(3), 125–144.
14. (2007). *Consistent Security Policy in a Changing World. Network Geographics white paper*. http://network-geographics.com/static/policy-validation.pdf.
15. Bell, D., and LaPadula, L. (1973). *Secure Computer Systems: Mathematical Foundations*. Technical Report MTR-2547. Vol I. MITRE Corporation, Bedford, MA. March.
16. Loscocco, P., and Smalley, S. (2001). Meeting Critical Security Objectives with Security-Enhanced Linux. *Proceedings of the 2001 Ottawa Linux Symposium*, http://www.nsa.gov/selinux/info/docs.cfm.
17. Ou, X., Govindavajhala, S., and Appel, A. (2005). MulVAL: A Logic-based Network Security Analyzer. *Proceedings of the 14$^{th}$ Usenix Security Symposium*, Baltimore.
18. Madsen, P., and Maler, E. (2005). *SAML V2.0 Executive Overview. OASIS SSTC Committee Draft∼sstc-saml-exec-overview-2.0-cd-01*. April.
19. Bajaj, S., Box, D., Chappel, D., Curbera, F., Daniels, G., Hallam-Baker, P., Hondo, M., Kaler, C., Langworthy, D., Nadalin, A., Nagaratnam, N., Prafullchandra, H., von Riegen, C., Roth, D., Schlimmer, J., Sharp, C., Shewchuk, J., Vadamuthu, A., Yalcinalp, U., and Orchard, D. (2006). *Web Service Policy 1.2 –Framework (WS-Policy)*. W3C Member Submission. April.

20. Lee, A. J., and Winslett, M. (2006). Safety and Consistency in Policy-Based Authorization Systems. *The 13th ACM Conference on Computer and Communications Security (CCS 2006)* Alexandria, VA. *October/November*.

## FURTHER READING

Peltier, T. R. (2004). *Information Security Policies, Procedures, and Standards: a practitioner's reference*. Auerbach Publications, A good overview of natural language security policies and standards. Auerbach Publications, Boca Raton, FL.

Verma, D. C. (2001). *Policy-Based Networking: Architecture and Algorithms*, New Riders. An overview of the IETF-based policy management framework, and a discussion of the technology used to create policy management frameworks in the network domain, Indianapolis.

# MULTILEVEL SECURITY

CYNTHIA E. IRVINE
*Naval Postgraduate School, Monterey, California*

## 1 INTRODUCTION

Multilevel security (MLS) refers to policies and techniques where the sensitivity of the information is immutably bound to an equivalence class. (One can think of *equivalence classes* as subsets of a set where there is no overlap or intersection among the subsets. For example, pens could be subdivided into red pens, blue pens, black pens, green pens, and so on. Information might be subdivided into *CRITICAL* and *NONCRITICAL* information or *PUBLIC* or *PROPRIETARY* information.) The active entities that access the information are also statically associated with equivalence classes. On the basis of the relationships between the equivalence classes, rules determine whether and with what rights an active entity can access the information. The mandatory policies associated with MLS can apply to integrity as well as confidentiality. Specific models and mechanisms have been developed to support MLS in computer systems. Requirements for multilevel secure systems span the private sector, the government, and the military.

## 2 BACKGROUND

Most organizations maintain information that is either protected or openly available. In government, information often is categorized as either classified or unclassified. Within

the context of classified information, various levels of information sensitivity may be established based upon the damage caused should that information become accessible to adversaries. The more grievous the damage resulting from unauthorized access, the more sensitive the information. For example, the recipe for Uncle Joe's secret sauce may be considered critical to the continued well being of a producer of barbeque sauce: it must neither be revealed to competitors, nor should be corrupted by changing the proportions of the ingredients. Physical documents containing sensitive information are protected through a variety of physical and procedural controls. Computer systems introduce new challenges.

Throughout the 1960s, as multiprocessing computer systems evolved, it became evident that the separation provided by the resource management mechanisms of typical operating systems was insufficient to prevent highly sensitive information from becoming accessible to unauthorized individuals. These controls were so inadequate that instead of utilizing the power of multiprocessing, classified information processing was conducted separately. At times, this meant that those with classified tasks had to wait until after hours, when the system could be dedicated to processing the sensitive information. Following the completion of the classified tasks, the system was purged of all sensitive information and restored to unclassified activity. This is what is called *periods processing*. If the amount of classified processing merited the additional expense, a *dedicated system* might be allocated to sensitive tasks.

Both these approaches were insufficient to meet the requirements of organizations that depended upon rapid access to information for military command and control. Periods processing could result in unacceptable delays and dedicated systems incurred both the expense of additional equipment and a high cost of ownership in terms of system maintenance and support personnel. If simultaneous processing at several classification levels, such as *CONFIDENTIAL*, *SECRET*, and *TOP SECRET*, was required, then the resources for either periods processing or dedicated systems could be inadequate. In addition, these approaches could be wasteful if the computing resources allocated to particular classification levels were underutilized.

In organizations where access to a broad spectrum of information is required for making informed decisions, the temporal and spatial separation of information with various sensitivities afforded by periods processing and dedicated systems was more than inconvenient: it could mean the difference between victory and defeat, life or death. Those at the management level wanted computer systems that would mimic the kind of access to information possible when using physical documents: timely simultaneous access to both classified and unclassified information, by properly authorized individuals.

MLS addresses these requirements. To understand MLS, it is necessary to understand the nature of the policies to be enforced, the challenges associated with enforcement of those policies in automated systems, how multilevel systems and networks are implemented, current approaches to MLS systems, and emerging technologies for MLS systems.

## 3 MULTILEVEL SECURITY POLICIES

Security policies are embodied in the laws, procedures, and rules used to manage and protect information. In general, policies reflect an organization's requirements for information confidentiality, integrity, and availability. MLS is applicable to both confidentiality and integrity policies. An organization may use labels to associate a particular

sensitivity level with particular piece of information, and people are vetted for access to sensitive information through checks that result in some form of authorization. For example, extensive and costly background checks are required to vet individuals as sufficiently trustworthy to merit access to *TOP-SECRET* information. Individuals lacking appropriate authorization will be unable to access any sensitive information, whereas those with many or high authorizations have access not only to nonsensitive information but also to highly sensitive information. MAC policies are policies that are both global in scope and persistent in time; users cannot override the policy during normal use. Sometimes mandatory policies are called *nondiscretionary* policies; the two terms are equivalent. In contrast, *discretionary access control* policies permit modification of the rules pertaining to access to information: a run-time interface is provided through which properly authorized users may modify policy. Consequently, it is up to the discretion of the individual to determine who will have access to information. A test for determining whether a policy is mandatory or discretionary is to examine the punishment associated with its violation [1]. Disclosure of state secrets can result in prison or firing squads, whereas violation of discretionary policy may only result in a reprimand.

*Sensitivity levels* are identifiers for equivalence classes of information and are based upon the secrecy and integrity attributes of the information. The choice of equivalence classes is up to the organization. For a private enterprise, the sensitivity levels might be *PROPRIETARY* and *PUBLIC*, whereas a military organization might choose *SECRET*, *CONFIDENTIAL*, and *UNCLASSIFIED*. Consider a few examples.

In a large company, only personnel in the *PRODUCT-RESEARCH* group may have access to *PRODUCT-RESEARCH* information, whereas only personnel in *CORPORATE-STRATEGY* group may access the *CORPORATE-STRATEGY* for next year. Information on the company web pages is *PUBLIC* and is readable by anyone, although the company is likely to restrict write access to its webmasters and system administrators. Management determines the membership of the respective groups. Lipner provided a discussion of the applicability of MAC policies in the commercial sector [2] and concluded that a very large number of labels would be required when many enterprises were involved. Military organizations may organize classified information into *TOP SECRET*, *SECRET*, and *CONFIDENTIAL* levels, and all nonsensitive information is *UNCLASSIFIED*. Individuals are given background checks and are assigned clearances such as *TOP SECRET* and *SECRET*.

There may be a hierarchical relationship between the major equivalence classes. For example, a user cleared for *TOP SECRET* is able to access *TOP SECRET*, *SECRET*, and *UNCLASSIFIED* information. In the corporate example, everyone in *PRODUCT-RESEARCH* may be allowed to access both *SHIPPING* and *PUBLIC*. Often an organization may impose further granularity on its access controls by imposing a mandatory *need-to-know* policy. Additional metadata is associated with both subjects and objects to reflect mandatory need-to-know policies. For example, an individual cleared for *TOP SECRET* may be vetted for access to information that is in special compartments such as *Imagery Intelligence* (*IMINT*), *Signals Intelligence* (*SIGINT*), and *Human Intelligence* (*HUMINT*). Such labels are commonly used by the intelligence community where the work of analysts is compartmented so that individuals have access only to the information required to do their job. These mandatory policies reflect a requirement to enforce the notion of least privilege [3]. Figure 1 shows both a hierarchical ordering of access classes and classes created from combinations of noncomparable attributes. For a mandatory confidentiality policy, information is allowed

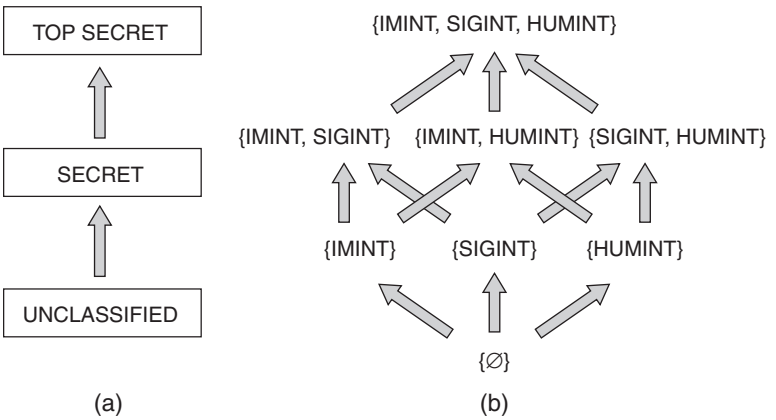



**FIGURE 1** A hierarchical ordering of classes is shown in (a). In (b), a set of noncomparable classes is depicted. Arrows show the allowed direction of information flow.

to flow from lower classification levels or combinations to higher ones. In the latter, any classes may receive information from classes with attributes that are a subset of its own.

A common misconception is that MLS applies only to the enforcement of mandatory confidentiality policies. MLS may also be used to enforce mandatory integrity policies. The semantics of integrity are as follows. If information is of high integrity, then it must not be corrupted by low integrity information. However, adding high integrity information to low integrity information does no harm, although there is no real improvement unless the low integrity information is somehow cleaned up. For example, the Royal Observatory at Greenwich, England, is a reliable and high integrity source for astronomical time, while an amateur sundial might be a relatively low integrity time source. Thus high integrity information should be readable by everyone, whereas low integrity information should be confined and readable within quarantine-like processes. Note that processing of high integrity information by low integrity software, whether being executed by a high integrity process or not, lowers the integrity of that information [4].

The sensitivity labels form a set of equivalence classes that can be organized according to the information flow intended in the system. Denning showed that these equivalence classes can be represented mathematically with respect to the flow of information via read and write operations [5]. This work demonstrated that all mandatory policies could be simply combined and that the resulting sensitivity classes could be easily compared with one another.

For both the corporate and the military examples, the policy regarding access to information is inflexible with respect to location. Even though the corporation may have offices across the world, only *PRODUCT-RESEARCH* group personnel may handle *PRODUCT-RESEARCH*; and, analogously, military access to *TOP-SECRET* information requires a *TOP-SECRET* clearance regardless of the location. These policies are also temporally inflexible. Information marked as *PRODUCT-RESEARCH* does not become *PUBLIC* at certain times of the week while it is marked *PRODUCT-RESEARCH* the rest of the time, just as the classification of information designated *TOP SECRET* does not become *UNCLASSIFIED* just for the weekends. Thus, we say that mandatory policies are *global* and *persistent*.

The global nature of MAC policies does not dictate that all components of a multilevel system, whether individual machines or elements of a highly distributed network, must enforce all policies. The system may be organized so certain components only process information at a single classification level and need not be required to enforce mandatory policy. Such components are *single level*.

In practice, certain information once highly classified may after some time be downgraded and released to the public. Certain situations may require the rapid *regrading* of selected intelligence information so that it is available to operational personnel. This might occur during military operations or in disasters involving first responders who are typically not cleared for access to sensitive information. Similarly low integrity information may be analyzed and judged qualified for use in a high integrity context. For example, integrity regrading might take place in the creation of software for a manned space mission. Initially, the software might be labeled *DEVELOPMENT*, but following proper analysis, it could be upgraded to *MANNED_FLIGHT*. These examples illustrate that the notion of persistence is not absolutely rigid; however, the processes used to regrade information, whether procedural or automated, must be carefully controlled.

Two techniques are commonly used to enforce mandatory policies. The first is physical and the second, logical. Enforcement of mandatory policies in a context without computers involves only individuals and documents. Individuals who have been properly vetted to handle sensitive documents are trusted to ensure that the sensitive information contained in those documents is not transferred to documents with inappropriate sensitivity markings. Organizations go to great lengths to ensure that corrupted insiders or spies do not cause the release of sensitive information. Physical protection can ensure that sensitive information is accessible only within confined spaces. Locks and guards ensure that only authorized individuals enter the sensitive enclave, and logging of entry and exit to the space as well as check-in and check-out of information while in the space deter malicious insiders. Special construction methods may protect the enclave from eavesdropping technologies.

Because an *organizational security policy* may be stated in very general terms, its translation to a form that can be implemented in computer systems results in an *automated security policy* [6]. This articulation of the policy permits access to information to be described in terms of the active and passive entities of the system. Ultimately this translates to execution of an instruction by the CPU that accesses resources managed by the system.

The active system entities, *subjects*, access information contained in passive entities, *objects*. Subjects are not the cleared individuals themselves, but generally are processes that execute software [7]. Subjects are surrogates for users who may be either administrators or normal users. The mechanism that implements and enforces the MAC policy exports subjects and objects at its interface. The enforcement mechanism binds a sensitivity level, either implicitly or explicitly, to each subject and object.

### 3.1 Confinement

In the world external to computers, individuals use their judgment to ensure that only authorized individuals have access to information. Subjects within a computer are programs in execution. Programs do not exercise judgment and thus may violate the intended policy if they are programmed to do so. An example of this problem is a *Trojan Horse*, that is, clandestine malicious software placed within an application. While the user

innocently uses the application, the Trojan Horse abuses the user's privileges to cause unauthorized information flow so that it may be accessed by unauthorized individuals.

To better appreciate the Trojan Horse problem, consider a system that enforces a discretionary policy using access control lists (ACLs). Each process has a binding to the individual upon whose behalf it is running, and a separate ACL is associated with each file and directory. Each ACL contains a list of individuals and their access rights to the object.

Suppose that Alice has *PRODUCT-RESEARCH* information in the file called *research-stuff* and that the ACL on *research-stuff* allows read and write access only to Alice and Bob, who are both members of the *PRODUCT-RESEARCH* team. Elmo is in the shipping department and has a file called *shipping-stuff* with an ACL that allows anyone in the company to have read and write access to it. In theory, Alice could use her computer to read information out of *research-stuff* and write it into *shipping-stuff*, but Alice is a good employee and would not do this. What Alice does not know is that her program, *research-SW*, contains a Trojan Horse. While she uses *research-SW* in the normal course of her job, it is clandestinely writing *PRODUCT-RESEARCH* information to Elmo's file, as illustrated in Figure 2. Elmo, a corporate spy, will sell this information to competitors who are stealing the intellectual property of Alice's company in order to dominate the marketplace. Of course, since a system enforcing discretionary access controls has a run-time application programming interface that may change the policy, it is possible that the Trojan Horse in research-SW might change the ACL on research-stuff, thereby allowing direct read by Elmo. However, the first approach is somewhat preferred as it is less likely to be detected by an auditing mechanism.

Integrity Trojan Horses are also possible. In this case, an integrity Trojan Horse would write to a high integrity object. An example of an integrity attack might be modification of critical avionics information on a commercial aircraft.

In an automated system, the mandatory policies can be enforced in a way that will prevent Trojan Horses from causing unauthorized information flows. Thus, unlike the world of people with judgment and paper, that of subjects and objects is constrained by rules that thwart attempts to violate policy.

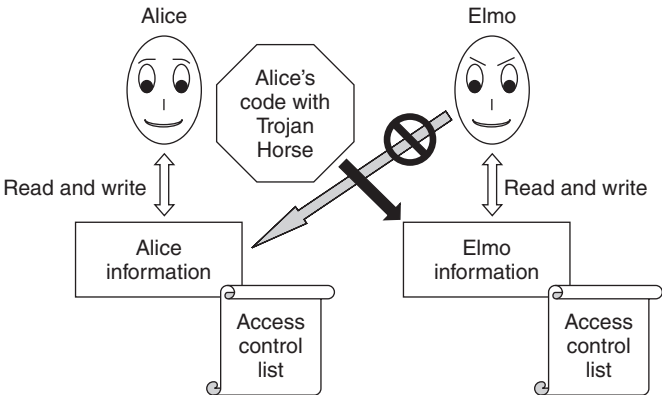



**FIGURE 2** A Trojan Horse executing in Alice's code is able to write to Elmo's information, thus circumventing Alice's intent to block Elmo's read access to her information.

Users set their session level before starting work on an MLS system. This sets the label on any subjects that will act on behalf of the user. Normally these subjects are single level. The systems' objects possess immutable labels indicating a single sensitivity level. Subjects may have access to objects with labels different from their session levels, but in the case of confidentiality they are neither authorized to read from objects that are more sensitive, nor permitted to write to objects less sensitive than the current session level. The former rule reflects the laws and practices imposed in the world of people and paper, whereas the latter is imposed specifically to prevent either accidental or malicious flow of information from high to low sensitivity. This is called *confinement*, and in formal security policy models is called the *confinement-property* (also called the **-property*) [8]. The rules for enforcement of integrity policies have an opposite symmetry. Subjects are permitted to read information of higher integrity and to write to low integrity objects, but they may not read low integrity information or write to higher integrity objects.

Mathematical models allow precise articulation of the properties to be enforced when mandatory policies are required. The Bell and LaPadula model [9] provides a formal representation of a mandatory confidentiality policy and the Biba model describes a mandatory integrity policy [9]. Figures 3 and 4 illustrate the rules of the Bell and LaPadula and Biba models, respectively.

The SeaView model was the first to illustrate that a single set of equivalence classes could be used to enforce combined secrecy, integrity, and least privilege policies in a system with mandatory controls [10]. The least privilege policy, implemented using protection rings [11], addressed process-internal integrity. Extensions to this work have been presented in the context of multilevel secure smart cards [12].

### 3.2 Supporting Policies

In an operational system, there must be a binding between the real user and the subjects acting on behalf of the user [3]. First, a user must be identified to the system, and then the user must be authenticated to the system by presenting something that only come from that user. This might involve a password, token, biometric factor, or some combination of these.

Once logged in, the user must set a session level. To accomplish this, the password file might be augmented to contain the maximum sensitivity level, such as a clearance,

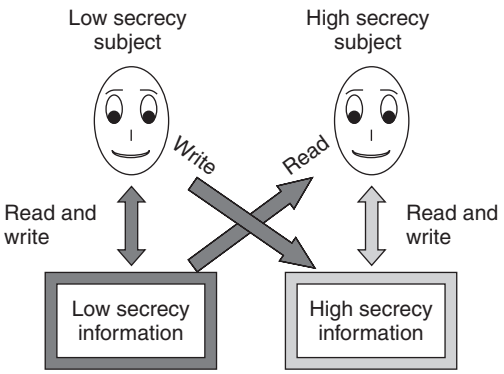



**FIGURE 3** High confidentiality subjects have read access to low confidentiality information; at the same time mandatory policy prohibits the flow of high information to low.

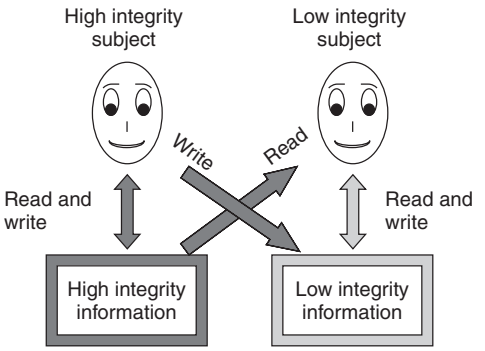



**FIGURE 4** Mandatory integrity policies prevent corruption of high integrity information by low integrity subjects, while low integrity domains benefit from high integrity information.

at which the user can work. Although this maximum sensitivity level might be possible, users may wish to work at lower levels and must select a *session level*. For example, Jane, who is cleared to *TOP SECRET*, could select any one of the following session levels for her current session: *TOP SECRET*, *SECRET*, or *UNCLASSIFIED*. Suppose the user logs on at *SECRET*, then, when a subject is instantiated on behalf of the user, one of its attributes will be the user's current session level, for example, *SECRET*.

The implementation of an identification and authentication policy requires a *trusted path*. The idea behind the trusted path is that the user is trustworthy, as is the identification and authentication mechanism. So, both the system and the users require an unforgeable connection that assures the user protected communication with the trusted system that communication is with the user and not a man-in-the-middle or some other malicious entity. Users invoke the trusted path using a *secure attention key*: a single key or some special combination of keys designated solely for the purpose of establishing a trusted path.

Since the attributes bound to subjects acting on behalf of users are the basis for access control decisions, it is clear that a well-defined identification and authentication policy is essential for multilevel systems.

Audit provides a record of security-relevant events. If bound to a rule-checking mechanism, audit may provide alerts of impending security violations. Policies must be established to determine what should be audited. For example, one might choose to audit all accesses to a particular object, but to no others; all activity on the system could be audited; the activities' subjects at a particular sensitivity level might be recorded; the use of selected system calls could be audited; and so forth. It is important to audit the activities of the security administrator and other trusted individuals so that a record of security-critical activities can be maintained. Also, good audit reduction tools are needed, otherwise voluminous audit records are not likely to be particularly useful.

In systems enforcing mandatory policies, the management of labels and the labeling of information being transferred into and out of the system should be reflected in supporting policies. For example, there may be a requirement that all printed documents contain markings in their headers and footers indicating whether the document is CORPORATE-STRATEGY or PUBLIC.

System support is also required for the enforcement of administrative policies, such as user account management and security configuration, including the configuration of mandatory sensitivity levels.

### 3.3 Trusted Subjects

To perform many of the tasks associated with supporting policies as well as to provide functionality such as regrading, systems enforcing MLS must support subjects that have the ability to both read and write to a label range that spans multiple sensitivity levels [13]. Trusted subjects do not violate the MLS policy, but are explicitly part of the system and adhere to a relaxed MLS policy. To ensure that the information flows resulting from the actions of trusted subjects are not in violation of the intent of the overall system policy, the code executed by these subjects must be analyzed for possible incorrect or malicious execution. As a result of this analysis, we can say that they are trustworthy [14]. A challenge associated with the design and analysis of trusted subjects has been the modeling of their correct behavior [15].

Trusted subjects execute at the login interface to allow each user to set a session level and create untrusted, single-level subjects at that session level. They are also used by security administrators to set the levels associated with single-level devices. For multilevel devices where the sensitivity level of incoming or outgoing information can require the use of explicit sensitivity labels, trusted subjects ensure that correct label-to-information bindings occur. Another service performed by trusted subjects is in regrading information. Many organizations enforce mandatory policies; however, operationally, they also require mechanisms where exceptions to these policies may be implemented. For example, consider a system that encrypts information before transmitting it on the network. The process of encryption can transform bits that represent proprietary sensitive information into bits that represent no information and, thus, can be seen by anyone. In essence, encryption is *downgrading* the information, viz., changing its sensitivity level from high to low. Modern systems may require additional downgrading functions that move certain information from high networks or repositories to low ones. A downgrader or *guard* will consist of a trusted subject that is able to read information from a high sensitivity level, for example, TOP SECRET, and write that information to an object at a lower sensitivity level, for example, SECRET.

Sometimes sensitive information is scanned for certain critical words that are then expunged from the data. This is called *sanitization*. A danger in downgrading systems is *steganography* [16]. Steganography, the art of hidden writing, involves a secret encoded by malicious code in seemingly innocuous data so that it is not visible to the casual observer. Clearly, filtering and regrading must be conducted using systems for which there is a very high confidence that only the correct actions will be taken.

Note that in the regrading example given above, the labels on the subjects and objects are immutable. A trusted subject does not change the label of the object, but rather reads the information from the source object and writes it to a destination object that has a different sensitivity level. This is an example of *tranquility*. Because of its lower complexity, label tranquility for both subjects and objects has been considered to be an essential aspect of highly trustworthy implementations of MLS policies.

The construction of *trusted systems* represents one of the great challenges in security modeling and engineering. Underlying operating system controls are used to enforce mandatory policies on its processes and, at the same time, permit *trusted* applications to be subject to relaxed mandatory constraints.

## 4 ENFORCEMENT OF MULTILEVEL SECURITY POLICIES

When constructing an MLS system, several approaches are possible. Threats will determine system requirements, which include those that specify functionality and those that determine its trustworthiness.

### 4.1 Design Approaches

To enforce policy using physical mechanisms, one must construct a separate single-level network for each sensitivity level. All users must be authorized for the sensitivity level of the network and all information created and managed in that network must be considered to be at the network's sensitivity level. The advantages of single-level systems or networks include the ability to identify and manage the access to information in a manner that is easy to understand. An isolated network may be maintained in a special facility and only authorized users may be granted access to the premises. Although costly, extremely critical information may warrant the protection afforded by isolated networks and systems.

In the case of physically isolated systems, users must either move from room to room to access different networks or they may have multiple systems on the desktop. The latter can lead to clutter and confusion. The user could use a keyboard, video, mouse (KVM) switch to minimize consumption of desktop space; however, multiple processors are still required and the possible advantage of simultaneously seeing information at different sensitivity levels is lost.

If nonsensitive information can be moved to networks of higher sensitivity, but without a highly trustworthy binding of sensitivity labels associated to the information, the users cannot distinguish nonsensitive from sensitive information. Also, to share nonsensitive information with individuals having lesser authorizations, users must go back to the nonsensitive system. If a user wishes to transmit nonsensitive information directly from the more sensitive enclave, complex procedures including automated guards are required, and the possibility of steganography [16] and other techniques for clandestine information hiding must be addressed.

Logical isolation depends upon an underlying mechanism that enforces the security policy. Because mandatory policies can always be characterized by comparisons between equivalence classes, it is possible to construct a relatively simple mechanism to determine whether a particular subject may have access to a given object. Systems that enforce logical isolation can provide users with a coherent view of all information at or below their sensitivity level. They also allow users to log into the system at any sensitivity level at or below their maximum authorization or clearance. Thus, from a single system, an authorized user is able to both access company proprietary information when logged in at *PROPRIETARY* and the Internet when logged in at the *PUBLIC* sensitivity level.

### 4.2 Threats to MLS Systems

The critical nature of information to be protected in MLS systems requires that threats to correct policy enforcement be carefully examined before system development. This

allows requirements to be elicited that will ensure threats are eliminated as part of a carefully articulated system life cycle process.

Threat analysis reveals that there are two broad classes of threats: *developmental threats* and *operational threats* [17]. Developmental threats include the introduction of flaws into the system through mistakes in design and implementation and through deliberate system subversion. The former introduces exploitable flaws, whereas the latter introduces trapdoors.

Operational threats occur when the system is in use. Adversaries can include malicious insiders as well as external activities. The mechanisms that have been designed into the system are intended to counter operational threats; however, system security also depends upon adequate user and administrator training, as well as good configuration management and system maintenance. Constructive techniques counter developmental threats, and systems must be designed and implemented so that operational threats are addressed.

A large number of failures in policy enforcement result from the presence of unspecified functionality in systems, for example, vulnerabilities in the form of system flaws and unintended artifacts that permit an adversary to bypass the policy enforcement mechanism of a system. These failures in design and implementation can be exploited by adversaries intent on gaining system privileges for the purpose of avoiding the constraints of the protection mechanism. Flaws range from inadequate bounds checking of interface parameters to pathological interactions between synchronizing processes. Such flaws were identified by Anderson in 1972 [18] and are still common. The Common Vulnerabilities and Exposures [19] website lists thousands of unique entries. A few of the major categories of flaws derived from Linde [20] and Anderson [18] are provided in Table 1.

The most insidious form of unspecified functionality is subversion [21], where a member of the system's development team intentionally adds clandestine functionality that permits the adversary to bypass system security mechanisms. The term *subversion* is generally applied to the operating system or kernel, whereas other forms of malicious

**TABLE 1 Examples of Errors Resulting in Security Flaws**

| General Error Category | Example |
|---|---|
| System design errors | Absence of least privilege |
| | Inappropriate mechanism for shared objects |
| | Poor choice of data types |
| Design errors | Error recovery results in exploitable side effects |
| | System modifications that deviate original intent of security mechanisms |
| Implementation errors | Buffers sizes are not checked, resulting in "buffer overflow" |
| | Failure to initialize variables |
| | Absent parameters are erroneously assumed |
| User interface errors | Gratuitous active execution |
| | Passwords too short |
| | Default access control lists are too permissive |
| Configuration errors | Insecure defaults render the system vulnerable |
| | Critical resources remain unprotected because of bad configuration choices |

software, for example, Trojan Horses, function in the context of applications. Karger and Schell [22] suggested a subversion in which a compiler could insert an artifice into an operating system. This concern regarding untrustworthy tools was popularized by Thompson [23].

A subversion mechanism executing within the operating system has full system privileges and is unconstrained by policy enforcement mechanisms. If it contains triggers for activation and deactivation, the adversary will have control over its execution.

In many cases, malicious code may be introduced into systems in the form of downloadable executables or scripts, updates, and patches. Code of unknown provenance should be given an integrity label such as *POND-SCUM* and be confined using mandatory integrity controls thus preventing the infliction of pervasive damage.

### 4.3 Assurance

As is the case with security, assurance is a term that is often misused. For example, some state that "software assurance" will improve the "security" of systems. Both these terms are meaningless without context. In the case of software assurance, some might say that a system possesses this quality if it functions as specified and if various tests indicate that the software behaves as expected over a set of inputs, but this definition assumes no malicious intent in the construction of the system. If, on the other hand, one assumes a malicious adversary, then assurance means correct policy enforcement in the face of sophisticated attacks.

The critical nature of the information processed within multilevel secure systems requires assurance through a carefully chosen combination of environmental and technical measures.

Given a particular security policy, an organization may seek more or less assurance that the policy is correctly enforced. For example, greater assurance might be required to show that only authorized individuals have access to trade secrets, whereas less assurance might be required for the protection of the agenda for the next staff meeting. Barriers to achieving high assurance multilevel secure systems include product development pressures that can lead to shortcuts and specious claims. For example, a vendor may claim to have a "secret" technique that makes a system secure, but close inspection by knowledgeable reviewers usually reveals serious flaws [17, 22]. (Such "secret" techniques often involve a combination of cryptography and handwaving.) It is generally accepted that an objective third party must provide an independent assessment of system assurance. The current framework for third party evaluation of system assurance is that of the Common Criteria [24], which provides for high-level requirements for various classes of security products. Through analysis and testing, product team evaluators establish that the product meets both functional and assurance security requirements. A second round of testing and analysis by independent evaluators validates the team's results.

### 4.4 Secure MLS System Development

Over time, a set of design principles that can guide the development of highly secure systems has emerged [14]. These principles take traditional constructive methods into account, as well as recent advances in hardware and networking.

A secure system should exhibit all of the characteristics of a classic *reference monitor* [17]: resistance to tamper, continuous policy enforcement, and an understandable implementation.

Dependencies are of great importance in designing a secure system. If the system is organized as a set of hierarchical layers, then it must be organized so that each layer of the system depends only upon layers that are of equal or higher assurance and that enforce equivalent or stronger policies. The number and extent of the layers depend upon whether the mandatory policy is void or richly populated, but it is important that mandatory policy enforcement mechanisms do not depend upon discretionary, viz., modifiable, policy components.

Once the system architecture has been delineated and policy has been allocated to its various layers, it is possible to focus on the construction of each layer. Here, the techniques used to develop a high assurance, low-level layer are sketched.

To start, a formal security policy model is developed. The model provides a proof that if the system starts in a secure state, then all operations will maintain that secure state [8, 9]. The formal model serves two important purposes: first, it demonstrates that the intended policy is logically self-consistent and not flawed, and second, it provides a mathematical description of the system to which the implementation can be mapped. The objective of this mapping is to demonstrate that everything in the implementation is both necessary and sufficient for the enforcement of the policy and that no unspecified functionality is present.

Because the objective in constructing the lowest layers of the system is to develop a coherent mechanism for the enforcement of the system's MLS policy, a combination of hardware and software is used to create the exported abstract machine. Rigorous security engineering techniques employing the concepts of layering, modularity, and data hiding ensure that the system has a coherent loop-free design and provides understandable abstractions. Within the system itself, the principle of least privilege can be applied as part of the engineering process. Ultimately, both the formal and informal efforts provide a mapping of the implementation to the formal security policy model as well as evidence that the system is correct and complete.

Although testing cannot prove that a system is secure, it can lessen the likelihood of obvious flaws. Traditional testing demonstrates that each function and module performs as specified. At the system level, this is supplemented by penetration testing. Here, the tester behaves as an adversary and attempts to abuse the system interfaces in an unexpected manner. A useful approach to penetration testing is the *flaw hypothesis methodology* [20].

System administrators and users must be provided with documentation and training. If a system with useful security mechanisms is configured and used improperly, a false sense of security may result that may have consequences far worse than if management believed security was inadequate.

Thorough documentation of the development process is needed so that the system can be assessed with respect to its security requirements by third party evaluators. To date, no viable alternative to either the reference monitor concept or the need for third party evaluation has been proposed. Future research may result in more streamlined approaches to secure system construction and assessment.

### 4.5 Covert Channels

A multilevel secure system is designed to export resources, including subjects and objects, at its interface and to actively mediate information flows between its exported subjects. Rules enforced by the MLS system will ensure that unauthorized flows do not occur as a result of interactions among exported resources; however, design measures must ensure

unintended information flows do not occur via covert channels [25] among elements internal to the policy enforcement mechanism.

Covert channels result from the manipulation of system interfaces in ways that cause unintended information flow and result from incomplete resource virtualization by the underlying protection mechanism. This means that some abstract data type presented at the system interface involves operating system constructs that can be manipulated to allow signaling to take place in violation of the system security policy.

An effective technique for covert channel analysis is the shared-resource matrix method [26]. Using this technique, the effects of each system call on operating system-level data structures are analyzed and their visibility, perhaps through exceptions or timing delays, to other processes is identified. When the effects could result in unintended transmission of information, either a system flaw or a covert channel is present.

Covert channels may take one of two forms: *storage channels* and *timing channels* (e.g. [27]). In the case of the former, a resource such as secondary memory is incompletely virtualized so that effects and exceptions viewed by the receiver can be manipulated by the sender. This causality permits the sender to signal a sequence of effects and exceptions, which may be interpreted as a series of 1s and 0s by the receiver, thus creating a binary channel. The bandwidth of the channel will depend upon the speed with which the sender can manipulate the observables for the sender. Complete elimination of covert storage channels is possible for classic monolithic single-processor systems. Multicore processors present new challenges to covert channel mitigation. Covert timing channels result from the ability of the sender to modulate the temporal activities of the system as seen by the sender. Because time is a shared resource that cannot be completely virtualized by the underlying security mechanism, requirements may only call for a reduction of the channel bandwidth below a certain threshold. This can prove challenging, as increases in processor speed can dramatically increase the bandwidth of a covert timing channel, and timing channel reduction may result in imprecise knowledge of system time, significant loss in overall performance, or both [28]. Careful configuration and scheduling can mitigate timing channels; their complete elimination has yet to be demonstrated in useful systems. If covert channel analysis is an objective, then the design and implementation framework and development methodology for the target system must ensure that adequate information for this analysis is available.

Another form of information leakage is via *side channels*. In this case, information leakage is not internal, but is possible through monitoring of external observables (e.g. [29]). Side channels are possible in any system intended to protect some secret, such as encryption key, from external observation.

### 4.6 Object Reuse Considerations

Objects, the information containers in systems, are constructed using system resources, usually primary and secondary memory, but devices must also be considered. When objects are deleted, the memory from which they were constructed is returned to a pool. To prevent inadvertent access to information previously stored in deleted objects, an object reuse mechanism is needed that will remove information from resources before their reuse. The system implementation determines whether the information is purged immediately after object deletion or before its allocation to a new object.

### 4.7 Target Environment

The requirements levied upon a multilevel system usually depend upon the conditions within which it is intended to operate. As a result, there are several *operational modes*.

*System high* operation requires that all users be cleared to the highest sensitivity level and all information is stored at the system high sensitivity level. Any labels are only advisory and a review is required to downgrade information for use in a less sensitive system. Physical controls commensurate with the highest sensitivity of information within the system are used to isolate the system and grant users physical access to it.

In a *compartmented mode* system, all information is treated to be at the highest sensitivity level. Users must be vetted to not disclose information on the system. Formal compartments subdivide the information and users are granted formal access to those compartments on a need-to-know basis. Information to be moved out of the system to lower sensitivity levels must be submitted to a review and downgrading process. Physical controls commensurate with the highest sensitivity of information within the system are used to both isolate the system and to control physical access to it.

A *multilevel mode* system permits information at more than one sensitivity level to be processed within the system for which users do not have authorizations to access all information on the system.

Multilevel mode does not imply that all sensitivity levels must be processed by the system, nor does it imply support for a full range of user authorizations. The range of information sensitivity levels and the range of user clearances will be dictated by the assurance of correct policy enforcement that the system provides. For example, in 1985, even with the highest assurance systems of the time, the risk was considered too high to permit the minimum clearance of users to be UNCLASSIFIED and the maximum sensitivity of data on a system to be TOP SECRET with multiple compartments [30].

### 4.8 Cascade Problem

Organizations may wish to link several MLS systems into a network. When doing so, it is necessary to consider the assurance characteristics of the interconnected components.

Consider two systems that have been certified to have sufficient assurance to separate two sensitivity levels. System A can process TOP-SECRET and SECRET information, and System B can process SECRET and CONFIDENTIAL information. As stand-alone systems, we are satisfied that although some information flow might occur, they will not be particularly damaging due to the small range in sensitivity levels being managed by the system. Now suppose that the systems are networked together so that the SECRET domain of System A is connected to the SECRET domain of System B, as shown in Figure 5. In this configuration, information might inadvertently flow from TOP SECRET to CONFIDENTIAL. This could pose an intolerable risk. The interconnection introduces an information flow cascade [31]. Because of the complexity of finding and correcting cascades, networks should be carefully designed to avoid the cascade problem from the outset.

## 5 PLATFORMS AND ARCHITECTURES FOR MULTILEVEL SECURITY

All multilevel secure systems must provide separation of the information equivalence classes derived from policy, enforcement of rules for interaction between the equivalence

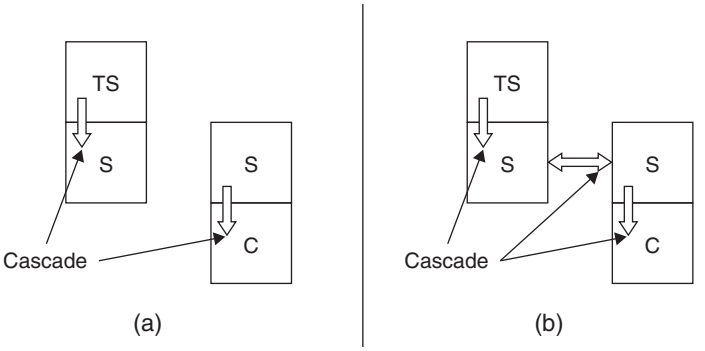



**FIGURE 5** Systems in (a) have sufficient assurance to address information flow between two equivalence classes. By interconnecting the same systems, as shown in (b), the assurance is insufficient with respect to flows between three equivalence classes, and an unacceptable cascade results.

classes, a mechanism to map the equivalence classes to human readable labels, and assurance that the system is complete and correct. Because enforcement of supporting policies, for example, identification and authentication and audit, would complicate the minimal kernel, an MLS system is usually organized as a *trusted computing base* (TCB) of which the kernel is a part. Figure 6 is a simplistic illustration of a kernel within a TCB.

Current approaches to multilevel secure platforms include classic security kernels [32] and separation kernels [33]. In the former, an internal policy module mediates access based upon the rules established for the equivalence classes it maintains. Information exported to networks will have either implicit labels, in the case of single-level networks, or explicit labels associated with each packet, in the case of multilevel networks. In these kernels, each process will be assigned either a single level or will be trusted over some range of labels. When combined with the use of ring-based privilege domains [11], traditional security kernels provide considerable granularity for information flow control.

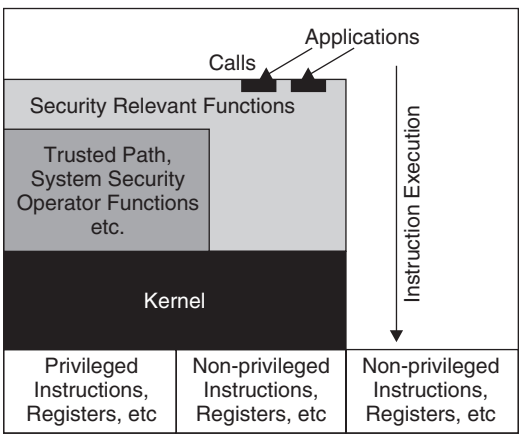



**FIGURE 6** A trusted computing base encompasses all security-relevant functionality and may contain a kernel.

Traditional security kernels dynamically allocate resources as different sensitivity levels are required.

A separation kernel creates partitions to which it exports resources based upon assignments loaded into the kernel in the form of a configuration table. Once the configuration is loaded, the sensitivity levels to be managed are fixed until a new configuration is applied, which in conservative cases requires a system restart [34]. Each partition represents an equivalence class, and an interpartition flow policy determines how subjects within a partition can cause flows to other partitions. These kernels are sometimes called *partitioning kernels* or *multiple independent levels of security* (MILS) architecture kernels, for example [35]. For these kernels, enforcement of the interpartition flow policy is allocated to a partition that has read and write access to all other partitions and contains a trusted subject to mediate and effect the interpartition flows.

Least privilege separation kernels [36] provide higher granularity with regard to flows than is present in MILS separation kernels. By combining a more granular configuration table with the use of hardware-supported rings and the ability to create many subjects per equivalence class, a least privilege separation kernel does not need a special partition for interpartition communication, but can create trusted partitions for other functions as needed.

The distinct advantages and disadvantages of each type of kernel should be considered when selecting a kernel to meet specific requirements [37].

Requirements exist for architectures that support heterogeneously trusted users, for example, [38]. Blacker was an early example of a multilevel secure network [39]. In essence, it was an MLS virtual private network (VPN) and was designed to provide both the platform assurance and cryptographic mechanisms required for highly distributed host-to-host communication. Various other solutions have been adopted as well. In system high and compartmented environments, workstations of low or medium assurance provide multilevel functionality, but do little to address the subversion threat. The cost is a specialized workstation for each user. Certain high assurance MLS systems can be used in distributed environments and a major vendor once developed a high assurance MLS virtual machine monitor (VMM), although the product was never released. Recent progress in VMMs has led to a resurgence of interest in their use for MLS.

Architectures that combine the use of popular commodity office productivity applications with components for high assurance of policy enforcement are possible [40]. This approach results in a network architecture that depends upon the use of high assurance multilevel components for servers as well as high assurance elements to support a distributed trusted path and for label enforcement at single-level network connections. An alternative approach uses many microarchitectural elements [41].

### 5.1 Use of Applications in MLS Systems

A challenge facing the developers of MLS systems has been the design of applications able to take advantage of the system's underlying multilevel technology. To avoid requiring every application to be a trusted subject, applications must be organized to execute as multilevel-aware untrusted single-level subjects that can easily read and write to objects as allowed by policy.

Early work in this area involved the design of a multilevel file system intended to provide applications with a complete set of file system features while constrained by

an underlying security kernel [42]. Subsequent work [43] has demonstrated that a wide variety of applications can be made multilevel aware.

User acceptability is often a problem for operational MLS systems. The rules to constrain Trojan Horses and other malicious software do not exist in the world of people and paper. A person cleared for TOP SECRET can hand write an UNCLASSIFIED memo without clearing the desk of all classified information. Typical users do not understand why the rules for automated MLS security policies exist and merely conclude that those developing MLS do not trust them. Others seek alternative solutions with relaxed rules or "vendor magic", which can endanger highly sensitive information.

## 6 CONCLUSION

Multilevel secure systems are required when heterogeneously trusted users must access information resources. They can be used to protect information from unauthorized disclosure and unauthorized modification of information. Although the challenges associated with the design and development of highly trustworthy multilevel secure systems have been understood since the late 1960s, their implementation and use have remained elusive. Consequently, many organizations adopt architectures comprising multiple single-level networks for which timely access to information at different sensitivity levels is often difficult or impossible. Challenges to the use of MLS systems include their proportionately higher cost relative to commodity products, user acceptability of the policy enforcement rules, and modern platform architectures that introduce opportunity for the existence and exploitation of high-bandwidth covert channels.

## REFERENCES

1. Brinkley, D. L., and Schell, R. R. (1995). Concepts and terminology for computer security. In *Information Security: An Integrated Collection of Essays*, M. Abrams, S. Jajodia, H. Podell, Eds. IEEE Computer Society Press, Los Alamitos, CA, pp. 40–47.
2. Lipner, S. (1982). Non-discretionary controls for commercial applications. In *Proceedings of the 1982 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Los Alamitos, CA, pp. 2–20.
3. Saltzer, J. H., and Schroeder, M. D. (1975). The protection of information in computer systems. *Proc. IEEE* **63**(9), 1278–1308.
4. Irvine, C. E., and Levin, T. (2002). A cautionary note regarding the data integrity capacity of certain secure systems. In *Integrity, Internal Control and Security in Information Systems*, M. Gertz, E. Guldentops, L. Strous, Eds. Kluwer Academic Publishers, Norwell, MA, pp. 3–25.
5. Denning, D. E. (1976). A lattice model of secure information flow. *Commun. ACM* **19**(5), 236–243.
6. Sterne, D. F. (1991). On the buzzword "security policy". In *Proceedings of the IEEE Symposium on Research in Security and Privacy*, IEEE Computer Society Press, Los Alamitos, CA, pp. 219–230.
7. Lampson, B. W. (1971). Protection. In *Fifth Princeton Conference on Information Sciences and Systems*, pp. 437–443; Reprinted in ACM SIGOPS *Oper. Syst. Rev.* **8**(1), 18–24.
8. Bell, D. E., and La Padula, L. (1973). *Secure Computer Systems: Mathematical Foundations and Model*, (Tech. Rep. No. M74–244). MITRE Corp, Bedford, MA.

9. Biba, K. J. (1977). *Integrity Considerations for Secure Computer Systems*, (Tech. Rep. No. ESD-TR-76-372). MITRE Corp, Bedford, MA.
10. Lunt, T. F., Neumann, P. G., Denning, D. E., Schell, R. R., Heckman, M., and Shockley, W. R. (1989). *Secure Distributed Data Views Security Policy and Interpretation for DMBS for a Class A1 DBMS (RADC-TR-89-313*, Vol **1**), Rome Air Development Center, Griffiss Air Force Base, NY.
11. Schroeder, M. D., and Saltzer, J. H. (1972). A hardware architecture for implementing protection rings. *Commun. ACM* **15**(3), 157–170.
12. Schellhorn, G., Reif, W., Schairer, A., Karger, P., Austel, V., and Toll, D. (2000). Verification of a formal security model for multiapplicative smart cards. *Proceedings of the 6th European Symposium on Research in Computer Security (ESORICS 2000)*, Lecture Notes in Computer Science Vol. 1895, Springer-Verlag, pp. 17–36.
13. Landauer, J., Redmond, T., and Benzel, T. (1989). Formal policies for trusted processes. *Proceedings of the Computer Security Foundations Workshop II*, IEEE Computer Society Press, Los Alamitos, CA, pp. 31–40.
14. Levin, T. E., Irvine, C. E., Benzel, T. V., Bhaskara, G., Clark, P. C., and Nguyen, T. D. (2007). *Design Principles and Guidelines for Security*, NPS-CS-08-001, Naval Postgraduate School, Monterey, CA.
15. Benzel, T., and Tavilla, D. (1985). Trusted software verification: a case study. In *Proceedings of the 1985 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Los Alamitos, CA, pp. 14–31.
16. Kurak, C., and McHugh, J. (1992). A cautionary note on image downgrading. In *Proceedings of the Eighth Annual Computer Security Applications Conference*, IEEE Computer Society Press, Los Alamitos, CA, pp. 153–159.
17. Irvine, C. E., Levin, T., Wilson, J. D., Shifflett, D., and Pereira, B. (2002). An approach to security requirements engineering for a high assurance system. *Requirements Eng.* **7**(4), 192–208.
18. Anderson, J. P. (1972). *Computer Security Technology Planning Study*, (Tech. Rep. ESD-TR-73-51, Vols. 1 and 2, NTIS Document No. AD758206). Air Force Electronic Systems Division, Hanscom Air Force Base, Hanscom, MA.
19. MITRE Corp (2007). *Common Vulnerabilities and Exposures*, Last Accessed 22 August 2007 http://www.cve.mitre.org/.
20. Linde, R. R. (1975). Operating system penetration. In *Proceedings of the National Computer Conference*, AFIPS Press, Montvale, NJ, pp. 36–368.
21. Anderson, E. A., Irvine, C. E., and Schell, R. R. (2004). Subversion as a threat in information warfare. *J. Inf. Warf.* **3**(2), 52–65.
22. Karger, P. A., and Schell, R. R. (1974). *Multics security evaluation: Vulnerability analysis.* Hanscom Air Force Base, Information Systems Technology Application Office Deputy for Command and Management Systems Electronic Systems Division (AFSC), Bedford, MA.
23. Thompson, K. (1984). Reflections on trusting trust. *Commun. ACM* **27**(8), 761–763.
24. ISO/IEC (2004). *Common Criteria for Information Technology Security Evaluation*, (Rep. No. CCIMB-2004-01-001, Ver. 2.2, Rev. 256). International Organization for Standardisation, Geneva, Switzerland.
25. Lampson, B. W. (1973). A note on the confinement problem. *Commun. ACM* **16**(10), 613–615.
26. Kemmerer, R. (1982). A practical approach to identifying storage and timing channels. In *Proceedings of the IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Los Alamitos, CA, pp. 66–73.

27. Levin, T., and Clark, P. C. (2004). A note regarding covert channels. In *Proceedings of the Sixth Workshop on Computer Security Education*, Naval Postgraduate School, Monterey, CA, pp. 11–15.
28. Hu, W. (1992). Lattice scheduling and covert channels. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, IEEE Computer Society Press, Los Alamitos, CA, pp. 52–61.
29. Kocher, P. C. (1996). Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems. In *Advances in Cryptology—CRYPTO'96, Lecture Notes in Computer Science*, Springer-Verlag, Vol. 1109, pp. 104–113.
30. Department of Defense (1985b). *Technical Rationale Behind csc-std-03-85: Computer Security Requirements –Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments*, June, US Government Printing Office, Washington, DC. URL: http://csrc.nist.gov/publications/secpubs/rainbow/std004.txt.
31. Millen, J. (1988). The cascading problem for interconnected networks. In *Proceedings of the Fourth Aerospace Computer Security Applications Conference*, IEEE Computer Society Press, Los Alamitos, CA, pp. 269–273.
32. Ames, S. H., Gasser, M., and Schell, R. R. (1983). Security kernel design and implementation: an introduction. *IEEE Comput.* **16**(7), 14–22.
33. Rushby, J. (1981). Design and verification of secure systems. *ACM Oper. Syst. Rev.* **15**(5), 12–21.
34. National Security Agency (2007). *U.S. Government protection profile for separation kernels in environments requiring high robustness*, Version 1.03. 29 June 2007.
35. Vanfleet, W. M., Beckwith, R. W., Calloni, B., Luke, J. A., Taylor, C., and Uchenick, G. (2005). MILS: architecture for high assurance embedded computing. *CrossTalk* **18**(8), 12–16.
36. Levin, T. E., Irvine, C. E., and Nguyen, T. D. (2006). Least privilege in separation kernels. *Proceedings of the International Conference on Security and Cryptography, Setubal, Portugal,* pp. 355–362.
37. Levin, T. E., Irvine, C. E., Weissman, C., and Nguyen, T. D. (2007). Analysis of Three Multilevel Security Architectures, *In Proceedings of the Computer Security Architecture Workshop*, Fairfax, VA, pp. 37–46.
38. National Security Agency (2004). *(U) Global Information Grid Information Assurance Capability/Technology Roadmap*, Version 1.0 (Final Draft), October. National Security Agency, Fort Meade, MD.
39. Weissman, C. (1992). Blacker: Security for the ddn examples of a1 security engineering trades. In *Proceedings of the 1992 IEEE Symposium on Research in Security and Privacy*, IEEE Computer Society Press, Los Alamitos, CA, pp. 286–291.
40. Irvine, C. E., Levin, T. E., Nguyen, T. D., Shifflett, D., Khosalim, J., Clark, P. C., Wong, A., Afinidad, F., Bibighaus, D., and Sears, J. (2004). Overview of a high assurance architecture for distributed multilevel security. In *Proceedings of the 2004 IEEE Systems, Man and Cybernetics Information Assurance Workshop*, IEEE Computer Society Press, Los Alamitos, CA, pp. 38–45.
41. Weissman, C. (2003). MLS-PCA: a high assurance security architecture for future avionics. In *Proceedings of the Annual Computer Security Application Conference*, IEEE Computer Society Press, Los Alamitos, CA, pp. 2–12.
42. Irvine, C. E. (1995). A multilevel file system for high assurance. In *Proceedings of the 1995 IEEE Symposium on Security and Privacy*, IEEE Computer Society Press, Los Alamitos, CA, pp. 78–87.
43. Nguyen, T. D., Levin, T. E., and Irvine, C. E. (2005). MYSEA Testbed. In *Proceedings of the 6th IEEE Systems, Man and Cybernetics Information Assurance Workshop*, IEEE Computer Society Press, Los Alamitos, CA, pp. 438–439.

# CYBER SECURITY STANDARDS

KAREN SCARFONE, DAN BENIGNI, AND TIM GRANCE
*National Institute of Standards and Technology, Gaithersburg, Maryland*

## 1 INTRODUCTION

The International Organization for Standardization (ISO) defines a standard as "a document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines, or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context" [1]. Numerous standards have been developed for cyber security to help organizations better manage security risk, implement security controls that meet legal and regulatory requirements, and achieve performance and cost benefits. This article provides an overview of cyber security standards in general and highlights some of the major ongoing international, regional, national, industry, and government standards efforts. It also discusses the advantages of having standards and explains how organizations can participate in standards research and development.

## 2 CYBER SECURITY STANDARDS OVERVIEW

Cyber security standards are proliferating. Governments and businesses increasingly mandate their implementation. More manufacturers and vendors are building and selling standards-compliant products and services. In addition, a growing number of organizations are becoming involved in standards development. Cyber security standards are being embraced because they are useful. They provide tangible benefits that justify the time and financial resources required to produce and apply them.

Security technology has not kept pace with the rapid development of IT, leaving systems, data, and users vulnerable to both conventional and innovative security threats. Politically motivated adversaries, financially motivated criminals, mischievous attackers, and malicious or careless authorized users are among the threats to systems and technology that have the potential to jeopardize cyber security, US economic security, consumer identities and privacy, and US public health and safety. While it is impossible to eliminate all threats, improvements in cyber security can help manage security risks by making it harder for attacks to succeed and by reducing the effect of attacks that do occur.

Cyber security standards enhance security and contribute to risk management in several important ways. Standards help establish common security requirements and the capabilities needed for secure solutions. For example, Federal Information Processing Standards (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, establishes standard requirements for all cryptographic-based security systems used by federal organizations to protect sensitive or valuable data [2]. Conformance testing can then be

performed against the standard to provide assurance to users that cryptographic modules are built to requirements.

Security standards facilitate sharing of knowledge and best practices by helping to ensure common understanding of concepts, terms, and definitions, which prevents errors. For example, the Information and Communications Technology (ICT) Security Standards Roadmap [3] includes references to several security glossaries, including the ISO/IEC JTC1/SC27 IT Security Terminology publication [4]. Other helpful resources include the Internet Security Glossary from the Internet Engineering Task Force (IETF), Request for Comments (RFC) 4949 [5] and a compendium of the International Telecommunications Union Telecommunication Standardization Sector (ITU-T) approved security definitions [6]. Using common definitions for security terminology saves time in the development of new standards and supports the interoperability of standards.

Cyber security standards also provide other benefits. Because standards generally incorporate best practices and conformance requirements, their use typically results in improvements in quality. Standards reduce the number of technical variations and allow consumers easy access to interchangeable technology. Standards compliance programs offer a way to measure products and services against objective criteria and provide a basis for comparing products, such as confirming that they offer certain sets of security features. Consumers often benefit from cost savings that result from the development, manufacture, sales, and delivery of standards-based, interoperable products and services. Another benefit of cyber security standards is that the standards development process, with its typical practices of involving a wide range of subject-matter experts, prototyping, and incorporating conformity assessment criteria and methodologies, helps ensure that standards are implementable and reflect recommended practices. Products or services that have been demonstrated to conform to IT security standards can then be expected to offer more assurance than nonstandard products.

When security standards are not available for a technology, several problems often occur. Organizations that adopt the technology may not be aware of its inherent security weaknesses and the implications of implementing the technology for the organization's security posture. Organizations also may not have reliable information on how to take advantage of the technology's security capabilities or on what additional security controls may be needed to compensate for weaknesses in those capabilities. This tends to lead to insecure implementations and insufficient security maintenance, making systems more likely to be exploited and the organization more vulnerable to harm.

### 2.1 Cyber Security Standards Characteristics

Standards can be defined as widely used rules or specifications for activities or their results. Nevertheless, there are often significant differences in how individual standards are developed and applied. These differences can help determine how quickly and easily a new standard is embraced and thereby influence the continued use or demise of alternatives. As a result, standards are often described by the specific characteristics of their development and intended application, including the development process used to produce the standard, the way in which the standard is regulated, the applicability of the standard to different audiences, the availability of the standard to the public, and the measurability of the standard.

Standards come into being in different ways. *Proprietary* or *company standards* are developed by companies with little or no participation by external parties. *De facto*

*standards* are created through the informal adoption of prevailing practices or norms. The majority are *voluntary standards* developed through some form of voluntary consensus process, in which stakeholders participate and agree. Some voluntary standards development efforts are open to all interested parties, while others are restricted to specific groups or individuals, such as members of a particular alliance or consortium.

Standards differ in the ways that they are regulated. Compliance with standards may be optional, or a governing or regulatory organization may make compliance a requirement. *Voluntary standards* are generally called *voluntary*, not only because they are created through volunteers' efforts but also because they are intended for optional use, although a regulating agency could adopt or mandate their use. *Mandatory standards* are standards whose use is prescribed by a regulatory agency or implementing organization. Mandatory standards typically implement laws and regulations.

The audience to whom a standard applies depends upon the entity that develops or adopts it. An *international standard* is one that is adopted by an international standards development organization (SDO) and made available to the public, such as ISO International Standards. A *regional standard* is a standard adopted by several nations in a particular geographic region, for example, European Committee for Standardization (CEN) standards. A *national standard* is a standard developed for use in a particular country either by a government entity or a national SDO. A national standard can also be an international standard that is adopted for use by an individual country. Examples include FIPS and American National Standards Institute (ANSI) standards in the United States and British Standards Institution (BSI) Standards in the United Kingdom. An *industry standard* is one that has been adopted by a particular industry for common use, for example, Security Industry Association (SIA) standards. Finally, a *company standard*, also known as a *proprietary standard*, is a standard developed and owned by a commercial entity that specifies practices or conventions unique to that entity.

Standards may or may not be freely accessible by everyone. By definition, *open standards* are publicly available, but their developer may charge for copies. Examples of open standards that are available to the public for a fee are ISO standards and standards developed by ANSI-accredited organizations. A vendor who develops and owns a *proprietary standard* may choose to make it available to promote interoperability and broaden the market, or choose not to share it.

A growing number of standards require a demonstration of conformance. A *performance standard* states requirements in terms of required results with criteria for verifying conformance, but without stating the methods for achieving required results. Examples of performance standards are the Federal Information Security Management Act (FISMA) and the Health Insurance Portability and Accountability Act (HIPAA). A *prescriptive standard* specifies design requirements, how a requirement is to be achieved, or how an item is to be constructed, but without criteria for measuring the conformity of the results with specified requirements. An example of a prescriptive standard is ISO/IEC 7810 on identification card physical construction. The development and use of performance standards are encouraged since they are less likely than prescriptive specifications to stand in the way of innovation. Still, prescriptive standards are sometimes more appropriate, particularly for describing test methods or procedures or for defining standards to achieve interoperability.

### 2.2 Cyber Security Standards Interaction

A standard is rarely applied in isolation. When technologies, processes, and management practices are combined to solve a business problem, multiple standards normally come into play. When components are integrated, each may entail one or more technical or management standards. For example, a given business solution is likely to involve a variety of IT security configuration standards, such as networking, communications, and security management standards. Each standard imposes requirements that may or may not conflict with the requirements of other standards.

Standards can interact in several ways. Some standards are *complementary*, which means that one standard supports or reinforces the requirements of another. For example, ISO frequently publishes multipart standards that can be considered complementary, where each part is a separately developed volume covering a different aspect of a central issue. Some standards may *conflict* with each other, which means that there are inconsistencies or contradictions between standards, resulting in issues such as technological incompatibility or legal noncompliance. Other standards are *discrete*, which means that they have no direct effect on one another. There are also *standards gaps*, where there is no formal standard developed for a particular area of security, although a guideline may exist. Standards gaps typically occur when a technology is evolving so rapidly that standards development cannot keep pace. In other cases, a gap exists because consensus has not been reached on either the technology or the standard.

### 2.3 Standards and Guidelines

Standards can be contrasted with another category of documents, generally referred to as *guidelines*. Both standards and guidelines provide guidance aimed at enhancing cyber security, but guidelines usually lack the level of consensus and formality associated with standards. Some standards, such as ANSI Standards and FIPS Publications, are easily recognized because they include the term *standard* in their titles. Others are harder to recognize. For example, standards issued by the International Telecommunications Union (ITU), an international standards developer, are designated as *Recommendations*. A standard issued by the IETF starts out as an *RFC* and retains that designation even after being adopted as a standard. In other cases, documents that are not standards in the strict sense of the word may be treated as such by an organization if it suits the organization's needs. For example, many US and international organizations and businesses have adopted National Institute of Standards and Technology (NIST) Special Publications as standards, even though those documents are published as guidelines for use by US Federal agencies.

Some organizations develop both standards and guidelines. For example, in addition to international standards, ISO/IEC issues several types of guidelines, including technical specifications, publicly available specifications (PAS), and technical reports, according to the ISO/IEC Directives, Part 1, Section 3 [7]. A technical specification may be published when the immediate release of an international standard is not feasible, such as when the subject in question is still under development. A PAS may be an intermediate specification published prior to the development of a full international standard, or in International Electrotechnical Commission (IEC) it may be a "dual logo" publication published in collaboration with an external organization. A PAS does not fulfill the requirements for

a standard. A technical report is an informative document generally intended to educate the reader, not to specify an international standard.

## 3 CYBER SECURITY STANDARDS DEVELOPERS

International, regional, national, industry, and government groups are involved in the development of cyber security standards. An *SDO* is an organization whose primary mission is the development of voluntary consensus standards on an international, regional, or on a national basis. Most SDOs cover a wide variety of technical areas, not just cyber security. *Consortia*, *industry alliances*, and *associations* are all groups of organizations or individuals with similar interests that promote standards development. A consortium is typically formed for a limited time to achieve a specific goal, such as the development of standards. *Industry alliances* and *associations* tend to be more loosely formed to foster common interests. Consortia and industry alliances comprise companies, and associations are made up of individuals. Finally, the US *government* and other national governments develop standards specifically intended for government audiences. Examples of organizations in each of these categories are provided below, along with brief discussions of some of the organizations' cyber security standards work.

### 3.1 International Standards Development Organizations

The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) develops standards in many areas, including information technology, telecommunications, and power generation. An example of IEEE-SA's security work is its 802 Local Area Network (LAN)/Metropolitan Area Network (MAN) Standards Committee. Various working groups within the committee develop widely used standards for many types of networking technologies, such as Ethernet, wireless LANs, Bluetooth, and Worldwide Interoperability for Microwave Access (WiMAX). These standards include the security features built into the wireless networking protocols.

The IETF is concerned with the evolution of the Internet architecture and the operation of the Internet. The IETF has dozens of working groups that each focus on a different element of the Internet, including several groups working on Internet security. Topics addressed by these working groups include Domain Name System (DNS) security, authentication protocols, routing protocol security, Internet Protocol (IP) version 6, public key infrastructure, e-mail security, event logging, and network traffic encryption.

ISO, whose membership consists of the national standards institutes of more than 150 countries, addresses all standards except those for electrical and electronic engineering, which are the responsibility of the IEC. ISO and IEC formed the Joint Technical Committee 1 (JTC1) for IT standards development, including standards for the security of systems and information. JTC1 has a number of subcommittees (SC) and working groups that address specific technologies. For example, the SC17 group addresses identification cards and personal identification, the SC27 group focuses on IT security techniques, the SC31 group works on automatic identification and data capture (AIDC) techniques, and the SC37 group develops biometric standards.

The ITU-T produces standards, called *Recommendations*, for telecommunication networks. ITU-T's standards are developed by study groups (SG) such as SG17, which covers security, languages, and telecommunications software. SG17 led the development

of the ICT Security Standards Roadmap, which provides information on previous and current security standards work from several major standards developers, including ISO, IEC, IETF, Organization for the Advancement of Structured Information Standards (OASIS), Institute of Electrical and Electronics Engineers (IEEE), and telecommunications-specific organizations. It also lists current security standards gaps and provides pointers to security glossaries. SG17 developed the ICT Security Standards Roadmap in collaboration with the European Network and Information Security Agency (ENISA) and the Network and Information Security Steering Group (NISSG).

### 3.2 Regional Standards Development Organizations

The European Telecommunications Standards Institute (ETSI) produces telecommunications standards within Europe. ETSI's cyber security standards activities include work on electronic signatures, smart cards, lawful interception, and 3GPP.

The CEN, whose members are the national standards organizations of 30 European countries, develops cyber security standards on its own and in conjunction with other international, national, and government standards developers.

### 3.3 National Standards Development Organizations

In the narrowest sense of the term, ANSI is not an SDO, since it does not develop standards; rather, it administers and coordinates the activities of the US private sector voluntary standardization system. ANSI sponsors cyber security-related working groups, such as a Homeland Security Standards Panel and a Healthcare Information Technology Standards Panel.

The InterNational Committee for Information Technology Standards (INCITS) is an ANSI-accredited organization, which develops US standards for information and communications technologies. INCITS comprise technical committees (TCs) that create standards for different technology areas. Examples of cyber security-focused TCs are B10 (identification cards and related devices), CS1 (cyber security), M1 (biometrics), and T6 (radio frequency identification (RFID) technology).

### 3.4 Consortia, Industry Alliances, and Associations

The Association for Automatic Identification and Mobility (AIM) is a trade association for entities that are interested in AIDC technologies. AIM performs the development of cyber security standards in areas such as barcodes, card technologies, electronic article surveillance, RFID, real-time locating systems (RTLS), and other AIDC-related technologies.

The British Security Industry Association (BSIA) is the professional trade association for the security industry in the United Kingdom. The BSIA develops codes of practice and technical documents and submits some of them for consideration as British Standards. Security areas addressed by the BSIA include access control, information destruction, physical security equipment, and security systems.

The Information Systems Audit and Control Association (ISACA) is an organization for information assurance, governance, security, and audit professionals. It is best known for its information system auditing and control standards and related initiatives. For example, ISACA has developed Control Objectives for Information and related Technology (COBIT), which is a control framework that encompasses several aspects

of IT governance, including risk assessment. COBIT is based on various international standards and can be used to identify appropriate standards references during audits.

The Instrumentation, Systems, and Automation Society (ISA) is a professional association that develops standards for automation technologies. For example, its SP99 working group develops security standards for manufacturing and control systems, such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS). Some of ISA's reports on this topic have become ANSI standards.

The OASIS develops standards for security and e-business, and is well known for its web services standards work. OASIS has several working groups focused on security topics such as biometrics, digital signature services, enterprise key management infrastructures, public key infrastructure adoption, and web services security.

The SIA is an ANSI-accredited SDO that develops systems integration and equipment performance standards. Several SIA working groups develop physical security standards on topics such as biometrics, mobile security devices, credential readers, security communications, and security control panels.

### 3.5 US Government Standards Developers

NIST develops security standards for US Federal information systems. NIST's FIPS have been made mandatory for federal use. Examples of FIPS include FIPS 200, which specifies minimum security requirements for federal information systems; FIPS 199, which provides standards for security categorization of federal systems; and FIPS 197, which defines the Advanced Encryption Standard (AES). NIST also hosts the National Center for Standards and Certification Information (NCSCI), which provides information on US standards and technical regulations, as well as other national, regional, and international standards.

The Office of Management and Budget (OMB) assists the President of the United States in the development of budget, management, and regulatory policies. OMB's products include OMB Circulars and OMB Memoranda, which are instructions or information issued to federal agencies. Some of these documents mandate the use of particular security standards or require federal agencies to meet other security requirements. For example, OMB Circular A-130 pertains to the management of federal information resources, and OMB Memorandum M-07-16 mandates security controls to protect the confidentiality of personally identifiable information.

## 4 GETTING INVOLVED IN STANDARDS DEVELOPMENT

In addition to those mentioned above, there are many other cyber security standards developers already working on creating new standards. The ICT Security Standards Roadmap provides information on a number of ongoing standards activities. Organizations interested in cyber security standards development can join existing standards efforts so that they can ensure that standards are developed in a way that is favorable to, or at least compatible with, their critical interests.

In addition to influencing the direction that a standard takes, actively participating in the standards development process offers other advantages. An organization gains a better understanding of the standards under development, their underlying designs,

the trade-offs and compromises made during their development, and the operating conditions and environments they are intended to serve. Organizations make contacts and build relationships with technical experts involved in the development effort, as well as improving their own technical knowledge. Participation in standards development also benefits the security community by sharing the effort across many organizations.

Most organizations do not participate in standards development activities. They may feel that it is not important, that it is impossible to influence the outcome, or that involvement is too expensive. Nevertheless, participation can be critical to realizing the benefits of standards. Also, organizations that choose not to get involved can find themselves faced with new standards with which they are not prepared to comply.

There are a number of ways to participate in the standards development process, each with its own level of resource commitment. Organizations can choose how fully to participate, depending upon the importance of the standard to the organization and the resources they have available to commit to the effort. *Trackers* follow the development of a standard at a high level, for example, by reading summaries and implementation timelines on the developer's public website. Tracking the progress of a new standard gives organizations the ability to anticipate its effects, even if they choose not to become more actively involved in its development. *Public reviewers* review drafts of the standard and submit comments, which can influence the content and impact of a standard under development. For particularly important standards, organizations should consider becoming *members* of the entity developing the standards. The role of *driver* may be appropriate when the organization's stake in a new standard is critical. It may be that producing the standard is part of the organization's charter or mission; driving the development of a standard may require significant resources.

In addition to contributing to the development of new standards, organizations should also consider participating in the maintenance of existing standards. Most standards undergo periodic review and revision. SDOs typically have established formal maintenance programs to help ensure that their standards do not become dated due to technological evolution, changes to related standards, or other causes.

## REFERENCES

1. International Organization for Standardization/International Electrotechnical Commission (2004). *ISO/IEC Directives Part 2:2004 (Rules for the Structure and Drafting of international Standards)*, 5th ed., http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/International%20Standardization/ISO/ISOIECDirectivesPart2pdfformat.pdf.
2. National Institute for Standards and Technology (2001). *FIPS PUB 140-2: Security Requirements for Cryptographic Modules*, May. http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
3. ITU-T, European Network and Information Security Agency (ENISA), Network and Information Security Steering Group (NISSG) (2007). *ICT Security Standards Roadmap*, version 2.2, September 2007. http://www.itu.int/ITU-T/studygroups/com17/ict/index.html.
4. ISO/IEC JTC1/SC27 (2008). *Standing Document 6 (SD6): Glossary of IT Security Terminology*, 2008-03-19. http://www.jtc1sc27.din.de/sce/SD6.
5. Internet Engineering Task Force (2007). *Internet Security Glossary*, August 2007. http://www.ietf.org/rfc/rfc4949.txt.

6. ITU Telecommunication Standardization Sector (2008). *Security Compendium, Part 2—Approved ITU-T Security Definitions*, http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0001MSWE.doc.
7. ISO/IEC (2008). *ISO/IEC Directives Part 1:2008 (Procedures for the Technical Work)*, 6th ed., http://isotc.iso.org/livelink/livelink/fetch/2000/2122/3146825/4229629/4230450/4230455/ISO_IEC_Directives_Part_1_Procedures_for_the_technical_work__2008_6th_ed.__PDF_format_?nodeid=4230504&vernum=0.

## FURTHER READING

American National Standards Institute (ANSI) (2008). *ANSI Standards Activities*, http://www.ansi.org/standards_activities/overview/overview.aspx?menuid=3.

Association for Automatic Identification and Mobility (AIM) *AIM Global Standards*, http://www.aimglobal.org/standards/.

British Security Industry Association (BSIA) http://www.bsia.co.uk/index.php.

Department of Homeland Security (DHS) http://www.dhs.gov/index.shtm.

European Committee for Standardization (CEN) http://www.cen.eu/cenorm/homepage.htm.

European Network and Information Security Agency (ENISA) http://www.enisa.europa.eu/index.htm.

European Telecommunications Standards Institute (ETSI) *ETSI Standards*, http://www.etsi.org/WebSite/Standards/Standard.aspx.

IEEE, IEEE Standards Association (IEEE SA) http://standards.ieee.org/.

Information Systems Audit and Control Association (ISACA) http://www.isaca.org/Template.

ISO/IEC Joint Technical Committee 001 "Information Technology". http://www.jtc1.org/.

InterNational Committee for Information Technology Standards (INCITS) http://www.ncits.org/.

International Electrotechnical Commission (IEC) http://www.iec.ch/.

Internet Engineering Task Force (IETF) http://www.ietf.org/.

International Organization for Standardization (ISO) http://www.iso.org/iso/home.htm.

International Telecommunication Union Telecommunication Standardization Sector (ITU-T) http://www.itu.int/ITU-T/.

Instrumentation, Systems, and Automation Society (ISA), ISA Standards http://www.isa.org/Template.cfm?Section=Standards2&Template=/customsource/isa/Standards/AutomationStandards.cfm.

National Institute of Standards and Technology (NIST) http://csrc.nist.gov/.

NIST National Center for Standards and Certification Information (NCSI) http://ts.nist.gov/Standards/Information/index.cfm.

Information & Communications Technologies (ICT) Standards Board Network and Information Security Steering Group (NISSG). http://www.ictsb.org/Working_Groups/NISSG/index.htm.

Office of Management and Budget (OMB) http://www.whitehouse.gov/omb/.

Organization for the Advancement of Structured Information Standards (OASIS) http://www.oasis-open.org/.

Process Control Systems Forum (PCSF) https://www.pcsforum.org/.

Security Industry Association (SIA), SIA Standards. https://www.siaonline.org/standards/index.html.

United States Computer Emergency Readiness Team (US-CERT), Control Systems Security Program (CSSP) http://www.us-cert.gov/control_systems/index.html.

# CYBER SECURITY METRICS AND MEASURES

PAUL E. BLACK, KAREN SCARFONE, AND MURUGIAH SOUPPAYA
*National Institute of Standards and Technology, Gaithersburg, Maryland*

## 1 INTRODUCTION

Cyber security metrics and measures can help organizations (i) verify that their security controls are in compliance with a policy, process, or procedure; (ii) identify their security strengths and weaknesses; and (iii) identify security trends, both within and outside the organization's control. Studying trends allows an organization to monitor its security performance over time and to identify changes that necessitate adjustments in the organization's security posture. At a higher level, these benefits can be combined to help an organization achieve its mission by (i) evaluating its compliance with legislation and regulations, (ii) improving the performance of its implemented security controls, and (iii) answering high-level business questions regarding security, which facilitate strategic decision making by the organization's highest levels of management. This article defines some terms, and then discusses the current state of security metrics, focusing on the measurement of operational security using existing data collected at the information system level. This article explains the importance of selecting measures that support particular metrics and then examines several problems with current practices related to the accuracy, selection, and use of measures and metrics. The article also presents an overview of a security metrics research effort, to illustrate the current state of metrics research, and suggests additional research topics.

## 2 CONTRASTING METRICS AND MEASURES

The term *metric* is often used to refer to the measurement of performance, but it is clearer to define metrics and measures separately. A *measure* is a concrete, objective attribute, such as the percentage of systems within an organization that are fully patched, the length of time between the release of a patch and its installation on a system, or the level of access to a system that a vulnerability in the system could provide. A *metric* is an abstract, somewhat subjective attribute, such as how well an organization's systems are secured against external threats or how effective the organization's incident response team is. An analyst can approximate the value of a metric by collecting and analyzing groups of measures, as is explained later.

Historically, many metrics efforts have focused on collecting individual measures, and given little or no thought as to how those measures could be combined into metrics. Ideally, organizations should first select their metrics, and then determine what measures they can perform that support those metrics. An organization should also have multiple

levels of metrics, each geared toward a particular type of audience. For example, technical security staff might be interested in lower-level metrics related to the effectiveness of particular types of security controls, such as malicious code detection capabilities. Security management might be interested in higher-level metrics regarding the organization's security posture, such as the overall effectiveness of the organization's incident prevention and handling capabilities. Lower-level metrics facilitate making more tactical decisions, whereas higher-level metrics are well suited for making more strategic decisions. The lower-level metrics are often used as input to the higher-level metrics.

Organizations can use measures and metrics to set goals, also known as *benchmarks*, and determine success or failure against the benchmarks. For example, suppose that an organization determines that 68% of its systems are in compliance with a particular policy. The organization could set a benchmark of 80%, implement changes in its practices to increase compliance, and then measure compliance again in six months to see if the benchmark has been achieved. Benchmarks are organization specific and are typically based on baselines from an operational environment.

## 3 SELECTING MEASURES TO SUPPORT METRICS

Once an organization has identified its metrics, it then needs to determine what measures can feasibly be collected to support those metrics. Organizations should favor measures that can be collected via automated means because they are more likely to be accurate than manual collection (e.g. self-evaluation surveys) and can also be collected as often as needed. Organizations should also seek opportunities to use existing data sources and automated collection mechanisms because of the cost of implementing and maintaining new systems and software simply for data collection purposes.

As measures are collected, organizations need a way to analyze them and generate reports for the metrics they support. Organizations can analyze the measures and metrics in many ways, such as grouping them by geographic location, logical division within the organization, system type, system criticality, and so on. Some organizations use products that roll up measures into metrics and present the metrics in a security dashboard format, with the measures underlying each metric available through drill-down. This allows a dashboard user to see the values of the presented metrics and changes in those metrics over time, as well as to examine the metrics and measures comprising those metrics.

## 4 PROBLEMS WITH THE ACCURACY OF MEASURES

The accuracy of a metric is by definition dependent on the accuracy of the measures that comprise the metric. Organizations currently face several problems related to the accuracy of measures. One problem is that measures are often defined imprecisely. Consider the percentage of systems that are fully patched: does this only include operating system patches or does it also include service and application patches? Does it only mean that the patches have been installed or that subsequent actions necessary to activate the patch (such as rebooting the system or changing configuration settings) have also

been performed? Another issue with measure definition is the terminology itself, such as measuring the number of port scans performed. What is the minimum number of ports that must be scanned in a port scan? If an attacker scans ports on 100 hosts, is it one port scan or 100 port scans? If the attacker performed the same scan but only scanned one host each day, is it one port scan or 100 port scans?

Measuring port scans is also a good example of a related common problem—inconsistent measurement methods. Port scans are often identified by intrusion detection systems (IDSs), but each IDS uses its own proprietary algorithms for identifying port scans, so activity identified as a port scan by one IDS may not be identified as such by another. This causes inconsistency in measurement if the organization uses multiple IDSs or if a single product is in use but its sensors have different port scan settings (e.g. the minimum number of ports in a scan or the maximum length of time to track a scan). Another example is system patch status—one operating system might report only on operating system patches, while another operating system might also include some application patches. In such a case, an organization could use multiple measures instead of one, with each measure corresponding to a different measurement method, and then combine the measures into a metric that approximates the collective values of the measures.

Many instances of problems with imprecise measure definitions have been mentioned in the security community, but to date no concerted effort has been made to exhaustively gather information on these problems, document it, and make it available to the security community. It would be much more helpful to identify the factors that organizations should consider when defining their measures than to attempt to provide a single definition for each measure. The best definition for an organization is driven by what the organization is trying to accomplish. For example, in the patching example mentioned above, an organization might be trying to gain insights on general patch distribution and installation practices to verify that all applications deemed critical by the organization have been patched or to verify that the organization's patch management software is functioning properly (e.g. patches are installed and operate properly based on a predefined schedule).

Another common problem with the accuracy of measures is the use of qualitative measures. As mentioned earlier, data collection methods such as self-evaluation surveys often produce inaccurate or skewed results, depending on the types of questions asked. For example, if users or administrators are asked if their systems comply with the organization's policies, they are very likely to say that they do. It would be more accurate to instead use quantitative measures that assess the systems' compliance. Qualitative measures that do not have well-defined scales or units of measure can be particularly problematic in terms of accuracy. For instance, asking a user to rate the reliability of their computer on a scale of 1–5 where 1 is simply defined as "poor" and 5 as "excellent" is subjective and imprecise. A qualitative measure may be useful if each rating is defined clearly without overlap between the ratings, so that different people, when given the same information, would be likely to assign the same rating. An objective scale might be 5—no crashes or hangs in six months, 4—one crash or hang, 3—two or three instances, 2—four to six instances, and 1—more than six instances. The rating may still be somewhat subjective because it is dependent on the user's recall or because "crash" and "hang" are not defined. Nonetheless, this qualitative measure is more precise than "poor" to "excellent".

Some measures are also considered qualitative because they provide absolute counts without a context, norm, or goal. For example, a measure that indicates that 100 attacks were attempted has no context. What is the period of time? Is 100 a lot or a little? A measure that indicates that 100 attacks were attempted out of 1,000,000 incoming Web server connections adds context.

Context is very important to measures and metrics. Most measures individually have little meaning. Even the example above—the number of attempted attacks per million incoming Web server connections—does not have much meaning by itself. Is the rate of attempted attacks rising, falling, or staying steady? Have any changes been made to the organization's security controls that would change how effectively they can detect attacks or has there truly been a change in the number of attacks? Do changes in the rate of attempted attacks correspond to observations about attack trends reported by other organizations? A single measure may need to be analyzed in context with several other measures, as well as separate events such as security control changes and external trends, to determine its true significance. It would be helpful to organizations to have additional information compiled on the relationships between measures and between measures and separate events, particularly if it includes empirical information based on analyses of real-world operational environments.

Also, because cyber technology is so dynamic, the meaning of measures and metrics changes over time. For example, a measure may have shown an increase in attacks succeeding last year, and the organization determined through other measures and knowledge of external events that this was primarily due to an increase in phishing attacks. This year antiphishing technologies are deployed, but the success rate for attacks continues to increase. Is this due to improved attack techniques, improperly configured antiphishing technologies, inadequately trained users, or other factors? Next year, there may be additional factors that influence the significance of the measure, as well as different relative importances for the existing factors.

## 5 PROBLEMS WITH THE SELECTION OF MEASURES

Most organizations have many existing sources of security measures, automatically generated by enterprise security controls such as antivirus and antispyware software, intrusion detection systems, firewalls, patch management systems, and vulnerability scanners. There may be accuracy issues with some of these measures, but this can still leave an organization with many existing measures from which to choose. Organizations could also create additional measures such as utilities to extract information from security logs, but there may be considerable cost in creating and deploying software and, in some cases, entire systems to collect such measures.

Some organizations collect many measures under the assumption that it is better to have more information than less information, or because it is easier to collect a lot of measures than it is to create a set of metrics and then determine which measures support those metrics. Collecting measures without evaluating their usefulness and having a plan for how to use them has several disadvantages. Firstly, it can waste considerable time and resources to collect, analyze, and report measures: only the measures that support the organization-selected metrics are generally needed. Secondly, if the measures are not selected and organized so that the dependencies between the measures

are clear and accurately represented in the corresponding metrics, analysis of the measures and related metrics is likely to generate misleading results. Thirdly, it often causes people involved in the measure collection process to feel that the effort is a waste of time, because it is unclear what value there is in collecting so many measures. Another reason is that if people are allowed to choose which measures they will collect and share with others, they are more likely to collect measures that demonstrate positive results (e.g. 100% of desktop computers have antivirus software installed) than measures that demonstrate negative results (e.g. 15% of antivirus software installations are up to date).

Currently, there are many suggestions in the security community for what measures organizations should collect. However, little work has been done to determine the value of these measures in real-world operational environments, including which measures are most supportive of particular metrics. For example, suppose that an organization wants a metric for how effectively its security controls detect and stop attacks. Dozens, if not hundreds, of measures that could support this metric have been suggested by the security community, but little research has been done as to which of those measures are most closely correlated with the metric. If the characteristics of real-world operations were studied and analyzed, it may become apparent which measures are most indicative of the overall security posture and which measures are of little or no value. It might also be possible to approximate a metric by using just a few carefully selected measures.

## 6 PROBLEMS WITH THE USE OF MEASURES

In addition to issues with measure accuracy and selection, many organizations also face challenges involving the use of measures. Some of these challenges, such as ensuring that the selected measures support the determination of the chosen metrics, have been discussed earlier. Another common challenge is determining how to combine the values of the measures into a metric. The measures may use different units of measurement, have different scales, and have varying precision; these issues can be addressed through careful creation of equations to combine the values. Also, some of the measures may be more important than others in the scope of the metric; however, it is often difficult to quantify what weight each measure should be given. Empirical research in this area could provide organizations with a factual basis for weighting measures instead of either guessing or weighting each measure equally.

Organizations need to recognize that over time, they will need to alter their measures and metrics. Although high-level metrics may stay the same, low-level metrics need to change over time as the security posture of the organization changes. For example, an organization with relatively immature security practices may need to initially focus on measures and metrics involving its most basic security controls, such as what percentage of computers are protected by antivirus software. As the organization's security controls mature, these metrics may become less useful, and the organization may want to answer new questions, such as how effective its security controls are at stopping malware. This may require the development of new metrics and corresponding measures, and the collection of the old metrics and measures can be stopped if the organization no longer finds them to be of value.

## 7 COMMON VULNERABILITY SCORING SYSTEM (CVSS)

To better illustrate the current state of research on security metrics, we will examine an ongoing research effort for metrics that indicate the significance of vulnerabilities in systems. The Common Vulnerability Scoring System (CVSS) is a standard for assessing the severity of flaws in operating system and application software [1]. CVSS is composed of three sets of measures: base measures that are constant over time, temporal measures that change over time but are the same for all environments, and environmental measures that may be different for each environment. There is a different equation for each set of measures, and the result of each equation is a score—a base, temporal, or environmental score—that is in essence a metric. The measures are for particular characteristics of each vulnerability, such as whether it can be exploited remotely (over a network) and to what degree the confidentiality, integrity, and availability of a target could be impacted. The score metric is intended to give a general indication of the relative severity of the vulnerability.

The initial version of the CVSS measures, equations, and metrics were released in 2005. On the basis of feedback from their real-world use, particularly examination of empirical measure and metric data by security experts, deficiencies in the CVSS standard were identified. The measures, equations, and metrics, as well as the corresponding documentation, have all been revised to make the measures more consistent and to improve the accuracy of the metric scores. Version 2 of the CVSS standard was released in mid-2007.

CVSS is most commonly used by organizations to prioritize their vulnerability mitigation activities, such as applying patches to systems. However, researchers are investigating other uses for CVSS. For example, work has been done at the National Institute of Standards and Technology (NIST) on using CVSS to determine metrics for security-related software configuration settings [2]. Researchers at Veracode are looking at using CVSS to rate software weaknesses [3]. There is also interest in bringing CVSS scores down from the enterprise level to the individual system level so that CVSS could be used to help assess the overall vulnerability of individual systems. To accomplish this, considerable research and empirical validation are needed for applying CVSS to software configuration settings and weaknesses, as well as a new way of measuring the strength of security controls on individual systems.

## 8 RESEARCH DIRECTIONS

Literature contains hundreds of measures. Research is needed to validate connections between measures and security, determine correlations, and model effects. Although there is some readily accessible data, for example, National Vulnerability Database [4] and A Chronology of Data Breaches [5], such research and analysis require more and higher-quality data. State laws requiring companies to notify consumers of data breaches have the benefit of supplying data. Additional information can come from developing or articulating motivations for organizations to share information, as is the practice for business case studies or the airline industry.

Beyond measures, a secure nation needs research to understand which metrics lead to higher security, the measures supporting those metrics, and analytical methods to aggregate measures.

## REFERENCES


1. Common Vulnerability Scoring System. (2008). *Forum for Incident Response and Security Teams (FIRST)*, http://www.first.org/cvss/.
2. Scarfone, K. and Mell, P. (2008). The Common Configuration Scoring System (CCSS) (Draft), NIST, NIST Interagency Report 7502, http://csrc.nist.gov/publications/PubsNISTIRs.html.
3. (2008). https://securitymetrics.org/content/attach/Metricon2.0/Wysopal-metricon2.0-software-weakness-scoring.ppt.
4. National Institute of Standards and Technology (NIST). (2008). *National Vulnerability Database*, http://nvd.nist.gov/.
5. Privacy Rights Clearinghouse. (2008). *A Chronology of Data Breaches*, http://www.privacyrights.org/ar/ChronDataBreaches.htm.


## FURTHER READING


Corporate Information Security Working Group. (2005). *Report of the Best Practices and Metrics Teams*, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Government Reform Committee, United States House of Representatives, 17 November 2004, revised 10 January http://www.educause.edu/ir/library/pdf/CSD3661.pdf.

Dorofee, A., Killcrece, G., Ruefle, R., and Zajicek, M. (2007). *Incident Management Capability Metrics*, Version 0.1, Software Engineering Institute/CERT, http://www.cert.org/archive/pdf/07tr008.pdf.

Herrmann, D. S. (2007). *Complete Guide to Security and Privacy Metrics*, Auerbach Publications, Boca Raton, FL.

Jaquith, A., (2007). *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Addison-Wesley, Upper Saddle River, NJ.

McCurley, J., Zubrow, D., and Dekkers, C. (2007). *Measures and Measurement for Secure Software Development*, Software Engineering Institute, https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/measurement/227.html.

Safety and Security Measurement Technical Working Group. (2005). *Security Measurement*, Practical Software and Systems Measurement (PSM), http://www.psmsc.com/Downloads/Other/Security%20White%20Paper%202.0.pdf.

(2008). securitymetrics.org, http://www.securitymetrics.org/.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. (2008) *Performance Measurement Guide for Information Security*, NIST, NIST SP 800-55 Revision 1, http://csrc.nist.gov/publications/PubsSPs.html.


### Conferences and workshops


(2008). *Third Workshop on Security Metrics (MetriCon 3.0)*, http://www.securitymetrics.org/content/Wiki.jsp.

(2008). Security measurements and metrics. *Fourth International Workshop on Quality of Protection (QoP 2008)*, http://dit.unitn.it/∼qop/.

(2005). *IEEE International Symposium on Software Metrics*, http://www.informatik.unitrier.de/∼ley/db/conf/metrics/ (latest year was 2005).

# TRUSTED PLATFORMS: THE ROOT OF SECURITY

ROGER L. KAY
*Endpoint Technologies Associates, Inc., Wayland, Massachusetts*

## 1 INTRODUCTION

The ancient adage admonishes that a chain is only as strong as its weakest link, but this maxim might as well have been coined for computer security. A chain of trust is only as trustworthy as its most vulnerable node or layer. The computing industry has long understood this principle and has even generated adequate technological solutions. Two challenges remain unmet, however: standardization and adoption. Toward the end of the Millennium, IBM and its partners in the development of trusted architectures realized that no solution would work unless it was adopted universally. The industry embraced the principle of standardized security, even before 9/11, but all the more ardently since. Hardware manufacturers and software platform developers agreed that hardware-based security was necessary as the root of trust, and the industry embodied the basic standard in hardware circuitry, essentially a silicon chip. This circuitry ships with an ever growing proportion of personal computers, smart phones, and particularly embedded devices, but has not been put into use widely, particularly in its broader manifestation among devices across a network. Although the circuitry is in the computer, it remains inactive for the most part. Usage, such as it is, is mainly restricted to user-to-platform authentication and password management. Thus, the pace of implementation of secure base computing in the decade succeeding 9/11 has slowed to a crawl, as users await software that makes better use of the secure hardware, and remaining standardization issues get sorted out. There are some exceptions, islands of adoption, and areas of usefulness, but much of the work lies ahead.

## 2 THE STATE OF TRUSTED COMPUTING

It did not take the computing industry long to realize what an optimal security architecture looked like. Work done on encryption had shown that key pairs based on large prime numbers, generated through Public Key Infrastructure (PKI) technology [1], were the mathematically simplest and best way to create robust keys that could be used to encode and decode data securely as well as to identify a user publicly and authenticate a user privately. PKI creates key pairs, sometimes several sets. Each pair has a private and public key. Each is mathematically related to the other, but neither can be derived from the other. True to its name, the public key, everyone knows. If you send me something encoded in my public key, no one can intercept it or make sense of it, but I can open

it with my private key. If I send you something encoded with my private key and you can decrypt it with my public key, knowing it is me because no one else has my private key.

Important to this architecture's viability is the fact that sender and receiver need never share a secret. And the same relationship between sender and receiver holds between any two nodes in the infrastructure (e.g. hardware and firmware, operating system and application within a system, or any two adjacent communications points within the network). As long as each element or layer can be publicly identified and privately authenticated, the chain of trust can be extended through it.

Keys are large and difficult to crack. Theoretically, a key domain can be expanded to the point of precluding a crack, but this degree of security is not desirable for practical reasons. Arguably, "commercial-grade" security, whose primary job is to rapidly encrypt and decrypt transactional data in high volumes, is sufficient and the type of security appropriate for military-grade protection is unnecessary. It is typical of the commercial world that none of the transactions is of earth-shattering importance. However, all these transactions taken together represent a profile of the business in question and therefore need to be kept from prying eyes.

In fact, the PKI algorithm is asymmetrical; that is, it is a "one-way" formula. The metaphor is breaking a champagne glass. It is easy to turn a glass into shards by throwing it into a fireplace, but extremely difficult to reassemble a glass from shards in a fireplace. This characteristic helps make PKI hard to break, but it is also a reason that PKI is slow [2]. For this reason, a different algorithm, Advanced Encryption Standard (AES), a method that has the virtue of being symmetrical but the weakness of requiring a shared secret, is used for bulk encryption. Called *Triple AES*, the data is wrapped three times in AES encryption, a method deemed sufficient to stave off most intruders. The shared secret, which is a relative handful of code, is encoded with the heavier weight, more robust PKI algorithm, and thus the data is safe, whether in flight (i.e. traveling over data communication lines) or at rest (i.e. sitting on a hard drive).

In the late 1990s, when the original architecture for trusted computing was being forged, IBM, the senior partner on the development team, realized that the elegance of PKI could only be realized if everyone agreed to adhere to the same standard. After all, if the public is to know that *I am me*, it must be all the public and not just some of it. And if I want to send something to you that only you can see, I can do so only if I have access to your public key and you and only you have your private key within a system that recognizes both as being part of the same pair. None of this can work if separate domains exist. Potentially, one needs to interact with someone else.

Seeing developments swinging in this direction, IBM realized that it could not propagate the system on its own. Rivals would perceive the move as an attempt to control the industry at a choke point. So, the company changed course and decided to contribute its intellectual property to a neutral industry body and work with other vendors to bring everyone over to the new standard. That group evolved into the Trusted Computing Group (TCG), which is now comprised of most of the key players in the information technology industry.

The membership of the TCG, 140 companies drawn from all geographies, has spent the past decade refining and promoting standardized security for a number of platforms and circumstances. The TCG board includes AMD, Fujitsu Limited, Hewlett-Packard, IBM, Infineon, Intel, Lenovo, Microsoft, Seagate, Sun Microsystems, and Wave Systems [3].

### 2.1 Why Hardware Security?

A primary reason that the TCG decided to back hardware-based security is its clear superiority over software-based solutions. Of course, every solution has software, but the critical issue is how keys are created and handled. Because a software-only solution requires that a key, the algorithm that uses the key, and the data to be encrypted all reside in main memory at the same time in order to function, the key is vulnerable.

This fact was proven in January 2000, when researchers at nCipher in Cambridge, England, came up with an algorithm that can search main memory, looking for a high degree of entropy [4]. A good private key is going to be exceedingly entropic; that is the random numbers in the key will be well dispersed in numeric space. Other elements in memory—such as the clear text to be encrypted and the encryption program itself—will not be. Since all three—the program, the data, and the key—have to be in main memory at the same time for software encryption to take place, the nCipher algorithm could allow an intruder to scan the contents of main memory and find the user's private key. The nCipher program has been able to find a 1,024-bit private key, the best in commercial use at the time [5].

Another weakness of software solutions is that they cannot prevent "hammering," the practice of trying one possible key after another in rapid fire, because they are unable to keep a counter. A hacker can always freeze the state of the machine and continue to bombard it with attempts. Hardware security cannot be bypassed in this way and thus can institute a progressive lock-out program if too many password attempts are made. This type of program increases the delay between log-in offers after a set number of failed attempts. But, as a reason to avoid software-only security solutions, the hammering flaw pales beside the problem of leaving highly entropic private keys around in main memory.

### 2.2 Essentials of Trusted Computing

Thus, the industry agreed to pursue an architecture based on a hardware implementation of established security principles. The actual hardware involved circuitry insulated from the main computing mechanism. This circuitry, named the Trusted Platform Module (TPM), contained read-only memory, preloaded with the basic security program and a small amount of memory for storing keys generated by the program [6]. The circuitry, in its discrete implementation (a separate chip as opposed to a section of a larger chip), was connected to the processor via a secure bus, and in the off chance that this bus was attacked, the mechanism was designed to flag that it was in an insecure state. A bus attack became less of an issue with integrated implementations, as when the TPM circuitry is added as a module to core logic, the I/O chip, or even the processor itself.

A generic view of TPM architecture shows how it sits on a bus connected to core logic (Fig. 1). The trusted platform provides three basic elements: protected capabilities, integrity measurement, and integrity reporting. Protected capabilities are a set of commands that can access shielded locations (e.g. in memory, in the registry), where data operations can take place safely. The TPM uses shielded locations to protect and report integrity measurements. In addition, the TPM generates and stores cryptographic keys used to authenticate reported measurements.

Among other functions, the TPM can attest to the reliability of a platform, providing proof of a set of the platform's integrity measurements through digital signing. Also, the

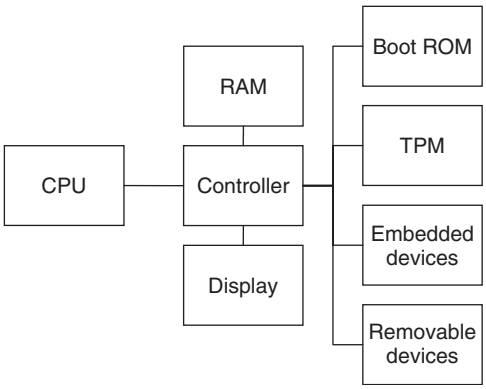



**FIGURE 1** Reference PC platform containing a TPM.

TPM can be used to authenticate a platform, a user, or both. Since the TPM is capable of generating an unlimited number of keys, it can be used to authenticate an unlimited number of identities, but in practice the number of identities is relatively few.

Integrity measurement assesses known platform metrics against the system state, stores this information, and reports it. This function is separated from judging the output, which is reserved for a policy entity. All the integrity measurement has to do is report accurately on the state of the computing platform. To do this, three functions—measurement, storage, and reporting—must be the basis for the roots of trust.

Outside the protected area, other building blocks based on the roots of trust do not have to be shielded. These building blocks include elements that may reside in main memory, core logic, the boot ROM, the processor, and I/O devices (Fig. 2). A combination of the roots of trust and the trusted building blocks constitutes a trusted boundary, within which measurement, storage, and reporting activity can take place. The basic operation consists of measuring an element in its known state, storing that information, and reporting this value when the element is encountered again in an unknown state. If the newly measured value agrees with the stored value, then the element is considered to be in a trusted state.

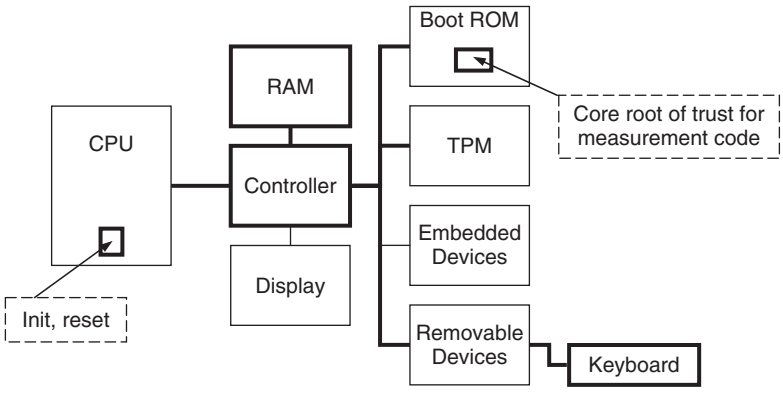



**FIGURE 2** Bold indicates part of the trusted building blocks of a trusted platform.

This basic function can be expanded through a property called *transitivity*. Essentially, the trusted boundary can be expanded if the already-trusted elements are used to attest to the trustworthiness of a secondary set of elements, assuming that the initial state of these secondary elements can be determined to be trustworthy. These secondary elements themselves can then be used to attest to the trustworthiness of a tertiary set, and so on, and the trusted boundary can be expanded theoretically infinitely in a chain of trust, so long as the roots of trust retain their integrity.

An example of transitivity demonstrates how the trusted boundary can be extended through various levels of the computing stack, right up to the application level (Fig. 3).

The TPM is capable of storing mathematically derived representations (hashes) of integrity measurements, which can be compared from time to time or on an event basis with system elements being measured.

A protocol has been established for reporting integrity to a challenger. This protocol involves an exchange of messages between the challenger and the platform, during which an agent on the platform receives the challenge, collects signed information from the TPM, and returns them to the challenger. The protocol is independent of transport and delivery mechanisms and is typical of remote procedure calls, messaging, and communications commonly in use [6].

From this infrastructure, a whole set of credentials can be developed, which allow platforms to gain access to services by disclosing only the minimum amount of identity information. Thus, if a service requires only that a platform be compliant, then it is not necessary to expose to the service the exact identity of the platform, only that it can be reliably said that it meets the compliance requirements. Hence, for example, a mapping service may only need to know that a platform is virus free in order to distribute geographic information to it, not that the platform belongs to a particular entity or individual.

As a communications' endpoint, the TPM is minimally comprised of asymmetric keys, key storage, and processing that protects protocol data items. With these capabilities, the TPM can perform traditional binding (encrypting a message with a public key), signing (using a separate key to compute a hash of the signed message and encrypt it), sealing

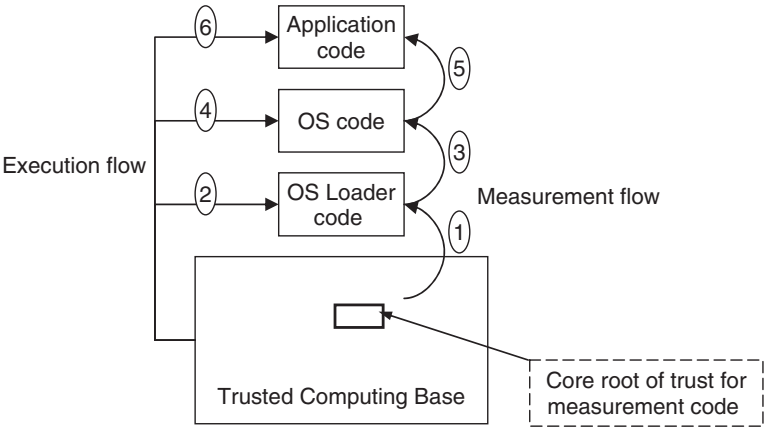



**FIGURE 3** Transitive trust applied to system boot from a static root of trust.

(binding a message further with platform metrics), and signed-sealing (a higher level of verified signing that takes into account the platform's configuration).

### 2.3 Extension to Storage

Although TPMs, despite widespread attachment, have not been put to much use, the architecture has been extended to storage devices successfully. Probably one of the most useful applications for TPM architecture to date has been its implementation in full- and partial drive encryption. Since the chain of trust can be extended to progressively larger areas, widening the trusted boundary, the hard drive is a natural candidate for inclusion inside the boundary.

Hard drives contain, in static form, all the most valuable information on a computer. Particularly given that an increasing proportion of personal computers are now mobile, the hard drive is constantly exposed to potential threats. The portable computer can be outright stolen, the drive can be read through the standard user interface, or its contents can be extracted by various means. It is highly important to encrypt the drive contents in such a manner that the information is readable only by authorized individuals and processes, but it is also critical that this encryption is easy enough to perform and fast enough so that the user is not tempted to eschew it. Drive encryption can be enforced by policy, but it still needs to be sufficiently usable so that ordinary operations can be conducted in a straightforward way. In schema available commercially today, encrypted data is written to the hard drive when the user execute a simple "save," and it is decrypted when the user performs a simple "open." The overhead of the encryption process is low enough so that, with modern high-speed processors, the user barely notices.

### 2.4 Biometric Devices as Physical Interface

One of the key issues with deployment, as opposed to implementation, is that the TPM circuitry is difficult to use. The software available thus far has not been user friendly, and many information technology (IT) managers have, after experimentation, declined to deploy the TPM widely in their organizations, despite its benefits, because of user resistance. This circumstance has left many organizations needlessly vulnerable.

One fairly straightforward way to bring the value of the TPM to the surface of the computer interface is through biometric devices, specifically fingerprint readers. A reader connected to the TPM allows a user to get immediate physical access to the encryption capabilities.

Fingerprint reader suppliers, notably UPEK and AuthenTec, offer software suits that allow a user to tie his or her unique identity to a particular platform without having to remember passwords or carry a secure token. In some circumstances, dual-factor authentication—such as fingerprint and password—may be desirable, but in many cases a fingerprint alone is sufficient.

Although the readers can operate without reference to the TPM, all available models allow for TPM interaction, which is useful since other utilities (e.g. full-drive encryption) may be tied to the TPM. The reader, which resides on the surface of an open laptop near the keyboard, on the keyboard peripheral of a desktop, or in an external device attached via USB connection, is the visible face of encryption, the simple, comprehensible interface through which secure procedures take place.

### 2.5 Usage Model

After failing to reach initial lofty goals of getting the whole world to interact across trusted platforms via standard hardware security, the industry turned to more modest objectives. The goal became to make the single-node experience workable. The areas of focus became user authentication to the platform, most often actuated by fingerprint sensor, file and folder encryption, and password management. File and folder encryption has evolved into full-drive encryption (FDE), which is one of the fastest growing areas of TPM adoption. Because of the hardware implementation, when file and folder encryption is working, the user perceives little latency. Nonetheless, TPM calculations do put a tax on system performance, which will disappear over time as hardware technology improves.

Password management has become the most popular consumer usage. The number of passwords users are called upon to manage has grown along with the Internet, and most people have far more than they can remember, particularly when strong password rules are enforced. It can be a great relief for a user to simply enter the user name and password once, and assign them to a fingerprint-actuated, encrypted password bank. And some utilities can generate strong user-password combinations automatically. Thereafter, the account owner can invoke the site with nothing more than a swipe of the finger. As trusted networking increases, the value of this capability will rise, aided by multifactor authentication backup.

## 3 INTERNATIONAL SCOPE

Over time, the TPM standard has been incorporated into basic technology. Microsoft uses the TPM to drive BitLocker, the FDE solution that the company incorporated into Vista, its mainstream operating system. The company continues to extend BitLocker technology to encompass server and mobile form factors. In the second half of 2008, Intel began including TPM support in high-end dual and quad desktops and advanced chipsets. Seagate offers a TPM-based FDE solution for its drives. Among PC hardware OEMs, TPM penetration has been heavier in commercial client lines and less so in consumer, but ecommerce opens a horizon of potential TPM usage among consumers over time. Virtually all embedded applications on kiosks, ATM machines, and factory automation systems now ship with TPM. In addition, the International Organization for Standardization (ISO) has recently approved the TPM specification. Finally, the governments of most countries in Western and Eastern Europe, including the EU as an entity, in Asia, and in North America have backed TPM architecture.

Support for TPM has been widespread geographically. Manufacturers of modules exist on most major continents, and many hardware OEMs ship systems with TPMs. China, Germany, Israel, Japan, Korea, Switzerland, and the United States all host factories that produce chips incorporating TPMs in various ways. TPM circuitry has been produced widely as a dedicated module and has also been realized as an integrated part of other subsystems, such as the processor, I/O chip, or core logic.

### 3.1 Integration

The inexorable economics of trusted computing rests on the simple idea that the wider the standard the better. It is not so much what the standard is exactly as the fact that

it is a standard at all. That is what makes the long-term adoption of this schema for secure storage and transmission of data more likely. As the volume rises, so the likelihood of incorporation in basic silicon, the way Intel has done. Thus, the modules are "free" in the sense that they come with, are there anyway, no extra charge, whether or not they are activated. A sufficiently large transistor budget, thanks to improved silicon processes, has made it simple to add the circuitry to core logic. Over time, this integration will likely lead some of the specialty subsystem vendors to leave the TPM market, but good arguments remain for others to continue to supply discrete modules. Funding in building the trusted stack will thus largely come from vendors in the field, with broad agreement about the architecture by participants and regulatory authorities.

### 3.2 Trusted Software

Software is readily available from many hardware OEMs and some software-only companies. Net-net, the interface, could stand an upgrade. Some of the lack of utilization by patrons of systems shipped with TPMs is due to poor usability. Nonetheless, hardware vendors such as Dell, Hewlett-Packard, and IBM, and software vendor Wave Systems all provide suites for individual and networked platform environments.

### 3.3 Networking Trusted Platforms

Another important and related TCG standard is Trusted Network Connect (TNC), which defines a protocol for any network element to conduct a dialog with any other over a trusted Internet Protocol (IP) network. This technology is in the infancy of its adoption, but long term it provides a powerful basis for ecommerce.

Essentially, a user is authenticated to a platform and a network, and the combination of the user and platform information becomes the basis for a grant of rights and privileges within a trusted network (Fig. 4). Authentication is performed via biometric, often fingerprint, and system information is read. The hash of this calculation becomes the stored value, which has to match on future entries. If it does not, the requestor can be denied entry. The technology is fine-tuned enough so that the concept of quarantine can be introduced. A system can be deemed friendly, but damaged; that is, it might be recognizable, but, for example, its virus signature file is out of date. This system can be granted provisional entry to a quarantined site, where it can be remediated, the virus definition file topped off, or whatever else needs to be done to prepare it for a retry. If it passes after remediation, it is granted its full rights and privileges, even if it is a mobile system connecting over wireless (Fig. 5).

For purchasing purposes, the Department of Defense (DoD), Office of the CIO, is on a several year program, moving toward requiring three infrastructure elements on all clients: a smart card, a fingerprint reader, and TNC connect activated through a TPM. This development is significant because DoD requirements are typically pushed out to contractors and vendors, expanding penetration.

In addition, the National Security Agency (NSA) has approved the TPM for its multiyear "high-assurance program" (HAP), a framework for next generation computing platforms. The effort has involved representatives from industry, academia, and other institutions, who are assembling a series of recommendations. HAP members are working

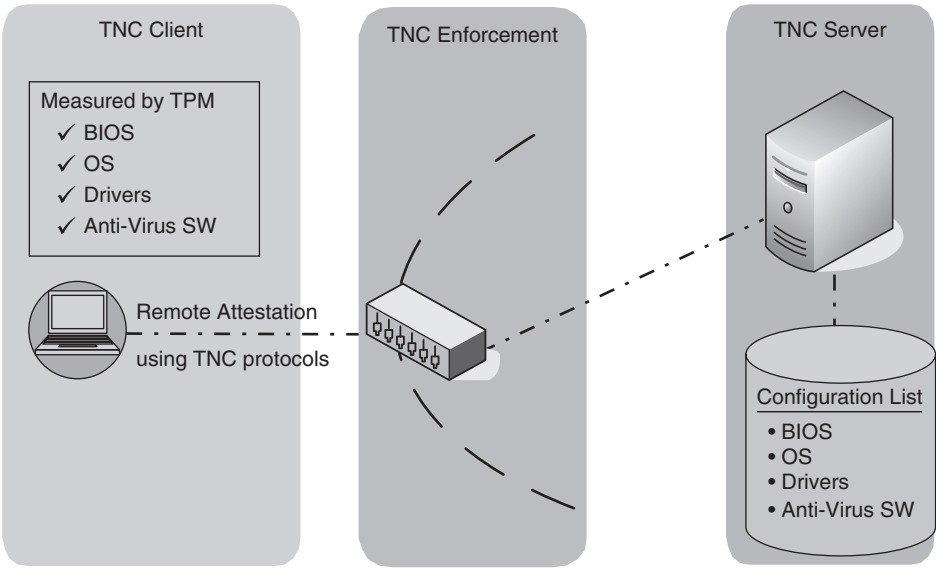



**FIGURE 4** Trusted hardware via the TPM and remote attestation via TNC verify critical client software.

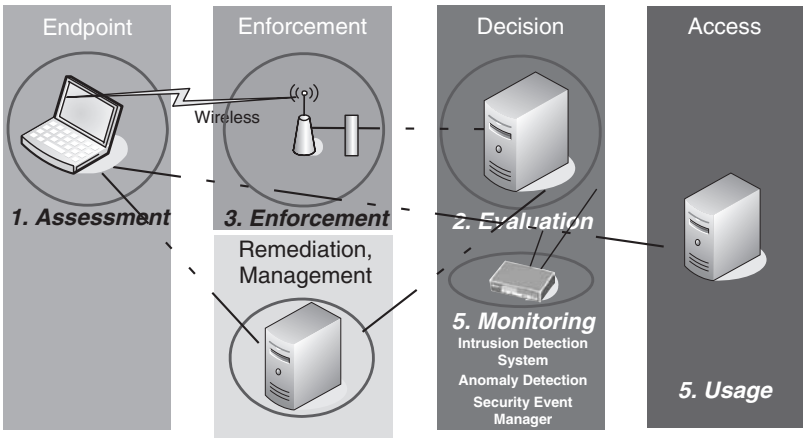



**FIGURE 5** Nodes with various roles challenge the endpoint. Its credentials are evaluated, policies are enforced, remediation occurs as necessary, and ongoing monitoring ensures that the endpoint's credentials remain valid.

with vendors to generate products and create initial applications for three levels of security clearance. With virtualization, these HAP platforms will allow three virtual machines, of varying levels of security, to reside together in a single physical computer. Each virtual machine will use its own TNC credentials to gain access to different networks, depending on its rights and privileges [7].

## 4 EXPANDING THE RING OF TRUST

The trusted computing base, grown as the rings of trusted computing expand, can be extended to vast networks, once the infrastructure is established, providing an umbrella under which eCommerce can be conducted safely. Any extension of trusted architecture benefits the whole. Any node can trust any other node. Friends and enemies are distinguishable. They can be sorted or not, depending on the need.

Thus, promoting the standard is advisable for the U.S. government, specifically with reference to homeland security and counterterrorism departments. Standards can be enforced within specific agencies as the need suggests itself. With an increasingly mobile workforce, trusted architecture can speed and secure remote access by laptops, which often seek a network connection from an unknown address.

While it is true that enemies can also conduct secure conversations and pass around secure communications among themselves, this behavior itself is indicative, and those who are interested can monitor those particular behavior patterns quite closely. Metadata, you could call them, information about the information. That notwithstanding, the value of the open use of common secure architecture outweighs the cost of allowing potentially unfriendly parties to use the same technology.

## 5 REMAINING CHALLENGES

Of course, every system is fallible, but it is useful to think of some helpful secrets sufficiently costly to crack so as to discourage all but the most determined adversary. It is not that back doors are built into these implementations of secure base computing. It is that by their nature, all secrets are subject to discovery. While the potential domain of keys in random space may be large enough to dissuade casual search, that space may be subject to preprocessing designed to intelligently limit it to a smaller portion for brute force hammering. Such techniques, when well funded, can yield results.

Thus, cracking a code could be a $64 problem or a $1 million problem. When the cracks start hitting $10 million, commercial entities back off. Only governments and very focused, well funded players remain in the game. And the stakes are generally small on any given device. Even given that valuable trade secrets reside on hard disks and credit card numbers are bought and sold on the open market, the average hard drive will yield information likely priced in the few hundreds of dollars, if that.

So, with the template for the infrastructure mostly in place, it is reasonable to ask why trusted base computing has not been more widely adopted by the public; that is, utilized, put into service, by IT departments and end users. Some industry watchers put the blame on lack of basic demand, saying the standard is being pushed by the industry and has no core constituency in IT departments and among users [8]. The real answer is probably somewhat less crisp. In fact, software needs to be made easier and public awareness increased. The whole trusted experience needs to be made smoother, and people find it difficult to imagine a capability they knew nothing about previously. The government could take a leading role here, creating a unifying voice. The cost is converging on negligible, and it will soon be included anyway.

Some of the attitude toward authentication and security is in flux in post-9/11 American culture. Before the attack, Americans ranked privacy at the very top of rights they valued,

whereas afterward their right to be proven who they are gained in stature. People want to be known as themselves. If they have to sacrifice a degree of privacy to achieve a clear identity, the cost seems relatively small compared to the value gained. For example, if swiping a finger on a reader gave a traveler rapid access to the flight areas of an airport, speeding the process through security, many users would agree to register a fingerprint.

The government should look at funding the promotion of trusted standards in wide usage. The flourishing of secure eCommerce alone promotes the interests of the United States, which is then the host to a leading-edge technical and social development. Over time, this ideal eCommerce infrastructure can be promoted to international audiences.

## REFERENCES

1. Yin, Y. L. (Ed.) (2004). *IEEE 1363-2000: Standard Specifications For Public Key Cryptography*, http://grouper.ieee.org/groups/1363/P1363/index.html.
2. Becker, P. (2004). *CoreStreet Cuts the PKI Gordian Knot, Digital ID World*, p. 22. http://magazine.digitalidworld.com/Jun04/Page22.pdf.
3. Trusted Computing Group membership, Website: https://www.trustedcomputinggroup.org/about/members/, 2008.
4. Shannon, Claude E. 1950. Prediction and entropy of printed English. *Bell Syst Tech J* **30**, 50–64.
5. Kay, Roger L. The Coming of Age of Client Security Technology, IDC, January 2003, P. 13.
6. Rotondo, S., Hammersley, J., Kotani, S., Balacheff, B., Perez, R., Rosteck, T., Vishik, C., Challener, D., Jong-Chen, J. D., Thibadeau, B., Berger, B., 2007. *TCG Specification Architecture Overview*.
7. NSA High Assurance Program. (2008). http://www.nsa.gov/ia/industry/HAP/HAP.cfm?MenuID=10.2.1.6.
8. IDC, Trusted Platform Module (TPM): Adoption Dynamics, by John Daly, Roseann Day, Charles Kolodgy, Bob O'Donnell, Shane Rau, and Bill Roch, August 30, 2006.

## FURTHER READING

Tamvada, J. H. 2007. *Posture of an End Point*, Helsinki University of Technology. Framingham, MA. http://www.tml.tkk.fi/Publications/C/25/papers/Tamvada_final.pdf.

Mayne, M. NAC: Growing pains, SC Magazine UK 2008. http://www.scmagazineuk.com/NAC-Growing-pains/article/112204/.

Santha, M., Vazirani, U. V. *Generating quasi-random sequences from slightly-random sources*. Proceedings of the 25th IEEE Symposium on Foundations of Computer Science: pages 434–440, University of California. October, 24, 1984. ISBN 0-8186-0591-X.

von Neumann, John (1963). Various techniques for use in connection with random digits. In *The Collected Works of John von Neumann*, Pergamon Press, Sunnyvale, CA. pp. 768–770. ISBN 0-08-009566-6. http://www.merrymeet.com/jon/usingrandom.html.

# HIGH ASSURANCE: PROVABLY SECURE SYSTEMS AND ARCHITECTURES

RANCE J. DELONG
*Santa Clara University, Santa Clara, California and LynuxWorks, San Jose, California*

## 1 INTRODUCTION

The need for high assurance provably secure systems and architectures is ever increasing due to the severity of the consequences of failure in critical cyber-physical systems and to the motivation of our adversaries to exploit those systems.

## 2 SCIENTIFIC OVERVIEW

### 2.1 Concepts of High Assurance Secure Systems

A *system* is an assembly of hardware and software that exhibits specific functional and nonfunctional properties. A *secure system* is one that, in addition to fulfilling its primary functional purpose, behaves in accordance with a security policy. The primary function delimits useful behaviors that give the system its reason for existence. Secure behaviors may be achieved by mechanisms that implement security functionality, such as authentication and access control, or by architectural structures that, without adding functionality, constrain the behaviors of a system to those that satisfy the desired security policy. To be considered secure, a system must be robust enough to resist attempts to violate the policy. Robustness may be achieved by requiring specific attributes of the design, implementation, or configuration, in concert with functionality that governs the behavior of the system at runtime to avoid actions that violate the security policy.

Unlike functionality, which often may be added or removed without affecting other features, security is a total system property, determining the legality of actions or states within the context of the system as a whole. The security properties of individual components of a system do not necessarily enable us to infer the security of the system as a whole.

Furthermore, security dictates that the system's behaviors comprise specified requirements *and nothing else*. This is a characteristic security shares with safety. Traditional approaches to safety strive to make a system robust in the face of probabilistic failures, while those for security strive to assure that a system is robust in the face of deliberate actions of intelligent and malicious agents. These considerations are not independent. In contrast with improbable random failures, a malicious agent can cause an otherwise improbable condition to occur with certainty. However, the similarities between safety

and security are too great to ignore, particularly considering that many safety-critical systems are subject not only to naturally occurring adverse phenomena but also to threats posed by deliberate human actions. Though typically pursued using distinct disciplines, it is advantageous to unify security and safety objectives and to pursue them together using common methods and tools.

### 2.2 Assurance as a Security Metric

It is said that in order to manage or control something it is necessary to measure it. Appropriately, to determine whether or not security has been achieved, to compare the security merits of alternatives, and, indeed, to manage the very pursuit of security a measure of security is needed. While security functionality is measured much as any other functionality, the system property of security requires a measure that reflects the *trustworthiness* of the system. That role has been filled by *assurance*: the basis for confidence that a system does what it is supposed to do, and does not do what it is not supposed to do. Reliance on assurance as a measure of security is based on the presumption that one could not produce assurance for the security of a system if it were not in fact secure.

Assurance is characterized as high, medium, low, or none, depending upon the extent of the evidence supporting the finding. *Assurance activities* are processes followed and analyses performed in the development or assessment of a secure system. Diverse assurance activities apply to each phase and aspect of development, for example requirements management, implementation standards, inspections, walkthroughs, formal verification, and testing. Traditional assurance activities are the result of experience, supposition, and anecdote, some having a dubious connection to the quality of security. As the needed level of assurance increases, the rigor of assurance activities increases, and the basis for confidence should be made explicit. Future research should strive to replace assurance activities that are costly and of dubious value with those having perspicuous connections to the practical security of a system.

### 2.3 Assessing Security: Evaluation, Certification, and Accreditation

The assessment of security amounts to judging the appropriateness of security functions and the evidence supporting confidence in claimed security properties. Products with a security component are individually subject to security *evaluation* according to the Common Criteria [1] or, for cryptographic components, *certification* according to FIPS PUB 140-2 [2]. Entire systems used in Department of Defense (DoD), intelligence, or other national security applications must undergo security *certification and accreditation* (C&A), a process through which the risks associated with operating a system in a particular environment are assessed, managed, and determined to be acceptable by a designated authority.

Security assessments, whether of products or systems, would not be useful if they did not have objective validity. Consequently, they are performed by independent experts according to established standards and repeatable assessment methodologies.

As a practical matter, production and assessment of assurance evidence are distinct activities. Developers of a system are uniquely positioned to produce the evidence, particularly for high assurance systems, since the evidence should be produced *during development*. According to the Common Criteria, evaluation confirms "that the

information provided [by the developer] meets all requirements for content and presentation of evidence." Evaluators are trained and approved to perform evaluations by a governing body, in the United States by the Common Criteria Evaluation and Validation Scheme (CCEVS).

C&A practices differ among the DoD, the intelligence community, and other government agencies, and often within those communities, making the C&A process a labyrinth. Efforts are underway to unify these practices through the Director of National Intelligence (DNI) CIO C&A revitalization effort [3].

### 2.4 Techniques and Tools for High Assurance

Specialized techniques and tools, and intricate and expensive processes are employed to develop systems with assurance. The highest form of assurance is widely recognized to be that which results from the use of *formal methods*, viz. analyses that establish a direct logical connection between security claims and objective supporting evidence. Formal verification requires a proof that a system possesses a certain property, or is free from a certain kind of flaw.

There are interactive and automated verification methods, each with its strengths and limitations. Other, less rigorous analyses may help to find certain kinds of bugs, but cannot guarantee the absence of bugs. A particular analysis method may be oriented toward a particular kind of property. Suppose we are interested in the property "free of buffer overflows." To perform the analysis one could determine the program features that characterize buffer overflow vulnerabilities, and then search for occurrences within a program of patterns that match those features. A failure to find matching occurrences supports the claim that the program is "free of buffer overflows." If the analysis is *sound*, then when it identifies a buffer overflow, we know it really is a buffer overflow. If the method is *complete*, then we know it will not fail to find a buffer overflow. Only the simplest of such analyses may be both sound and complete. Many analyses are either unsound, incomplete (or both), resulting in imprecision that manifests as false positives (indicating occurrences that are not real problems) and false negatives (failing to find real problems).

Verification requires the construction of a formal model of the system, a formal specification of the properties of interest and of a formal proof showing that the system model exhibits the specified property. The formal model is typically not the actual code but an abstraction of it. The executable code for the system should be developed to correspond closely to the formal model so that there is assurance that the proven properties are preserved in the implementation. Methods that can examine the code itself permit direct verification of the code. Often, the size and detail of the implementation make a direct proof of the code infeasible, and correspondence between the formal model and the code must be established by manual inspection or other informal processes. The Common Criteria, even at the highest assurance level, do not require a formal proof of correspondence between the code and the model. Special implementation languages and techniques, as well as advances in formal verification tools, are making feasible the formalization of the code to model correspondence.

Of central importance to verification is the property or properties to be verified. If the property is simple, the specification of the property may be a "one liner." If total functional correctness is desired, then the specification of the property may be of comparable size to the code. Fortunately, the properties of interest for security may often be

represented in a small number of lines of formal specifications, and only a portion of a system is security enforcing. In fact, it is known that many useful security policies can be reduced to assertions over the state of a system that can be checked by an execution monitor [4].

Formal method techniques and their supporting tools fall roughly into these categories: interactive and automated theorem proving, model checking, abstract interpretation, and other static and dynamic analyses. Interactive theorem proving is labor intensive, and, while it has experienced advancements over the decades, the changes brought about by new technologies, such as decision procedures, SAT solving (boolean satisfiability) [5], SMT solving (satisfiability modulo theories) [6], and model checking [7], have created a disruptive effect on the field, automating more of the verification activity. Model checkers, though subject to the state explosion problem, have increased in performance and can now handle much larger state spaces; and strategies such as abstraction and bounded model checking can cope with infinite state problems. SMT solvers and constraint solvers provide effective automation to a broader range of satisfiability problems.

Each technology has its strengths and weaknesses, and in yearly competitions developers pit their tools against each other. Future research may produce disruptive advancements from the fine-grained application of multiple methods interoperating in novel, mutually supportive combinations [8, p. 5].

### 2.5 Secure Architectures

Many of the principles that apply to systems apply also to architectures, if we regard an architecture as a class of systems that share the same early, or high level, design decisions. Abstractly, an architecture identifies a set of components, their interfaces, and their interactions. An architecture is an underspecified system, in that the details of the components are not specified. Normally, all details of a system design and implementation are considered in the performance of a complete security assessment. We are interested in how an architecture, as an underspecified system, can be said to be secure.

To say that an architecture is secure, one of two conditions must be met. Either the security properties of the architecture are independent of the details of the underspecified portions, or the security of the architecture can be proven by making assumptions concerning particular properties of the underspecified portions. Then, the security of a system based on the architecture is contingent upon proofs that the components corresponding to the underspecified portions possess the assumed properties.

## 3 RESEARCH INITIATIVES WORLDWIDE

Many countries have research programs in high assurance security. Following are a few of these initiatives in the United States and worldwide.

### 3.1 In the United States

Many high assurance security initiatives in the United States, as elsewhere, originate with defense acquisitions, but there are several noteworthy initiatives intended to substantially improve the practice of system security across a broad range of application areas.

Since November 2006, a series of workshops sponsored by NSF, DHS, IARPA, NSA, ONR, and OSD have considered the broad problems of security facing the nation, and approaches that might yield revolutionary improvements. Ranging in size up to 80 invitees, the workshops included many of the leading security experts in the nation. This ongoing activity is intended to produce a research agenda that is highly relevant to current and projected problems, and a "grand challenge" project to showcase the research results. The first meeting, the NSF Safe Computing Workshop, held in November 2006 resulted in an affirmation that the computer security ills facing the nation are real but curable with an appropriate application of resources. Subsequent meetings have elaborated prospective research thrusts. At the NCDI Workshop on Game-Changing Solutions for Cyber Security, in November 2007, 72 technology proposals in 18 topic areas were presented by the attendees.

The DoD sponsors research efforts through DARPA, NSA, NRL, AFRL, and ARL (the Navy, Air Force, and Army Research Labs, respectively) intended to advance high assurance security for application to DoD programs. These efforts include the MILS (Multiple Independent Levels of Security) initiative, the HAP (High Assurance Platform) program, the high robustness VMM (virtual machine monitor), and the Trusted Computing Exemplar (TCX).

The MILS initiative, promoted by AFRL and pursued by a coalition of vendors, integrators, and research labs, seeks to develop a marketplace for high assurance COTS components [9–11]. High assurance MILS systems, providing robust enforcement of application-level and system-level security policies, may be constructed from components in a layered compositional approach. MILS applications are being researched at the University of Idaho under sponsorship from NSA, and MILS theoretical foundations are being researched at SRI International under sponsorship from AFRL and Raytheon. Applied research and MILS product development are being performed by a number of product vendors, including Galois [12], Green Hills [13], LynuxWorks [14], Objective Interface Systems (OIS) [15], real-time innovations (RTI) [16], and Wind River [17].

The HAP Program [18], sponsored by NSA, seeks to develop a well-defined platform architecture that can be built from COTS hardware components, and securely provide access to COTS applications by running COTS operating systems within virtual machines. Specifications have been written for HAP security functions and subsystems, and prototypes have been developed. A series of HAP releases, with increasing levels of assurance and capability, are currently being developed. HAP, a successor to the NSA's NetTop project, is currently being performed by General Dynamics, IBM, and other vendors.

The High Robustness VMM project, being pursued at NRL, seeks to develop a robust VMM by analyzing the open source Xen hypervisor [19] to identify a provably secure subset that can then be enhanced with security features to meet military requirements. "The NRL project has two goals: (i) demonstrate the usefulness of VMMs for realistic security applications and (ii) using Xen, demonstrate how the US Navy, the DoD, and other enterprises with high robustness security requirements can take advantage of open source technology [20, p. 1]."

Since most existing instances of high assurance systems are proprietary and not available for study by students and other developers, the methods remain esoteric and the industry's ability to build such systems falls far short of the demand. The TCX Project, being performed at the Naval Postgraduate School, intends to "provide an openly distributed worked example of how high assurance [sic] trusted computing components can

be built [21, p. 109].” The reference implementation will be taken through high assurance evaluation.

Vendors such as Intel, AMD, IBM [22], and VMware [23] have research programs that include advanced virtualization support and secure hypervisors, while Secure64 [24] is delivering a hardened DNS server based on a small, robust operating system and communication stack.

Finally, Microsoft, though at one time widely maligned for the frequent crashes of the Windows operating system, has taken a prominent role in the assurance research community, with theoretical contributions and a variety of sophisticated tools developed at Microsoft Research [25] that are deployed in the company’s day-to-day software development practice.

In networking, two projects are concerned with the next-generation global communication infrastructure: Global Environment for Network Innovations (GENI) [26], sponsored by NSF, and Stanford University Clean Slate [27], sponsored by NSF and industry. Clean Slate intends to explore designs for the Internet in 15 years. Unlike the original Internet design, these research projects consider security to be an integral element of proposed designs.

### 3.2 Around the World

There are a number of national high assurance system initiatives, such as Germany’s Verisoft and Australia’s L4.verified projects. Similar initiatives are being pursued in Great Britain, France, Italy, and Japan.

The Verisoft project [28] is a long-term project funded by the German Federal Ministry of Education and Research (BMBF). “The main goal of the project is the pervasive formal verification of computer systems. The correct functionality of systems, as they are used, for example, in automotive engineering, in security technology, and in the sector of medical technology, is to be mathematically proved.” [28] The project has produced a verified processor and is working on the software stack.

L4.verified is a collaborative effort of the Australian Government Department of Defense DSTO (Defense Science and Technology Organisation), NICTA (National ICT Australia Limited), and the University of New South Wales. “The L4.verified project is developing a mathematical proof that the seL4 microkernel does exactly what it is intended to do.” [29] The seL4 kernel [30] is a secure version of the internationally known L4 microkernel [31].

Another noteworthy, truly international effort is the Verified Software Initiative (VSI), a series of international conferences and research efforts dedicated to “making verified software a reality within the next 15–20 years.” [32–35] The VSI was inspired by Sir Tony Hoare’s exhortation [36] to take up the goal of developing a verifying compiler as a scientific grand challenge for computing.

## 4 CRITICAL NEED ANALYSIS

Provably secure systems and architectures support critical needs of homeland security and counterterrorism. Their deployment in critical infrastructures can help to avoid mass disruption and crippling economic consequences; and, in military command and control systems to prevent the disabling, degrading, or usurping of military information and

weapon systems. Secrets obtained by hostile nation states or terrorists from the compromise of government or industrial computer systems could be used to harm the country diplomatically, economically or militarily. Subversion during development is a threat as well.

### 4.1 Critical Domestic Infrastructures

Security assessments have demonstrated vulnerabilities in the information systems that control and supervise the resources and processes of the nation's critical infrastructures, such as power, gas and water utilities, transportation systems, financial systems, SCADA (Supervisory Control and Data Acquisition) systems, and Internet-based supply chain support for commerce. Successful hacker or cyber terrorist attacks against these and other systems could wreak economic havoc and jeopardize lives. These infrastructure systems should be hardened, as should be tactical military systems, since in the post-9/11 world they must be viewed as prime targets of cyber-warfare and cyber-terrorism.

### 4.2 Counterterrorism—Critical Intelligence Sharing

A key finding of the 9/11 commission was that government agencies, such as law enforcement and intelligence agencies, did not effectively share information that might have thwarted the terror plot. While directives have subsequently been issued to rectify some of these inadequacies, effective technical measures are still needed to fully enable controlled information sharing. To share information, systems must be connected; to increase connectivity is to increase risk as systems are exposed to users having a range of authorizations. A system must be able to effectively control information whenever any of its users are unauthorized to access all of the information managed by the system. Such a user must be presumed to pose a threat of compromise, and the mechanisms that protect against unauthorized access must be strong enough to withstand a determined and skillful attack.

### 4.3 Contributions from High Assurance Secure Systems

Critical systems must be exceptionally dependable and robust against attack. The Department of Homeland Security's project, "Build Security In" [37], provides "resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development." Initially, this project is focused on the low-hanging fruit of COTS software and commercial low to medium assurance practices, but it calls for collaboration from the community to broaden and deepen the resources presented. The aforementioned MILS and HAP initiatives are stimulating the emergence of affordable technologies that are robust by design and provably secure.

Network-based communications and transactions are even more pervasive and sophisticated. New protocols for such interactions are being designed and deployed regularly. They employ cryptographic operations that must be used appropriately, and the supporting cryptographic mechanisms must be securely embedded into the systems implementing the protocols. Experience has proven that even simple protocols can be wickedly difficult to design without introducing subtle vulnerabilities. Such protocols, and their supporting mechanisms, should be formally analyzed and verified.

## 5 RESEARCH DIRECTIONS

### 5.1 Foundations for Composable High Assurance Systems and Architectures

Previous studies and reports, such as [38] on composable high assurance secure systems, should be pursued to further the field's rigorous theoretical foundations and practical applications. The report urges "establishment and use of soundly based, highly disciplined, and principle-driven architectures, as well as development practices that systematically encompass trustworthiness and assurance as integral parts of what must become coherent development processes and sound subsequent operational practices. Only then can we have any realistic assurances that our computer-communication infrastructures—and indeed our critical national infrastructures—will be able to behave as needed, in times of crisis as well as in normal operation [38, p. ix.]."

### 5.2 Science of Certification

Corresponding to the need to build high assurance systems, there is the need for their effective and timely certification. The classical methods of certification used in security and safety are being taxed by the escalating demands. High assurance certifications of software systems can cost much more than developing the software. Complex and dynamic systems and systems-of-systems simply cannot continue to be certified in the labor-intensive and time-consuming ways of the past, which require scrutiny of the details of every component of the system as well as the structure and function of the system as a whole. A science and logic of certification would enable component-wise, incremental, and just-in-time certification [39]. The needs of both system construction and certification can be met by principled construction methods that produce, as a natural byproduct, the evidence needed for certification and a science of certification would provide the quantitative methods to combine the evidence and reach a certification judgment.

### 5.3 Formal Verification of Critical Properties of Systems

High assurance and provable security depend upon formal methods to model systems and to model and verify the properties that they are intended to exhibit. Such methods have often been very expensive to apply and have come to be considered limited in applicability to relatively simple systems. It should be noted that techniques to overcome such limitations were published in the 1970s! [40]. Technical advancements over the past decade have set the stage for disruptive innovation in formal verification [8]. Interactive theorem proving, the well-established but labor-intensive staple of formal methods, is now accompanied by powerful and highly automated methods, such as SMT, model checking, abstract interpretation, and counterexample-guided abstraction refinement [8]. Needed now are frameworks in which to combine the powerful new methods and tools in more automated ways to attack the old problems more comprehensively, and new, larger problems. The effective combination of methods through communication and interaction frameworks could dramatically advance further research and the power that could be delivered to practitioners.

### 5.4 Verified Software Initiative/Verified Software Repository

The aforementioned Verified Software Initiative has adopted a goal to establish a world-wide Verified Software Repository (VSR) [41].

### 5.5 Integrated Development Environments for High Assurance Systems

Developer tools have been combined through graphical user interface (GUI) to provide developers with unprecedented productivity for conventional software. Such integrated development environments (IDEs) must be extended with tools for high assurance development.

### 5.6 Design Patterns for Provably Secure Systems and Architectures

The monumental effort that goes into proving a system or architecture should be leveraged through reuse of secure design patterns and architectures [42–44].

### 5.7 Test Beds for Development, Integration, and Study of New Approaches

The research community should go beyond publications to share ideas and build on past results. Test beds for providing the integration of experimental systems would enable researchers to build on others' results in a concrete way. This capability would accelerate advancement and lead to innovative new ways of combining current technologies.

### 5.8 Open Source Examples of High Assurance Development

The demand for high assurance security has far outstripped the capacity of the industry to provide provably secure systems and architectures. Most software engineering curricula and development programs for practicing professionals do not teach the principles and methods of high assurance development. Those who are given the task of developing such systems have no obtainable examples upon which to pattern their work, because the few existing examples are proprietary. The aforementioned TCX project is the first of many needed examples. Future research projects should endeavor to go beyond simple examples in areas such as the design and implementation of protocols and cryptographic algorithms.

### 5.9 Next-Generation Processors and Networking Infrastructures

Contemporary processors and networking infrastructures evolved in an environment in which security was not a primary concern. Performance, features, and ease of implementation were the driving factors. Without assurable security as an imperative, these technologies have evolved to a state far from optimal, and in some respects outright inadequate, for the achievement of high assurance and provable security. The dilemma we now face is the enormous investment in the current infrastructure and the procrustean bed of backward compatibility. Research such as GENI and Clean Slate hold promise for networking.

Future processor design must better support high assurance security. The large vendors have had little incentive to undergo high assurance evaluation of their processor designs. The lack of independently evaluated proofs of hardware has left software system verification with an incomplete basis for confidence. The Verisoft project developed a new processor so that every detail of the hardware would be known and could be verified. Since the x86 architecture may reasonably be expected to continue to be dominant, the verification of such processors would be welcomed by the high assurance security community. A preliminary study done by the University of Texas at Austin and Centaur

Technology, a supplier of x86-compatible microprocessors, demonstrates the feasibility of a fully verified commercial microprocessor design [45]. It would be a great benefit to those attempting to develop high assurance and provably secure systems if other hardware vendors were to undertake similar efforts.

## 6 CONCLUSION

We have seen that critical systems are growing in complexity and facing escalating security challenges. The need for high assurance provably secure systems and architectures is ever increasing. We have surveyed concepts in assurance and techniques for achieving it. We presented examples of what has been achieved in the past, what is being pursued currently, and what are the challenges that research must still meet. The cited examples of ongoing research and development efforts represent only a snapshot in time. The field of provably secure systems is evolving rapidly in terms of both challenges and technologies.

## REFERENCES

1. *Common Criteria for Information Technology Security Evaluation*, Version 3.1, CCMB-2006-09-001, -002, -003, September, (2006).
2. Federal Information Processing Standards Publication (2001). *FIPS PUB 140–2 Security Requirements for Cryptographic Modules*. National Institute of Standards and Technology. Gaithersburg, MD.
3. *FAQs for the C&A Revitalization*, http://www .dni.gov/canda/blogs/faq.html, 2008.
4. Hamlin, K. W., Morrisett, G., and Schneider, F. B. (2003). *Computability Classes for Enforcement Mechanisms*, Technical Report TR2003–1908, Cornell University, August 2003.
5. Zhang, L. and Malik, S. (2002). The quest for efficient boolean satisfiability solvers. *CADE-18*, Lecture Notes in Computer Science, Vol. 2392, Springer, Berlin, Germany, , pp. 313–331.
6. Sebastiani, R. (2007). *Lazy Satisfiability Modulo Theories*, Technical Report #DIT-07-022, University of Trento, April 2007.
7. Clark, E. M., Grumbert, O., and Peled, D. A. (1999). *Model Checking*. The MIT Press, Cambridge, MA.
8. (a) Rushby, J. (2007). Automated formal methods enter the mainstream. *Commun. Computer Society of India* **31**(2), 28–32; (b) (2007). *J. Univ. Comput. Sci.* **13**(5), 650–660.
9. Vanfleet, W. M., Beckwith, R. W., Calloni, B., Luke, J. A., Taylor, C., and Uchenick, G. (2005). MILS: architecture for high assurance embedded computing. *CrossTalk* **18**, 12–16.
10. Alves-Foss, J., Harrison, W. S., Oman, P., and Taylor, C. (2006). The MILS architecture for high-assurance embedded systems. *Int. J. Embed. Syst.* **2**(3/4), 239–247.
11. Boettcher, C., DeLong, R., Rushby, J., and Sifre, W. (2008). The MILS component integration approach to secure information sharing. *Presented at 27th IEEE/AIAA Digital Avionics Systems Conference (DASC)*, St. Paul MN, October 2008, www.csl.sri.com/users/rushby/abstracts/dasc08.
12. www.galois.com, 2009.
13. www.ghs.com, 2009.
14. www.lynuxworks.com, 2009.
15. www.ois.com, 2009.
16. www.rti.com, 2009.

17. www.windriver.com, 2009.
18. www.nsa.gov-index.shtml, 2009.
19. Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., and Warfield, A. (2003). Xen and the art of virtualization. *SOSP'03, October 19–22, 2003*, Bolton Landing, New York. ACM 1—58113—757—5/03/0010.
20. McDermott, J., and Kang, M. (2006). An open-source high-robustness virtual machine monitor. *ACSAC 2006*, Miami Beach, FL, www.acsac.org/2006/wip/ACSAC-WiP06-06-McDermott-WIP0.pdf.
21. Irvine, C. E., Levin, T. E., Nguyen, T. D., and Dinolt, G. W. (2004). The trusted computing examplar project. *Proceedings of the 5th IEEE Systems, Man and Cybernetics Information Assurance Workshop*. United States Military Academy, West Point, NY, pp. 109–115.
22. www.research.ibm.com/secure_systems_department/projects/hypervisor/, 2009.
23. www.vmware.com, 2009.
24. www.secure64.com, 2009.
25. (a) http://research.microsoft.com/slam; (b) http://research.microsoft.com/SLAyer; (c) http://research.microsoft.com/TERMINATOR, 2009.
26. www.geni.net, 2009.
27. http://cleanslate.stanford.edu, 2009.
28. www.verisoft.de, 2009.
29. http://nicta.com.au/research/projects/l4.verified/, 2009.
30. http://nicta.com.au/research/projects/secure_embedded_l4, 2009.
31. *System Architecture Group, Department of Computer Science. L4 eXperimental Kernel Reference Manual*, Revision 5. System Architecture Group, Department of Computer Science, University of Karlsruhe, Karlsruhe, Germany, , 2004.
32. Jones, C., O'Hearn, P., and Woodcock, J. (2006). Verified software: a grand challenge. *IEEE Comput.* 93–95.
33. Shankar, N. (2005). *The Challenge of Software Verification*. HCSS, ftp://ftp.csl.sri.com/pub/users/shankar/HCSS05.pdf.
34. Meyer, B., and Woodcock, J. (Eds) (2005). Verified software: theories, tools, experiments. *Proceedings of the First IFIP TC 2/WG 2.3 Conference, VSTTE 2005*, *Lecture Notes in Computer Science*, Springer, Zurich, Switzerland, Berlin, Vol. 4171, October.
35. Shankar, N. and Woodcock, J. (Eds) (2008). Verified software: theories, tools, experiments. *Proceedings of the Second International Conference, VSTTE 2008*, *Lecture Notes in Computer Science*, Springer, Toronto, Canada, Berlin, Vol. 5295, October.
36. Hoare, C. A. R. (2003). The verifying compiler: a grand challenge for computing research. *J. ACM* **50**(1), 63–69.
37. https://buildsecurityin.us-cert.gov/daisy/bsi/home.html, 2009.
38. Neumann, P. G. (2004). *Principled Assuredly Trustworthy Composable Architectures*, Final Report, Contract number N66001-01-C-8040, DARPA Order No. M132, SRI Project P11459, December 28.
39. Rushby, J. (2007). Just-in-time certification. *12th IEEE International Conference on the Engineering of Complex Computer Systems (ICECCS)*, Auckland, New Zealand, July 2007, pp. 15–24.
40. Robinson, L., and Levitt, K. N. (1977). Proof techniques for hierarchically structured programs. *Commun. ACM* **20**(4), 271–283.
41. Bicarregui, J. C., Hoare, C. A. R., and Woodcock, J. C. P. (2006). The verified software repository: a step towards the verifying compiler. *Formal Aspects Comput.* **18**, 143–151. DOI 10.1007/s00165-005-0079-4. Springer.

42. Blakley, B., and Heath, C., (2004). *Members of The Open Group Security Forum. Introduction to Security Design Patterns*. The Open Group. Reading Berkshire, UK.

43. Kienzle, D. M., Elder, M. C., Tyree, D., and Edwards-Hewitt, J., (2009) *Security Patterns Repository Version 1.0*, http://www.scrypt.net/~celer/securitypatterns/.

44. Moriconi, M., Qian, X., Riemenschneider, R. A., Gong, L. (1997). Secure software architectures. *Proceedings of the IEEE Symposium on Security and Privacy, May 1997*, Oakland, CA, pp. 84–93.

45. Hunt, W. A., and Parks, T. (2007). COTS x86 specification & verification. *NCDI Workshop on Game-Changing Solutions for Cyber Security*, College Park, MD, Nov 7, 2007.

# SECURITY OF DISTRIBUTED, UBIQUITOUS, AND EMBEDDED COMPUTING PLATFORMS

ANTHONY D. WOOD AND JOHN A. STANKOVIC
*University of Virginia, Charlottesville, Virginia*

## 1 INTRODUCTION

Computer systems and networks are becoming more capable—and more vulnerable—as they are embedded more deeply into our environment. In this article, we describe security challenges faced by ubiquitous distributed systems: ad hoc networks of handheld computers, sensor networks for directly interacting with the world, and radio frequency identification (RFID) tags that instantiate real-world objects with elements in our virtual computer systems. We review promising research approaches, and identify important future directions in these application areas.

## 2 SCIENTIFIC OVERVIEW

The confluence of wireless networking, increasing transistor densities (Moore's Law), and miniaturization of manufacturing processes has accelerated the deployment of computer networks. Computing devices are now lightweight, portable, unobtrusive, powerful, and more well connected than ever. Adding environmental and biological sensors tightens the connection with the real world, so that computing is not just embedded in non computing devices (like the proverbial Internet toaster), but is embedded in our living spaces.

We focus on three developing technology areas, represented in Figures 1 and 2: ad hoc networks, wireless sensor networks (WSNs), and RFID tags. Their applications range widely and are expanding, including military battlefield awareness, airport surveillance, emergency medical care, disaster response, critical infrastructure monitoring, container tracking, facilities access control, firearm and vehicle immobilizers, currency and travel document fraud detection, and border enforcement.

Security requirements are unique for each application, but overall they are becoming increasingly significant due to several factors. The systems being monitored, controlled, or protected are often critical for economic or safety reasons. Technological societies are becoming more dependent on their proper operation and real-time response. The networks are pervasive in many environments, where they are easily accessible and, therefore, exposed to greater threats. For example, wireless accessibility, while a great convenience, also makes it easier for attackers to find and interact with devices. Finally, the deepening of familiarity with and acceptance of computing devices extends to the unscrupulous, as well. The constant attacks that occur daily on the Internet, from ego-boosting web defacements to vengeful distributed denial of service botnets, may eventually be the norm on any accessible network.

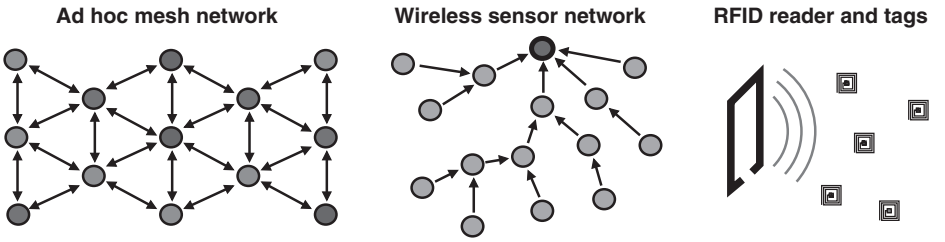



**FIGURE 1** Example network connectivity for an ad hoc network, sensor network, and RFID reader and tags.

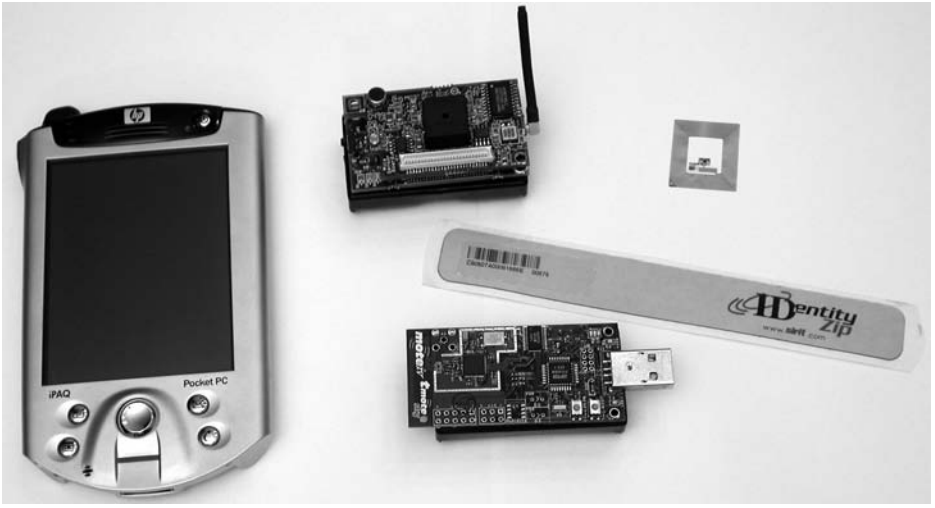



**FIGURE 2** Examples of embedded devices: PDA, sensors, and RFID tags.

### 2.1 Security Properties

Security properties can be distilled to a core set, many of which may be important for a given application. Many others are defined in the literature [1], and here we describe those discussed in this article, giving brief examples of their use.

- *Confidentiality.* Secrecy of communication between parties. Exposure of communications in wireless networks makes eavesdropping a constant threat.
- *Integrity.* Assurance that data has not been modified by an unauthorized party. This applies to messages in transit, records stored in databases, and even data possessed by attackers (such as on stolen smart cards).
- *Authenticity.* Assurance that a message originated from a known other party. Among others, command and control systems require high confidence that actions with large or dangerous effects have been issued by appropriate means. Message authentication codes (MACs) are often appended to protocol messages to provide this property.
- *Identification.* Determination of a contextually unique label for a party. It enables authentication of a party and authorization of actions it may take. Also, a persistent ID allows goods to be tracked through supply chains, from manufacturers to shelves.
- *Authorization.* Determination of privileges from a party's identity. System designs may change the authorized set of actions a party may take based on environmental contexts, for example, granting additional access during medical emergencies.
- *Access control.* Limitations on exposure or modification of protected resources to authorized parties. An RFID token that serves as a "key" for an automobile is a form of access control.
- *Availability.* A service or system performs its function in a timely manner for legitimate users. Denial of service attacks may crash a system completely, or may only slow it down enough to cause significantly disrupted service.
- *Auditability.* Logging of security-relevant actions or events for later analysis. Many attacks cannot be reliably detected in real time, but can be analyzed after the fact to help with future defenses.
- *Tamper resistance.* Ability of a device's packaging and design to withstand physical modification or interrogation. Smart cards, though in public possession, often contain secret keys, which must remain secret to prevent changing credit balances.
- *Nonrepudiation.* Inability of a user or device to deny participation in a protocol or performance of an operation after the fact. This is often related to auditability.

### 2.2 Constraints on the Design Space

Constraints on design are imposed by considerations such as available power, cost to manufacture and maintain, form factor and size, tamper resistance, development effort, the ability to dynamically reprogram, and intended architectures for deployment. Devices in ubiquitous embedded networks form a spectrum of capabilities, from PDAs to passive RFID tags, and are connected together in varying ways.

Ad hoc networks [2] connect (frequently) mobile devices together in a relatively flat mesh and usually depend on peer routing for connectivity (Fig. 1). Hardware typically consists of cell phones, mobile handheld computers (PDAs), and laptop computers, with

relatively powerful processors such as the Intel PXA255 running at 400 MHz. They may use networks with high bandwidth, for example Institute of Electrical and Electronics Engineers (IEEE) 802.11b/g, to deliver multimedia. Storage on internal and removable flash drives with capacity up to 2 GB is common.

WSNs [3] may also use node-to-node ad hoc connectivity, perhaps organized hierarchically with one or more nodes to act as sinks for generated data. Devices are primarily constrained by size, cost, and power. For example, the Crossbow Mica2 family of motes uses the 8-bit Atmel ATMEGA128 processor operating at 8 MHz, with 4 KB RAM and 128 KB flash. Simple Frequency Shift Keying (FSK) modulation at 900 MHz, IEEE 802.15.4, or Bluetooth radio communication is common.

RFID tags [4] are even more limited. Most are completely passive, using the energy of a reader's transmission to briefly power the tag's processing circuit. The tag communicates by modulating the reader's transmission. Tags may be smaller than 1–2 mm (without the antenna), and operate in the high-frequency (HF) band (13.56 MHz) for intermediate range.

Security comes at the cost of memory, computation, and messaging [5, 6]. Ad hoc network devices may be able to afford expensive asymmetric cryptography, storing 1024-bit keys for their neighbors, and participating in multi-round key establishment protocols. Sensor network devices cannot afford this computation and storage expense, unless very efficient elliptic-curve cryptographic (ECC) methods are used only infrequently. Instead, most researchers focus on lighter-weight symmetric cryptography and hashing in this context. Many RFID tags provide no security at all. Those that do may use only hashing or very efficient symmetric methods.

Hence, there are considerable differences in the security approaches that are practical and possible in distributed, embedded, and ubiquitous networks. Next, we describe the state of important research areas in security for these types of systems.

### 2.3 Solution Approaches

Distributed devices typically use layering to modularize hardware and software. Figure 3 shows generic software stacks for ad hoc and wireless sensor devices, and how services may be classified by layer. Because of their limited capabilities, RFID tags may be considered to have only a couple of layers. For this discussion, we abstract away many details unique to each network type.

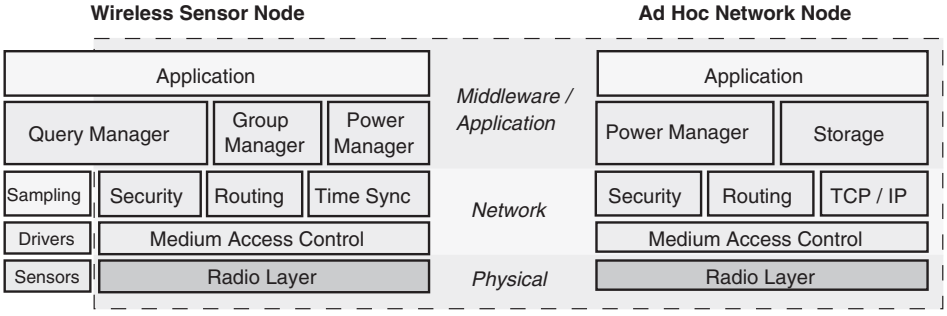



**FIGURE 3** Typical software stacks for wireless sensor network and ad hoc network devices. A dashed box surrounds the communication layers, which contain various services often found in the networks.

Strong security mechanisms at higher layers may be completely subverted by design or coding flaws at lower layers. Nowhere isthis more evident than at the physical layer. Therefore, we describe attacks and defenses proposed in the state of the art by focusing on solutions to securing services at the critical physical, network, and middleware/application layers of the stack, starting at the bottom. We discuss ad hoc, sensor, and RFID networks together in each layer.

### 2.4 Physical Layer

The ubiquity of network devices means that they are easily inspected and probed by attackers. There is by definition no physical access control to sensors that are deployed throughout a public building, in parks, forests, or other open spaces. RFID tags attached to books, clothes, or supplies are necessarily as accessible as the asset they help to track.

The simplest attack is to destroy or disable the devices entirely, creating a denial of service. This is as low-tech as briefly putting a banknote or passport in a microwave oven. However, a destruction attack can often be mitigated using fault-tolerant protocols. For example, a mesh network can continue to operate despite some fraction of the devices being destroyed—remaining connected nodes take over routing. Or, if a passport's RFID tag is destroyed, backup procedures such as optical scanning of barcodes may be used instead.

Probing of the physical device to deconstruct its internals is more powerful and damaging. By reading the contents of memory cells, the secret keys are recovered and then programmed into another device, which can fully masquerade as the original—yet is under attacker control. Messages originated by the clone are fully authentic, and the device can actively participate in formerly inaccessible transactions, as between a smart card and a payment terminal [7].

In addition to invasive techniques that usually require partial depackaging of a device, various physical properties of the circuits can be inspected without leaving a trace. Data-dependent computation affects the power consumption and timing of circuits, which can be analyzed statistically over many trials to determine bit patterns of a key [8]. Faults may be injected using heat or radiation, while the observed behavior is compared with correct behavior. Electromagnetic emissions may be inspected similarly to power consumption.

Proposed solutions include tamper-resistant packaging [7], better attack detection, fault recovery mechanisms, and reducing trust in external components [9]. For example, if a device can detect that it is being tampered with, it may erase its memory to prevent disclosure of sensitive data. Circuits may be shielded by distributing logical components across the die, bus traffic may be encrypted, and data values and timing can be randomized or "blinded" to thwart side-channel attacks.

Devices' use of wireless communication leaves them vulnerable to denial of service by radio jamming, which can be perpetrated at large distances and unobtrusively. Xu et al. propose channel hopping and "retreats" [10] to physically move away from the jammer. This is most appropriate for ad hoc networks, as it may be too energy consuming for sensor devices. Law et al. propose data blurting and changing transmission schedules as countermeasures [11]. Another approach, when the jamming cannot be avoided, is for nodes to determine the extent of the jammed area in a wide-scale network by collaboratively mapping and avoiding the region [12].

### 2.5 Networking Layers

We group the networking layers of the stack together to examine the security needs and vulnerabilities created when connecting multiple devices in networks. Services provided include channel arbitration, link establishment, one-hop data transmission, routing, and end-to-end data transport.

A primary concern is keeping data private, given the innate vulnerability to eavesdropping of wireless networks. Ad hoc networks often use protocols developed for the Internet, such as IPSec [13] and SSL/TLS [14]. Both these protocols allow the use of suites of cryptographic mechanisms to provide authenticity, integrity, and confidentiality of messages. IPSec is commonly used to establish a secure virtual private network (VPN) connection between peers. Secure Sockets Layer/Transport Layer Security (SSL/TLS) operates end-to-end, above an existing Transaction Control Protocol (TCP) connection, and further allows the client and server to negotiate a common set of capabilities. Though asymmetric methods may be used to establish keys and authenticate certificates, symmetric cryptographic protocols are used for data transfer.

In WSNs and RFID devices, symmetric mechanisms are encapsulated in lightweight protocols to provide data security. SPINS [15] provides two-party confidentiality and authenticity with the SNEP protocol. TinySec [16] similarly provides these properties using Skipjack or RC5 ciphers, in a fully implemented and compact form with low overheads.

Because of energy constraints, sensor devices cannot use asymmetric cryptographic operations often. TinyPK [17] is an implementation of the relatively less demanding signature verification and key agreement for sensor devices. Though processing times for a single message may be over a minute (depending on the key length), they argue that it is acceptable for rare events, like code updating. Recent elliptic-curve implementations [18] improve efficiency, making slightly more frequent use of public-key infrastructures possible. For RFID tags with modest resources, researchers have proposed simple authentication and encryption to prevent "skimming," or physical proximity-based interrogation of tags [4].

In addition to neighbor-to-neighbor communication, many networks require secure broadcast and multicast communication. Often a control station must broadcast parameter changes to an entire network, and authentication of these messages is imperative. Both Timed Efficient Stream Loss-tolerant Authentication (TESLA) [19] (for ad hoc networks) and uTESLA [15] (for sensor networks) provide broadcast authentication. A base station commits to a chain of one-way hashes, and then uses each in reverse sequence as a key to authenticate a message. After the message has been distributed, the next key in the chain is released. Network nodes validate that $K_i = H(K_{i-1})$ and deliver the message. If all keys in the chain are exhausted, the base station must again securely distribute the commitment (last value) for a new chain to every network node.

LKHW [20] merges logical key hierarchy (LKH) with directed diffusion to provide secure multicast for groups in sensor networks. Directed diffusion is a routing protocol in which sinks diffuse interests for events, and sources send messages along "interest gradients" that find all sinks. LKHW allows group membership to change and provides backward and forward secrecy.

Any protocol that uses cryptographic protection for confidentiality, integrity, or authentication relies on the presence of shared keys. Many approaches for creating and distributing these keys have been proposed. For public-key algorithms, a traditional centralized key distribution architecture may be used, such as Kerberos [21]. Centralized

key distribution centers can become performance bottlenecks and attractive targets for attacks, however. By using threshold cryptography, the certification function is distributed among multiple authorities, such that at least $k$ out of $n$ are required to grant certificates [22]. This is more resistant to compromise than a centralized approach, but has higher overhead.

Ad hoc network devices often must collaborate together in groups, using secure multicast communication. In the group key management protocol (GKMP) [23], a centralized controller for each group generates and distributes pairwise keys to the other members. The secure spread service [24] provides multiparty key creation using Group Diffie–Hellman, in which each member contributes to the key.

Any scheme that requires cryptography also requires keys. Much research on key distribution in WSNs has focused on distributing secrets prior to deployment [25–28]. Nodes are preloaded with multiple keys from a large key space. After deployment, nodes discover neighbors with whom they share keys, and use these paths to indirectly establish keys with other neighbors. Adding the requirement for nodes to share $q$ common keys improves the protocols' resistance to compromise. Other protocols, such as Localized Encryption and Authentication Protocol (LEAP) [29], use a globally shared key to create pairwise-shared keys with neighbors during a short initialization period. The network is assumed to be free from compromises during this time, and the global key is erased thereafter.

RFID tags interact only with readers and certain special purpose tags, so the security concerns mostly center on identification and authentication. To prevent cloning attacks, a tag may implement lightweight symmetric cryptography or hashing and be programmed with a unique key. A challenge-response protocol prevents replay attacks, and provides simple identification or authentication. With the most constraints on size and cost, RFID tags are often vulnerable to physical attacks such as those described in the previous section.

Tags that respond to any reader or that respond using the same ID or key pose privacy risks. Weis et al. propose using key-search techniques to conceal a tag's identity from any except legitimate readers [30]. The reader receives $H(k_i, N)$ from a tag, for key $k_i$ and nonce $N$, and searches through all keys known to the reader for a match, identifying tag $i$. This is expensive for large numbers of tags, however. Others propose tree-based and synchronization-based schemes to limit the searching necessary, for example, by computing outputs based on an increasing counter.

Ad hoc and sensor networks use devices connected together wirelessly for multihop routing. The use of redundant, dynamic routing paths provides protection against link failures, but it increases the risk of relying on a compromised or adversarial node.

Approaches to securing ad hoc routing have focused on retrofitting existing protocols, or creating new ones to provide desirable properties. Secure Ad hoc On-Demand Distance Vector (SAODV) [31] provides authentication, nonrepudiation, and integrity by means of a protocol extension to Ad hoc On-Demand Distance Vector (AODV) that relies on digital signatures and hashing.

Secure Efficient Ad hoc Distance-vector (SEAD) [32] also addresses security in distance-vector routing protocols, which are suitable for networks with limited mobility. It uses hash chains to secure routing updates, an approach that is more computationally efficient than SAODV and which provides some defense against denial of service attacks.

Protocols such as SEAD and SAODV rely on periodic routing updates, which have high overhead or poor performance when node mobility is high. In these networks, on-demand protocols like Ariadne [33] may be more suitable. Ariadne provides secure

on-demand routing based on the Dynamic Source Routing (DSR) protocol, and requires one of the following: network-wide pairwise-shared keys, neighborhood pairwise-shared keys and broadcast authentication (such as TESLA), or digital signatures.

WSNs require very efficient routing mechanisms, since radio transmission consumes so much of their energy budget. Their unique characteristics also pose special difficulties for secure routing [34]. Addressing the many attacks given the constraints of low-end sensor devices is problematic.

Aggregation of information to a centralized base station is a common communication pattern in WSNs. The authors of SPINS [15] suggest using underlying secure unicast and broadcast links (SNEP and uTESLA, respectively) to form routing trees from nodes back to base stations. LKHW targets communication within groups of collaborating devices (as described above), and secures directed diffusion for routing.

Secure Implicit Geographic Forwarding (SIGF) [35] is a family of routing protocols for WSNs, which allows very lightweight operation when no attacks are present, and stronger defenses—at the cost of overhead—when more attacks are detected. It is a form of on-demand routing based on geographic forwarding, where the message destination is specified as a location toward which each hop makes progress. The set of candidates considered at each hop may be increased, and their selection is randomized to prevent persistent selection of neighboring compromised nodes.

INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS) [36] is an intrusion tolerant protocol for WSNs that need little or no sensor-to-sensor communication, but which have well-defended base stations. Network topology is collected from sensor devices by the base station. Routes are centrally computed and securely distributed to sensors using one-way hash chain sequence numbers, similar to uTESLA.

### 2.6 Middleware and Applications

Above the networking layers, which are concerned with relatively low-level details of interconnection, middleware and application-layer software provide rich and varied services. Networks connected to the physical world must provide mechanisms for extracting important data to authorized parties for analysis and manipulation. Several protocols have been proposed for querying, aggregating, and validating sensor data collected by WSNs.

Secure information aggregation (SIA) [37] uses special nodes in the network to aggregate sensor data. As data are collected and aggregated, results are reported to the base station along with a commitment to the data. Commitments are formed using a binary Merkle hash tree, which reduces the size of the verification information. The base station may then request particular sensor values from the aggregator in an interactive proof, until results are verified with a desired probability.

For large-scale networks where events of interest are witnessed by multiple sensors, Ye at al. propose statistical en-route filtering (SEF) of injected false data [38]. Nodes compute message authentication codes that are aggregated and sent with the reported data. Intermediate nodes check the MACs probabilistically, dropping incorrect messages. A Bloom filter is used to decrease the cost of aggregating multiple MACs.

Reprogramming widely distributed systems is expensive if it requires manual retrieval and manipulation of unattended devices. Over the network reprogramming alleviates this practical difficulty, but presents significant security concerns. All other hardware and software defenses may be subverted by a flaw that allows an attacker to replace nodes' programs with custom code.

Deng et al. [39] propose related schemes for securely distributing code in WSNs. The first uses a chain of hashes, where each message contains segment $i$ of code and a hash of segment $i + 1$. Upon receipt of a message, the previous code segment can be immediately and efficiently verified. To bootstrap the chain, an ECC signature of the first hash value is computed using the base station's private key. This method is suitable when there is little message loss and packets are received mostly in order. The second scheme uses a hash tree to distribute all the hashes in advance, so that out-of-order packets can be quickly checked. Resistance to denial of service is improved since packets need not be stored if they are corrupt.

SCUBA [40] is a protocol for detecting and recovering compromised nodes in sensor networks. Base stations verify code images on nodes using an indisputable code execution (ICE) facility, which ensures that unmodified self-checksumming code runs on the target in the expected time. The ICE code computes checksums over the ROM, ICE function, and main executable. Incorrect checksums or executions that take too long indicate that malicious code is interfering with proper operation of the device. The result of the full Secure Code Update By Attestation (SCUBA) protocol is a repaired or blacklisted node.

Many applications may be built upon the foundations provided by the protocols we have reviewed: physical and radio-layer protections, secure node-to-node communication, multihop routing, data aggregation, and code updating. System designers must determine the attack model most appropriate for their application domain and deployment environment, carefully choosing protocols that defend against possible attacks and that do not create additional points of vulnerability.

## 3 GLOBAL RESEARCH AND FUNDING

National Science Foundation (NSF)'s Embedded and Hybrid Systems (EHS) Program [41] supports research in many aspects of embedded systems technology. A pervasive theme of the EHS program is the high-confidence integration of real-time and other service guarantees with the coordination requirements of next-generation complex, secure, networked, embedded systems.

NSF's Cyber Trust (CT) Program [42] envisions computer networks that are more reliable, accountable, and resistant to attacks, and a workforce that is well trained and educated to operate them. Research proposals that will target security for applications, security for computer systems, security for networks, and new security foundations are solicited. The entire system life cycle may be considered, and multidisciplinary projects with behavioral and social science participation are encouraged.

The European ARTIST2 Consortium [43] supports the Network of Excellence on Embedded Systems Design, which intends to strengthen European research in this area. The testing and verification cluster targets verification of security properties in designs.

## 4 CRITICAL NEEDS ANALYSIS

Embedded systems have already become ubiquitous, but their composition into large-scale systems for monitoring and controlling the physical world is nascent. Advancements

in this field will enable many advanced applications, such as secure communication for emergency personnel, disaster-site coordination, border patrol, container tracking and inspection, biological and radiological sensing, traffic control, and civil infrastructure monitoring. Realization of these critical applications will be subject to research progress on many technical fronts, including security and privacy.

## 5 RESEARCH DIRECTIONS

Physical-layer security is often a weak spot in embedded devices even when higher layers are provably sound. Tamper-resistant packaging and designs for smart card, RFID, and sensor devices will be necessary for ubiquitous deployments and deserve more research.

Wireless devices expose the system to monitoring by and remote interaction with attackers. More research in resistance to denial of service attacks by jamming, flooding, and invoking expensive computations is needed to enable continued operation of critical components even while attacks are ongoing.

Connecting virtual and physical worlds raises many privacy concerns. Controversies over RFID-enabled passports and banknotes, urban camera networks, tracking of consumer-products post sale, and disclosure of aggregated data by companies and government agencies all portend a complex future of interdependent technical, legal, and political effects on personal privacy. More fundamental research is needed in ways to preserve privacy despite the collection of unprecedented amounts of data in the public and private sectors.

Data collected by WSNs will be useful for many purposes, but may inadvertently disclose sensitive information—even if the data payloads in network are encrypted. Traffic analysis or simple radio-activity detection may reveal to an attacker whether a home is occupied, the nationality of a traveler in a crowd, or the location of important control devices. Comprehensive research that crosses traditional functional layers and includes noncryptographic approaches to information hiding is needed.

## REFERENCES

1. NIST.(2006). *Glossary of Key Information Security Terms*, R. Kissel, Ed. NIST IR, Gaithersburg, MD, 7298. April 25.
2. Royer, E., and Toh, C. A. (1999). Review of current routing protocols for ad-hoc mobile wireless networks. *IEEE Personal Commun*. **6**(2), 46–55.
3. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002). Wireless sensor networks: a survey. *Comput. Networks* **38**(4), 393–422.
4. Juels, A. (2005). *RFID Security and Privacy: A Research Survey*. Technical Report. RSA Laboratories, pp. 1–19.
5. Perrig, A., Stankovic, J. A., and Wagner, D. (2004). Security in wireless sensor networks. *Commun. of the ACM* **47**(6), 53–57.
6. Ravi, S., Raghunathan, A., Kocher, P., and Hattangady, S. (2004). Security in embedded systems: Design challenges. *Trans. on Embedded Computing Sys*. **3**(3), 461–491.
7. Anderson, R., and Kuhn, M. (1996). *Tamper resistance—a cautionary note*. *Usenix Workshop on Electronic Commerce*. Oakland, California, pp. 1–11.

8. Ravi, S., Raghunathan, A., Chakradhar, S. (2004). Tamper resistance mechanisms for secure, embedded systems. *Proceedings of 17th International Conference on VLSI Design*. Washington, DC, p. 605.
9. Suh, G., Clarke, D., Gassend, B., van Dijk, M., and Devadas, S. (2003). AEGIS: architecture for tamper-evident and tamper-resistant processing. *Proceedings of ICS.* San Francisco, CA, pp. 168–177.
10. Xu, W., Trappe, W., Zhang, Y., Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. *Proceedings of MobiHoc*. New York, pp. 46–57.
11. Law, Y. W., Hartel, P. H., den Hartog, J. I., and Havinga, P. J. M. (2005). Link-layer jamming attacks on S-MAC. *Proceedings of EWSN*. Alexandria, Virginia, pp. 217–225.
12. Wood, A. D., Stankovic, J. A., and Son, S. H. (2003). JAM: a jammed-area mapping service for sensor networks. *Proceedings of IEEE RTSS*. Cancun, Mexico, pp. 286.
13. Kent, S., and Seo, K. (2005). *Security Architecture for the Internet Protocol*. IETF RFC-4301.
14. Dierks, T., Allen, C. (1999). *The TLS Protocol*, Version 1.0. IETF RFC-2246.
15. Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D. (2001). SPINS: security protocols for sensor networks. *Proceedings of MobiCom*. Rome, Italy, pp. 189–199.
16. Karlof, C., Sastry, N., and Wagner, D. (2004). TinySec: a link layer security architecture for wireless sensor networks. *Proceedings of SensSys*. Los Angeles, CA, pp. 162–175.
17. Watro, R., Kong, D., fen Cuti, S., Gardiner, C., Lynn, C., and Kruus, P. (2004). TinyPK: securing sensor networks with public key technology. *Proceedings of SASN*. New York, pp. 59–64.
18. Malan, D. J., Welsh, M., and Smith, M. D. (2004). A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. *Proceedings of SECON*. Santa Clara, CA.
19. Perrig, A., Canetti, R., Tygar, D., and Song, D. (2002). The TESLA broadcast authentication protocol. In *RSA Cryptobytes*, RSA Laboratories, Bedford, MA, Vol. 5.
20. Pietro, R. D., Mancini, L. V., Law, Y. W., Etalle, S., and Havinga, P. J. M. (2003). LKHW: a directed diffusion-based secure multicast scheme for wireless sensor networks. *32nd International Conference on Parallel Processing Workshops (ICPP 2003 Workshops)*. Kaohsiung, Taiwan.
21. Steiner, J. G., Neuman, C., and Schiller, J. I. (1988). Kerberos: an authentication service for open network systems. *Proceedings of USENIX*. San Francisco, CA, pp. 191–200.
22. Zhou, L., and Haas, Z. (1999). Securing ad hoc networks. *IEEE Network* **13**(6), 24–30.
23. Harney, H., and Muckenhirn, C. (1997). *Group Key Management Protocol (GKMP) Architecture*. IETF RFC 2094.
24. Amir, Y., Kim, Y., Nita-Rotaru, C., Schultz, J. L., Stanton, J., and Tsudik, G. (2004). Secure group communication using robust contributory key agreement. *IEEE Trans. on Parallel and Distributed Syst*. **15**(5), 468–480.
25. Du, W., Deng, J., Han, Y. S., and Varshney, P. K. (2003). A pairwise key pre-distribution scheme for wireless sensor networks. *Proceedings of ACM CCS*. New York, pp. 42–51.
26. Chan, H., Perrig, A., and Song, D. (2003). Random key predistribution schemes for sensor networks. *IEEE Symposium on Security and Privacy.* Oakland, CA, pp. 197–213.
27. Liu, D., and Ning, P. (2003). Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks. *Proceedings of NDSS*. San Diego, CA, pp. 263–276.
28. Eschenauer, L., and Gligor, V. D. (2002). A key-management scheme for distributed sensor networks. *Proceedings of ACM CCS*. Washington, DC, pp. 41–47.

29. Zhu, S., Setia, S., and Jajodia, S. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks. *Proceedings of ACM CCS*. Washington, DC.

30. Weis, S., Sarma, S., Rivest, R., and Engels, D. (2003). Security and privacy aspects of low-cost radio frequency identification systems. In *International Conference on Security in Pervasive Computing (SPC 2003)*. v. 2802 of Lecture Notes in Computer Science, D. Hutter, G. Mueller, W. Stephan, and M. Ullmann, Eds. Springer-Verlag, Berlin, Germany, pp. 454–469.

31. Zapata, M. G. (2001). *Secure Ad hoc On-Demand Distance Vector (SAODV) Routing*. IETF Internet Draft, draft-guerrero-manet-saodv-00.txt.

32. Hu, Y.-C., Johnson, D. B., and Perrig, A. (2002). SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications*. Callicoon, NY.

33. Hu, Y.-C., Perrig, A., and Johnson, D. B. (2002). Ariadne: a secure on-demand routing protocol for ad hoc networks. *Proceedings of ACM MobiCom*. Atlanta, Georgia.

34. Karlof, C., and Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *In First IEEE International Workshop on Sensor Network Protocols and Applications*. Anchorage, AK.

35. Wood, A. D., Fang, L., Stankovic, J. A., and He, T. (2006). SIGF: a family of configurable, secure routing protocols for wireless sensor networks. *Proceedings of SASN*. Alexandria, VA.

36. Deng, J., Han, R., and Mishra, S. (2005). INSENS: Intrusion-tolerant routing for wireless sensor networks. *Elsevier J. on Comput. Commun., Special Issue on Dependable Wireless Sens. Networks* **29**(2), 216–230.

37. Przydatek, B., Song, D., and Perrig, A. (2003). SIA: secure information aggregation in sensor networks. *Proceedings of ACM SenSys*. Los Angeles, CA.

38. Ye, F., Luo, H., Lu, S., and Zhang, L. (2004). Statistical en-route detection and filtering of injected false data in sensor networks. *Proceedings of IEEE INFOCOM*. Hong Kong.

39. Deng, J., Han, R., and Mishra, S. (2006). Secure code distribution in dynamically programmable wireless sensor networks. *Proceedings of ACM/IEEE IPSN*. Nashville, TN, pp. 292–300.

40. Seshadri, A., Luk, M., Perrig, A., van Doorn, L., and Khosla, P. (2006). SCUBA: Secure Code Update By Attestation in Sensor Networks. *Proceedings ACM WiSe*. Los Angeles, CA, pp. 85–94.

41. NSF's Embedded and Hybrid Systems (EHS) Program, (2006). URL: http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=5139.

42. NSFs Cyber Trust (CT) Program, (2006). URL: http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=13451.

43. European ARTIST2 Consortium, (2006). URL: http://www.artist-embedded.org/FP6/.

## FURTHER READING

Anderson, R. (2001). *Security Engineering*, John Wiley & Sons, New York.

Karl, H., and Willig, A. (2005). *Protocols and Architectures for Wireless Sensor Networks*, John Wiley & Sons, England.

Zhao, F., and Guibas, L. (2004). *Wireless Sensor Networks: An Information Processing Approach*, Morgan Kaufmann, San Francisco, CA.

Murthy, C. S. R., and Manoj, B. S. (2004). *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall Ptr, Upper Saddle River, New Jersey.

Basagni, S., Conti, M., Giordano, S., and Stojmenovie, I., Eds. (2004). *Mobile Ad Hoc Networking*, Wiley-IEEE Press, New York, NY.

# SECURITY OF WEB APPLICATION AND SERVICES AND SERVICE-ORIENTED ARCHITECTURES

MARC GOODNER
*Microsoft, Redmond, Washington*

## 1 INTRODUCTION

Service Oriented Architecture, or SOA, has had many characteristics ascribed to it. It has been hailed as a way for organizations to integrate heterogeneous systems, provide for increased reuse of software assets, provide multichannel access to common components, and as the way to build distributed systems, all while reducing complexity and increasing interoperability. SOA can mean all of these things depending upon how its principles are applied in a given project. Seen as a natural outgrowth of previous software design paradigms, the key distinguishing characteristic it has is facilitating interoperability between distributed software components. As an architectural style for designing software SOA does not mandate one implementation choice over another. While there are many realizations of these principles, Web services is the most pervasive implementation choice for SOA. This is because Web services are platform-agnostic protocols; thus they greatly facilitate interoperability between different implementations. This is critically important in enabling software systems that need to connect new and existing applications in and across environments as heterogeneous as a typical corporation, government agency, or even a home. The security requirements for these applications will vary greatly depending on the type of information they use, the policies of the application users, and the threats to the messages being exchanged. The techniques available to mitigate threats to the security of an SOA-based software application will be the same regardless of whether the threats are from non-state actors, corporate espionage agents or common criminals. From the perspective of homeland security, many of the sources of each of these threats are increasingly blurred due to an emerging common underground economy for those perpetrating the attacks. In that respect it is an imperative that security be a foremost concern in all distributed software implementations. This article will describe the security challenges in SOA, relate them to Web service protocols that address these challenges, and introduce some areas for further consideration.

## 2 SOA SECURITY CHALLENGES

In order to properly discuss the security challenges of SOA let us look a little closer at what SOA is. Newcomer and Lomow provide a succinct description: “A service-oriented architecture is a style of design that guides all aspects of creating and using business services throughout their life cycle (from conception to retirement). An SOA is also

a way to define and provision an IT infrastructure to allow different applications to exchange data and participate in business processes, regardless of the operating systems or programming languages underlying those applications." [1] The following properties of SOA can be derived from the above description:

- *Explicit boundaries.* When exposing functionality as a service it is important that the choice of what to expose is carefully considered. Only what is needed to exchange information should be exposed. What is critical here is that while services are explicitly exposed, nothing should ever be exposed as a service by default;
- *Service autonomy.* The application that supports a service should be independent of the service definition itself. This allows for revisions of the application while keeping the interface used by client applications stable. Services may also need to change their location over time;
- *Contracts.* There needs to be machine-processable formats to produce the necessary message structures for the service. Classes should never be shared to enable invocation of services;
- *Compatibility based on policies.* There also needs to be machine-processable policies in place at a service so that client applications can determine if they are compatible;
- *Interoperability.* Services need to be exposed in a way that facilitates use by the broadest base of applications.

What you can see in SOA are services exposed in a highly interoperable and machine-processable fashion. As SOA has gained the most traction within larger enterprises, it is important to step back and recognize that the environments in which these services are commonly deployed are often secured via tight perimeter controls. To properly secure these services a more granular approach is needed. Remember that a key promise of SOA is re-use. Services may not only find re-use within more areas of the organization that created them, but potentially externally as well as they begin to offer value to an organization's partners. The remainder of this section will focus on specific security concerns and concepts that need to be considered in the design of an SOA-based system. The next section will map these security concerns and concepts to specific Web services protocols.

It is important to state that this section is not intended as a substitute for proper risk analysis of your software design. The concerns and concepts below should be used in a formal risk assessment, not as a checklist. The following advice is based on applied experience in this area: "Before you take any technical steps to implement a specific security structure, you should capture the security requirements for all relevant pieces of software during a risk analysis. Based on this analysis, you build the software architecture to incorporate the defined security requirements" [2].

Choosing explicitly what to expose as a service is an important decision. If something does not need to be exposed as a service, it should not be. Services that are exposed should present the minimum amount of surface area for a malicious client to probe. At the point that a choice to expose a service is made, the decisions about how to protect the service endpoint and the messages it exchanges should also be made. The value of the information contained within the messages exchanged will guide some of the choices during a full risk assessment of what mechanisms to employ. From the client's

perspective, the analysis of the value of the information being exchanged is just as important. Clients should not interact with services that do not meet their own security requirements.

SOA-based systems are vulnerable to threats targeted at the messages they exchange over networks. These threats revolve around classic man-in-the-middle scenarios where messages are intercepted for inspection or alteration. In particular, substitution of messages in whole or in part must be guarded against. For instance, an attacker should not be able to change the message content while leaving security credentials intact; such a condition must be detectable. Similarly messages should not be allowed to be replayed, as that can be used to introduce application errors or cause other problems.

There are many other security challenges that need to be considered in designing an SOA-based system. We will attempt to answer many of these in the remaining space but this list should not be considered exhaustive.

- *Access.* How is access to a service granted?
- *Confidentiality.* How can the contents of a message be kept secret?
- *Integrity.* How can a message be protected from alteration en route to a recipient?
- *Non-repudiation.* How can it be proven that a message was received?
- *Trust.* How can parties in a given interaction rely upon the security credentials of each other?
- *Sessions.* How can a set of messages be exchanged securely?
- *Description.* How can the security requirements of a service be expressed?
- *Federation.* How can resources in one security domain be provided to clients whose identities are managed in another?
- *Identity.* How are the participants in an exchange known?
- *Privacy.* How is inadvertent information disclosure prevented?

There are other questions that cannot be answered within the scope of this paper as the answers are specific to the technologies used in an implementation, or to local requirements.

- *Performance.* Is there a resource penalty for securing services?
- *Audit.* How can messages be traced in a distributed environment?
- *Regulatory compliance.* Are there mandated security requirements from government agencies?

An SOA-based infrastructure may have many different types of client applications present, from large back-end systems and middleware to rich desktop applications and lightweight web clients. This article has not discussed the security issues involved in developing the client applications themselves.

## 3 SECURE WEB SERVICES FOR SOA

The use of Web services is one of the most common implementation strategies for SOA. Web services are widely supported and provide a high degree of interoperability. What

helps to make Web services interoperable is that they are based on XML [3] and a set of standards and specifications that have been developed by a diverse group of software vendors and users, and validated through implementation.

When a service is exposed as a Web service, it is typically exposed with a contract consisting of Web Services Description Language (WSDL) [4] and XML Schema [5]. The WSDL describes the message exchange patterns supported by the service. The XML Schema describes the message formats themselves, especially the application payload. Additional semantics around usage of the service, characteristics such as security and reliability, are expressed via WS-Policy [6]. This allows a client to determine if it is compatible with a given service or not by comparing the service's capabilities to its own. A Web service must have a service location, or address, where it can be accessed. The address is expressed in terms of WS-Addressing [7]. The messages themselves are based on SOAP (Simple Object Access Protocol) [8]. SOAP messages are broken into two basic wrapper elements, the header and the body, both of which are contained in a common "envelope" element. The SOAP header contains infrastructure information; the SOAP body contains the application message payload.

Before going on, it is worth noting that most other strategies for implementing SOA are specific to a particular vendor's software platform. As such, they each must have their own unique strategies for meeting the security challenges with the SOA outlined above. This situation is similar in a standards-based environment of Web services as well which has been described by Thomas Erl: "However, the SOAP messaging communications framework upon which contemporary SOA is built, emphasizes particular aspects of security that need to be accommodated by a security framework designed specifically for Web services." [9] Here, we look at the specifics without needing to consider a specific vendor's platform as we have publicly available specifications and standards to refer to.

Broadly speaking, there are two primary ways to secure Web services: transport, or message-based security.

### 3.1 Transport-Based Security

The most common way to secure Web service messages at the transport layer is SSL (secure sockets layer) or TLS (transport layer security) [10]. It can provide for both confidentiality and integrity, and it has an in-built mechanism for exchanging credentials. It is also widely supported and well-understood. Its use can even be described using WS-SecurityPolicy [11].

SSL/TLS protects communications from one point to the next point. This is satisfactory protection in many cases but it is also a limitation that must be considered when choosing to use it. At any time that communications need to be routed through an intermediary, the SSL/TLS session ends and the message will be in the clear. The lack of the client's visibility to this occurring makes SSL/TLS unacceptable in many cases.

While many think of Web services as being used exclusively over HTTP, they are not bound to that choice alone; they may be used over TCP (Transmission Control Protocol), SMTP (Simple Mail Transfer Protocol), UDP (User Datagram Protocol) etc. SSL/TLS can limit these choices of your underlying transport layer as some, like UDP, cannot support it at all, while others are not broadly supported. SSL/TLS is also limiting in the types of security credentials that can be used in establishing the secure channel. Both of these factors will be overly constraining in many instances.

SSL/TLS is suitable for short-lived sessions, but it does not provide the same capability for long-running protected sessions that something like WS-SecureConversation [12] does. While SSL/TLS does provide the capability for resumption, where the same SSL/TLS session is re-established after it is interrupted, it is not commonly implemented or used. In practice SSL/TLS is best used for short exchanges where communications are not expected to be interrupted or where it is acceptable for them to be resumed over a new protected channel. Note that in many instances it is not acceptable to resume communications from an invalidated secure channel, over a new one.

SSL/TLS should not be ruled out as a way to protect Web services but it is important to keep its constraints in mind. It is often best used in conjunction with the message-based security mechanisms described below.

### 3.2 Message-Based Security

Web Services Security (WSS) [13] enables the exchange of trusted messages. It defines an information structure for use in the SOAP header that provides the capability for expressing security information about a message. It leverages the capabilities of the SOAP header to facilitate securing parts of messages to specific roles in a message exchange, thus enabling end-to-end message security even in the presence of intermediaries.

A key part of WSS is its support for attaching and referencing security tokens. WSS was designed to be as flexible as possible in its support for different token types. It defines a Username Token and extensible binary and XML token types. These extensible types have been further refined by WSS token profiles that include X.509, SAML, Kerberos and others.

WSS builds on the work of XML-Signature [14] to address threats related to message alteration and to facilitate nonrepudiation. WSS uses signatures as a means to verify a message's integrity, that it was not altered in transit, and as a way to validate the claims of security tokens associated with the message. WSS also allows for the inclusion of multiple signatures and signature formats. This is important in distributed applications where different parts of a message may need to be signed by different parties involved in the processing of the information.

Message confidentiality is provided in WSS by leveraging XML Encryption [15]. There are facilities provided for protecting individual SOAP header or body elements or sub-elements.

WSS also introduces a security time-stamp element for use in protecting against message replay threats.

In order to ensure broad interoperability of WSS, the WS-I Basic Security Profile (BSP) [16] was created. The BSP constrains many of the options present within WSS, its security token profiles, as well as the carrying-forward requirements that are important for interoperability.

While WSS describes how to use different security token types, it does not describe how to get them. WS-Trust [17] describes a Web service-based interaction for the request and issuance of security tokens from a Security Token Service (STS). This takes the form of a Request Security Token (RST) request and a corresponding Request Security Token Response (RSTR). The tokens requested and issued are also capable of being scoped to a specific purpose. It is recommended that this scope be as constrained as possible to prevent possible abuse of issued tokens.

There is also the capability in WS-Trust for more complex negotiations for the establishment of the requested security tokens. This is accomplished by adding Signature Challenge and Response legs in between the initial RST and eventual RSTR. In addition to these capabilities, WS-Trust also provides capabilities for the validation, renewal, and cancellation of security tokens that have been issued.

In order to address the need to authenticate a series of messages, WS-SecureConversation [12] was defined. WS-SecureConversation builds upon WS-Trust to define a protocol that allows for the establishment of a security session including the establishment of efficient keys and key material. It defines the Security Context Token (SCT) to be used over the lifetime of messages that are part of an exchange. The SCT is referenced like any other token using the capabilities of WSS. It is important to note that an SCT need not contain any identity-related information. An SCT is often used just for a single exchange and may be discarded when it is completed.

The security requirements of a Web service are expressed using policy assertions that are defined by WS-SecurityPolicy (SP) [11]. There are assertions that allow the expression of a service's requirements of features provided by WSS, WS-Trust, and WS-SecureConversation. These assertions provide the necessary information for a client to determine its compatibility with a service and configure itself to produce messages that meet the service's security requirements. The assertions provide a great deal of flexibility for expressing the necessary token types, cryptographic algorithms, and transport requirements of the service.

## 4 WEB SERVICE SECURITY DIRECTIONS

### 4.1 Federation

Looking to more advanced security requirements, one that stands out is the need to enable different security realms to work together, where a realm is seen as a single unit of administration or trust. This is known as federation, where resources managed in one realm are made available to security principals whose identity is managed in another. The WS-Federation [18] specification addresses this topic by building upon WS-Trust.

WS-Federation provides capabilities for the sharing of identity, authentication, authorization, and privacy data when appropriate. It allows for the remote access of services without requiring the service provider to maintain local user identities. It provides optional pseudonym services that allow for the protection of identity information by providing alternative representations of it. A common claims dialect is also defined that allows for the expression of basic claims in WS-Trust messages. WS-Policy assertions are defined to allow a service to advertise its support for the features defined by WS-Federation.

WS-Federation defines bindings of WS-Trust for use with web-browser clients. This enables the use of web browsers in interactions in which they cannot directly make Web service requests on their own.

### 4.2 Identity

Another evolving area in WSS is identity. The internet has no identity layer. This is becoming increasingly problematic as mechanisms for managing who is connecting to

what on the internet are increasingly under attack, especially the most common form of user name and password. Kim Cameron's Laws of Identity [19] were arrived at through a dialog of many experts in digital identity and serve as the principles for establishing an Identity Metasystem for the internet to address this problem. The core idea is to put the user back at the center of managing their identity on-line. The realization of these concepts has been through the use of Web service protocols discussed above, especially WS-Trust.

The Identity Metasystem has three essential roles. Note, however, that participants may fulfill more than one of the following roles:

- *Identity providers.* the issuers of digital identities. Examples of potential identity providers are credit card issuers, banks or government agencies;
- *Relying parties.* parties that require a digital identity for use. On-line merchants are a fine example of a relying party that would require a digital identity issued by a credit card company;
- *Subjects.* the individual or other entity that claims are made about, for example, an end user or company.

The Identity Metasystem is an open and nonproprietary concept. The concepts that it consists of, described above, are realized using web service protocols that are not restricted to a specific platform. Specifically an identity provider is an STS as described in WS-Trust. Relying parties describe their own requirements using WS-SecurityPolicy and make them available through WS-MetadataExchange [20].

Users are always aware of interactions that are made on their behalf between parties, in the Identity Metasystem. This awareness is made possible through a consistent experience provided by an identity selector. The identity selector presents a user with the credentials that satisfy the requirements of the relying party. The relying party is clearly revealed as are the identity providers to the user. The user has visibility to whom is making the request (the relying party) for their digital identity. The user also has visibility to who issued the digital identity (the identity provider) they are going to release to the requestor. This identity selector is invoked by an application typically, but not necessarily, a web browser, and performs the necessary negotiations between identity providers and relying parties. The user has complete visibility to the claims being requested and released as part of this interaction.

The ideas of the Identity Metasystem have been reflected in implementations of both commercial and open-source software such as Microsoft's CardSpace, Mozilla Firefox, and Higgins which has backing from IBM and Novell.

## 5 SUMMARY

SOA will remain a popular approach to building distributed software applications for many years. Web services are, and will remain, a common SOA implementation strategy on many platforms. The above article has described many of the common threats present to SOA applications and how those threats are addressed via Web service security protocols. The threats to SOA applications are the same irrespective of the attacker; for example, a criminal, espionage agent, or common vandal. While transport security will remain an important option for securing Web service messages, message-based

security provides more flexibility, capability and generally better protection when properly deployed. This is an evolving area, particularly in the areas of federated trust and identity. The reader is encouraged to follow the references from this article to stay up-to-date.

## REFERENCES


1. Newcomer, E., and Lomow, G. *Understanding SOA with Web Services*. Addison Wesley Professional.
2. Krafzig, D., Banke, K., and Slama, D. *Enterprise SOA: Service-oriented Architecture Best Practices*. Prentice Hall.
3. *W3C Recommendation. Extensible Markup Language (XML) 1.0 (Second Edition)*. Available at http://www.w3.org/TR/2000/REC-xml-20001006.
4. *W3C Note. Web Services Description Language (WSDL 1.1)*. Available at http://www.w3.org/TR/2001/NOTE-wsdl-20010315.
5. *W3C Recommendation. XML Schema Part 1: Structures Second Edition*. Available at http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/.
6. *W3C Member Submission. Web Services Policy 1.2—Framework*. Available at http://www.w3.org/Submission/2006/SUBM-WS-Policy-20060425/.
7. *W3C Recommendation. Web Services Addressing (WS-Addressing)*. Available at http://www.w3.org/TR/2006/REC-ws-addr-core-20060509.
8. *W3C Note. SOAP: Simple Object Access Protocol 1.1*. Available at http://www.w3.org/TR/2000/NOTE-SOAP-20000508/.
9. Erl, T. *Service-oriented Architecture: Concepts, Technology, and Design*. Prentice Hall.
10. *IETF Standard. The TLS Protocol*. Available at http://www.ietf.org/rfc/rfc2246.txt.
11. *OASIS Committee Draft. WS-SecurityPolicy 1.2*. Available at http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200512.
12. *OASIS Committee Specification. WS-SecureConversation 1.3*. Available at http://docs.oasis-open.org/ws-sx/ws-secureconversation/200512.
13. *OASIS Standard. OASIS Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)*. Available at http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.
14. *W3C Recommendation. XML-Signature Syntax and Processing.* Available at http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.
15. *W3C Recommendation. XML Encryption Syntax and Processing*. Available at http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/.
16. *WS-I Working Group Draft. "Basic Security Profile Version 1.0*. Available at http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html.
17. *OASIS Committee Specification. WS-Trust 1.3*. Available at http://docs.oasis-open.org/ws-sx/ws-trust/200512.
18. Kaler, C., Nadalin, T., et al. *WS-Federation*. Available at http://schemas.xmlsoap.org/ws/2006/12/federation/.
19. Cameron, K. *The Laws of Identity*. Available at http://www.identityblog.com/?page_id=354.
20. Curbera, F., Parastatidis, S., Schlimmer, J., et al. *WS-MetadataExchange*. Available at http://schemas.xmlsoap.org/ws/2004/09/mex/.

# CYBER SECURITY TECHNOLOGY USABILITY AND MANAGEMENT

DIANA K. SMETTERS
*PARC, Palo Alto, California*

## 1 INTRODUCTION

Why does usability matter? Particularly when placed in the context of security, it sounds nice but is not *necessary*—after all, who would place their systems or data in jeopardy just for a little convenience? In practice, the answer to this question is anyone for whom maintaining system security is not the primary job, or in other words, almost everyone. People use computers to accomplish particular tasks, and anything ancillary to those tasks, and particularly anything that gets in the way of their accomplishment will be worked around, disabled, or avoided [1]. The net result of an unusable security measure is likely to be a system less secure than the one that started out as more insecure in the beginning. Luckily, recent work at the intersection of computer security and human—computer interaction (HCI) has begun to demonstrate that the "human element" is a critical component of security, and that it is possible, with care, to build systems that are both usable and secure.

## 2 USABILITY AND SECURITY: CURRENT RESEARCH

In their seminal 1974 paper, Salzer and Schroeder listed eight principles for the design of secure systems. The last was "psychological acceptability"—usability, which they saw as critical if mechanisms designed according to the other seven principles were to be applied correctly [2]. After 25 years of relative quiet, there has been an explosion of interest in how to make secure systems "psychologically acceptable", and how to make "acceptable", or *usable* systems secure.

We can divide the body of research in this new field, often referred to as *HCISEC* (referring to the interface between the fields of *human—computer interaction* and security), into three loose classes. The first takes existing secure systems, identifies their usability flaws, and then (sometimes) attempts to improve them through interface redesign. The second tries to design new systems from the ground up to be both usable and secure, often arriving at significantly different solutions than traditional, solely security-focused designs. The last attempts to develop design principles, or guidelines, to aid practitioners in better designing future systems. An overview of research in each class is given below.

Throughout, it is useful to consider the identity of the "user" in *usable*—while most usability work focuses on end users, usability for systems administrators and developers is also important to the building of effective systems. It is also useful to keep in mind

the difference between "security technologies"—technologies designed to accomplish an explicitly security-focused task, such as login interfaces or policy management systems, which permit a certain level of "security focus" in their design and interfaces, and systems that have security requirements, but whose primary goal is something other than security, for example, file sharing systems and e-mail systems [3].

## 2.1 Improving Existing Security Technologies

***2.1.1 Failures of Existing Systems.*** Perhaps the largest body of research in security usability looks at systems that are not studies of real users and the ways in which they find existing systems impenetrable or use them incorrectly. The first of these, due to Whitten and Tygar [4], asked users in a laboratory setting to encrypt their e-mail using relatively popular commercial e-mail encryption software (PGP 5.0), and demonstrated that the majority were simply unable to do so.

Even more disturbing is that users not only find managing security difficult, but they are also often unable to determine when they have accomplished security-critical tasks and when they have not. Good and Krekelberg looked at use of a popular peer-to-peer file sharing program, and discovered that the majority of users were unable to determine what files they were sharing with others, sometimes sharing the entire contents of their hard drives when they thought they had exposed nothing [5]. Notable industry studies have shown that although 92% of users think they have up-to-date antivirus software, only 51% actually do; even though 73% of users think they have a firewall, only 64% have turned it on; and that only a small fraction of users who think they have antispam and antiphishing software actually do have [6].

In case we forget that usability problems plague not only end users but also trained system administrators, a large-scale automated survey of secure web servers shows that as of January 1, 2008, 68% of web server SSL/TLS certificates were invalid [7].

***2.1.2 Passwords.*** Passwords are the most common form of security technology experienced by users, and perhaps the most overused—many users manage 15 or more [8–10]. Studies confirm that users do not know to pick good passwords, and are asked to remember far too many of them and change them too often, resulting in poor password choice, or passwords that are written down [9, 11].[1] Situations that require individuals to act on each others' behalf result in passwords that are shared [9, 12]. Users frequently reuse passwords across sites [10], reducing cognitive load but allowing an attacker to capture a password in one place and successfully use it in others.

A number of attempts have been made to help users choose better passwords and remember them more effectively [11, 13]. Better password choice algorithms suggest that users derive passwords from memorable phrases rather than words, resulting in passwords that appear as difficult to crack as random passwords but are more memorable [14]. An increasing number of graphical password systems ask users to draw, remember, or select regions of images rather than entering text-based passwords [15, 16]. Unfortunately, the very features that make things memorable to humans—their patterns and predictability—also make them vulnerable to attack. Humans can indeed remember

[1]Merely writing down a password is not always a security risk. Using a complex on-line banking password that you must write on a note attached to your monitor is much better protection against hackers on the internet than using a shorter password you can remember. However, it is not very good protection against your cleaning people.

phrase-derived passwords better than random passwords, but they also tend to pick the *same* phrases as easily memorable, making it possible to build a phrase-based dictionary that is highly effective at breaking such passwords [17]. Similarly, the properties of an image or image component that makes it likely a person will remember it or choose it as part of a graphical password are also predictable, resulting in the ability to construct "graphical dictionaries" effective in attacking such passwords [18, 19].

An alternate approach to this problem can be seen in the design of tools that help users remember their existing passwords, such as password toolbars. The best of these help the user create stronger passwords, while reducing the user burden. They do this by taking one (user-remembered) "master" password and generating from it individual, random passwords for each site the user visits. This limits the risk to the user if any single password is compromised [20, 21]. Such systems also attempt to protect the user from phishing attacks (see below) by detecting when the user attempts to enter such a protected password into a site that does not match the one it was created for, either warning the user [20, 21], or actually generating an incorrect password as a result [22]. These are difficult to implement in a fashion that can be used effectively and correctly, however [23], leaving the ultimate effectiveness and practicality of such approaches open to future research.

## 3 SYSTEMS MANAGEMENT

Systems management contains the largest fraction of "security-focused" tasks, and so is perhaps the area where usability of security comes first to mind. The "users" involved in systems management, however, range tremendously. There are typical end users struggling to update and secure their home PCs, who are asked to take on increasingly sophisticated management tasks [24]. There are systems administrators who, as "trained professionals", are often considered not to require special attention to usability, but who frequently have no special expertise in security. And there are specialized security administrators, often dealing with vast amounts of time sensitive information, usually with text-based tools [25].

Several recent ethnographic studies have documented the tools and practices of systems [26, 27] and security administrators [25]. These studies have documented that administrators are often skeptical of graphical management tools, particularly that they will scale effectively, and prefer to build tools themselves or adopt tools built by others within their professional communities. At the same time, these studies have examples where more effective tools would help administrators in visualizing information to more effectively monitor and understand situations, or to configure systems in ways that minimize error or increase speed or effectiveness. It is also the case that "user-friendly" tools designed to help end users with management tasks are sometimes adopted by professional administrators when they see that they can indeed simplify their work (e.g. [28], discussed below, where a secure wireless local area network (WLAN) configuration tool designed for end users was adopted for enterprise use at the request of administrators, and which has been used by those administrators in deployment for over 4 years at this writing).

Well-designed information visualization tools can aid in almost any complex task, including systems administration. An early example of a visualization tool designed specifically to illustrate the frequency of network attacks is the compellingly named

*Spinning Cube of Potential Doom* [29].[2] Though not designed for use in real-time administration of networks, one could easily imagine that a successor to this tool could be a powerful aid in understanding current network state. Recent work has begun to leverage visualization tools to assist even untrained end users in understanding and managing their computers. *Sesame* [30] is a visualization system that allows end users to graphically "drill down" and examine the state of their computer, its processes, and network connections, and to manage basic aspects of their systems. Using Sesame, users were more effective at simple security tasks than users using traditional tools (e.g. firewalls).

A number of studies have looked at whether better interfaces or tools can improve administrator effectiveness on standard security tasks.[3] Perhaps the largest group of these have looked at access control or the configuration of permissions to determine who can use files or other resources. The results are very encouraging, suggesting that effective attention to usability in system design can really improve performance on security tasks.

One of the earliest efforts to identify a link between usability and security is that of Zurko et al. [31, 32], who demonstrated that appropriate attention to usable interface design could improve the effectiveness of a role-based access control system. More recent work [33, 34] has demonstrated that improved graphical interfaces to traditional access control lists can improve users' ability to rapidly and correctly specify access policies. Going further, the SPARCLE system [35] allows minimally trained administrators to specify privacy policies in natural language; perhaps signaling the ultimate direction such management systems must go in to reach the ever-larger classes of individuals that must use them. Finally, Cao and Iverson [36] attempted to build the first systems—"intentional access management"—capable of taking a simple specification of what policy the user intends to apply, and automatically navigating the often complex and conflicting maze of effector mechanisms that can "make it so", avoiding common user error in the process.

## 4 WEB SECURITY AND PHISHING

Perhaps the most significant battleground wherein the end user is on the front lines, directly determining the success or failure of an attack, is the war against phishing. *Phishing* is the attempt to get users to hand over personal information or credentials to an attacker via subterfuge.[4] A user receives an e-mail message containing a request for information (e.g. "Update your account information to make sure your access is not disabled!"), and usually a clickable link to an attacker's website where that information can be entered. The e-mail, link, and website are carefully crafted by the attacker to resemble communications from a trusted provider with whom the user already has a relationship (e.g. their bank or an Internet provider such as PayPal or Amazon). Successful attacks enable the attacker to drain the user's bank or PayPal account, or to engage in further forms of identity theft [37].

The fundamental problem underlying the success of phishing attacks is the lack of effective *mutual authentication* in web-based interactions. Logins and passwords are designed to protect websites from unauthorized use. Unfortunately, the mechanisms

[2] So compelling is the name that I challenge any reader of this manuscript *not* to go and look at the corresponding website.

[3] By effectiveness here, we mean the administrator's ability to accomplish their stated goal rapidly and without error.

[4] Phishing is perhaps the most technical form of traditional social engineering attacks.

designed to protect users from being tricked into communicating with sites other than the ones they intend are much less effective. In the former case, a web server can automatically verify user credentials, in the latter a human user must look at a set of security indicators—for example, the use of TLS/SSL, the URL they are connecting to, and the content of the page—and determine whether they are connected to the correct server. Though some effort has been made to design features into modern web browsers to aid users in making this determination, most users do not look at them, instead primarily make trust decisions based on insecure aspects of the web content [38, 39] or use ineffective decision strategies [40].

Approaches to prevent or defend against phishing attacks largely take three forms. The first class of approaches attempts to educate the user: teaching them basic security information and heuristics to help them authenticate the websites they communicate with [41]. Some of these efforts are effective, increasing users' ability to distinguish good from malicious sites [41], and can even be enjoyable—embedding the learning experience in a game [42]. However, other attempts to educate the user about security indicators have resulted in subjects misidentifying malicious sites as good with improved confidence after training [39].

The second class of antiphishing efforts attempts to detect "bad" sites and warn users about them. All major web browsers incorporate increasingly sophisticated tools to do this, using a combination of website analysis and blacklisting. Add-on "antiphishing toolbars" abound. Unfortunately, users tend to ignore such warnings [43]. Even the best of current detection technology is highly inaccurate [44], making it currently unacceptable to simply prevent users from visiting identified supposedly malicious websites. Research continues on improving malicious website detection, from better approaches to content analysis [45], to combined analysis of phishing e-mails and the websites they point to [46], to attempts at large-scale surveys of every malicious site on the Internet [47].

The third class of antiphishing efforts focuses on improving users' abilities to authenticate the websites they interact with—to detect correct sites, rather than to be warned about impersonators. Dynamic security skins [48] allow the user to associate each website with a personal image, stored by that web server, and carefully integrate into the user interface (UI) presented to them in a manner that resists spoofing. Unless the server is able to present the correct image, the user is supposed to reject it as being a malicious impersonator. Limited features of this approach have been integrated into commercial banking sites in a system called *SiteKey* [49]. Though a promising approach, studies have determined that users do not notice the absence of their security image or other security indicators [50]. Password protection toolbars, mentioned above, can help prevent users from giving away their passwords. Some toolbars ensure that the user has a unique password for each site, and resist attempts by users to enter a protected password into the wrong site [20, 21]. Others operate by keying each password to the url of the site being visited, so that the password presented to a phishing site will not be the password required for the corresponding legitimate site [22]. However, they are often difficult to use correctly, and users may achieve a lower level of effective protection than they think they have [23].

### 4.1 Designing New Technologies with Usability in Mind

One of the most common complaints of security experts is that systems designers often attempt to "add security on at the end", after a system has already been built. This

is highly ineffective. Usability experts similarly run into efforts to "add-on usability", for example, to bring in an interface designer late in the development of a system in the hopes that better-designed dialog boxes will make up for a fundamentally flawed system interaction design. To design systems that are both usable and secure, perhaps the only truly effective approach is designing for both usability and security from the start [51]. Also the key is to take both seriously—for example, discounting neither security to get greater functionality in an end user focused application nor usability to get greater security. As we have seen, this often ends with users avoiding or abusing the provided security mechanisms, resulting in a system that is less secure than one that had not tried so hard for security to start with. Most interestingly, attempts to "design *usable* security in" from the start often result in systems that use existing technologies in creative and effective ways, as well as designing new technologies potentially useful for future systems. We sample a few such systems here.

The cryptographic literature abounds with techniques for securing network connections; however, difficulties in managing and distributing keys limit their use. *Public key infrastructures* (PKIs), an approach to binding public keys to user identities via signatures by trusted authorities on digital certificates, have been proposed as the universal solution to this problem, but they require that users obtain keys and certificates, and that there be a mechanism for distributing trust in the certificates of the very authorities used to bootstrap the system. Although used extensively to verify web transactions through the use of the SSL (TLS) protocol, digital certificates are in general only used to authenticate servers. Distributing client certificates to authenticate users is considered too difficult, so they are generally authenticated using only passwords.

The largest difficulties in deploying PKIs come firstly from attempting to manage PKIs "in the large" as they were originally designed—to identify people as part of a large-scale, even global, naming infrastructure; and secondly from forcing users to explicitly play their part in the PKI enrollment process—namely generating public/private key pairs and having them certified. By rethinking these assumptions, and considering PKI, or infrastructure "in the small", one can create flexible, small-scale public key infrastructures designed to meet particular goals [52]. If these PKIs, or "instant" PKIs, are tailored to a particular application context, the process of enrollment can then be made transparent to end users, by embedding it in that application's context. This approach tends to use such certificates as simple group membership credentials—group members have a certificate, others do not—rather than the more traditional identity credentials that at least X.509 digital certificates were designed to be.

Balfanz et al. [28] used this idea of an "instant" PKI to address the problem of allowing end users to easily set up highly secure WLANs in a system called *Network in a Box* (NiaB). The NiaB access point configured itself into all the components necessary to secure a WLAN using digital certificates and strong authentication. Users wishing to join a given NiaB-controlled WLAN simply "point out" the access point controlling the network using the infrared port of their laptop or PDA, as if they were using a remote control. Using this infrared connection as a form of *gesture-based authentication* [53], the prospective client and NiaB access point (AP) exchange public key information over this out of band channel, allowing them to authenticate each other and set up a secure connection over the WLAN. Over this wireless connection, the client is automatically given a digital certificate and configured to use this wireless network in the future. The resulting system is both intuitive and secure; providing a simple trust model wherein only people with physical access to the NiaB AP (able to communicate with it via infrared) are

able to join the WLAN. The user-friendly approach of using an automated out of band channel to bootstrap authentication between devices [53, 54] has been extensively used in recent years (e.g. [47, 55]). Similar approaches for automatic provisioning of certificates have also been used, for example, to provide client credentials for authenticating to secure websites [48, 49, 56, 57].

Another intuitive approach to delivering and establishing trust in public keys is termed *key continuity management* (KCM) [50, 58]. This simple model, originally adopted by the program *ssh*, simply promiscuously accepts the first key proffered for any identity for which it does not currently know one (offering the user the chance to verify that key first, though they rarely do), and sounding a warning if that key then changes. This approach significantly lowers the barriers to entry for using public key cryptography, in return for slightly reduced initial security. Garfinkel and Miller applied this model to the problem of key management for e-mail encryption, embedding it into a popular e-mail client program [51, 59]. Their results suggest that KCM offers promise for easing practical deployment of e-mail encryption.

Finally, one of the most promising approaches to easing the interface between security and the user is through the use of portable personal devices, such as cell phones, which can carry credentials and perform cryptographic protocols on behalf of end users. Such devices have been used as intermediaries to protect users from giving credentials away in response to phishing attacks [52, 60] or as intuitive tools for authenticating users [28, 61] or creating [53, 62] or effecting [54, 63] access control policy.

### 4.2 Design Guidelines for Building Better Systems

Finally, there has been extensive work developing design guidelines that aim to help systems designers come up with systems that are both usable and secure. Perhaps the most influential, clearly stated, and comprehensive of these is due to Yee [64, 65]. Yee's guidelines blend long-agreed security design goals, such as *the principle of least authority* (or *privilege*)—which says that systems should operate with only the ability to access those resources necessary to do their job, with the best interests of end users. The results are principles such as *the path of least resistance* [64], which say that the easiest way to perform a task ought to also be the one that requires the least granting of authority. These guidelines argue for a distinctly user-focused view of security, arguing that systems should respond to the user's expressed intent to grant or remove authority, where intent should be expressed in terms of the task at hand—terms that are relevant, and understandable to the user. Other guidelines emphasize both that the input from the user is privileged, and must be protected so that user intent can be correctly captured; and that clear and understandable feedback of state to the user is critical for allowing the user to achieve both their task and security goals. These guidelines can be further refined and specialized to address particular user aims; for example, Chiasson et al. present a set of usable security design guidelines tailored toward the needs of systems administrators [66].

## 5 OPEN CHALLENGES AND TAKE-AWAYS

The field of usable security is still very young, and it is marked more by the number of open questions than of accepted answers. The good news is that users generally want to "do the right thing" with regard to security—if only they can figure out what that is,

and it does not keep them from getting their primary tasks done [9]. The goal of usable system design is to help them do just that.

One of the most open areas of research mentioned above is that of developing usable tools for secure, and *correct*, systems management. Because the users in this case are often administrators, not end users,[5] the requirement for improved usability is often underestimated (even by the users themselves [26, 66]). Because the tasks and tools involved are *security focused*—designed to solve a task wherein security management is often an explicit goal—it is perhaps easier to achieve effective security while keeping the user's primary task foremost [3].

The failure of existing tools and approaches for usable systems management can most clearly be seen in the prevalence of configuration errors in deployed systems—for example, the fact that 68% of deployed web server security certificates are currently invalid [7]. Such misconfigurations are surprisingly common, and reflected to the user in potentially confusing ways (Figs. 1 and 2).

While it is well known that configuration errors may result in insecure systems, there is a more subtle effect of such mistakes—every misconfiguration, on any system, decreases the ability of all other existing systems to recruit end users in defending their own security. Consider the *error attack*. If a malicious server is attempting to impersonate a critical system to a user (e.g. to capture passwords or other credentials), the attacker can explain the absence of any security indicator the user has been trained to rely upon simply by suggesting that "there is a problem with the system" [50].

As long as attacks and system configuration errors generate warnings that are indistinguishable to the end user, the end user must make a determination—"does this warning signal an actual attack or merely a misconfiguration?" Evidence suggests that overwhelmingly they assume the latter [67]—that the warning simply reflects a *false alarm*, and that they should proceed with what is for them, their much more urgent primary task. Given the relative frequency of genuine attacks and simple configuration errors, *this is the rational decision for them to make*. And it will continue to be, until configuration errors are vanishingly less common than genuine attacks. There are two ways to achieve this state: the first is to wait until the attack frequency rises to the point that systems are completely unusable (and hope that configuration errors do not rise in parallel). The better option is to reduce the incidence of configuration errors to the point where warnings


**FIGURE 1** This figure shows an error message generated by the Mozilla Firefox web browser when attempting to visit the default secure (SSL-protected) management page offered by a common consumer-grade wireless access point. The access point has been provisioned by the vendor with an invalid certificate. The antiphishing protections built into Mozilla Firefox make it impossible to actually visit this site and administer the device.

[5]Though as computers get more critically involved in every aspect of day-to-day life, "average" users are more and more often systems administrators as well [24].

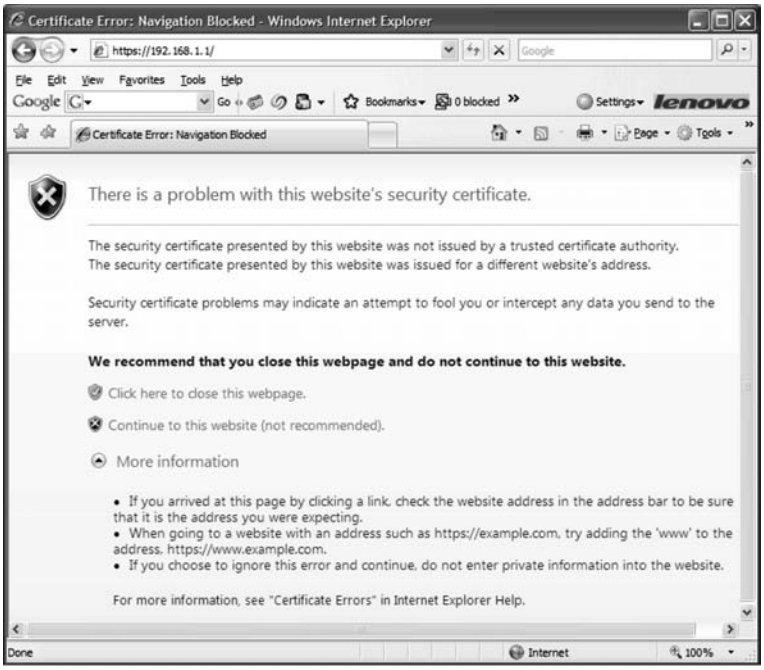



**FIGURE 2** This figure shows the error message generated by Internet Explorer 7 when attempting to visit the same SSL-protected configuration page as displayed in Figure 1. Using IE, one can override the security warnings and determine that the device contains a self-signed certificate with the serial number 0; this might be a certificate generated automatically by the device (and all devices incorrectly select 0 as a serial number, rather than say choosing a random value) or all devices might even be configured with the same certificate and private key. Note that the errors presented by Firefox and IE cite completely different problems with the certificate.

of attack are, with overwhelming likelihood, just that. To reduce configuration errors to that degree, we must either reduce the amount of configuration that must be performed or ensure that more of it is done correctly—this requires better systems management and configuration tools. Though those tools may not be "security tools" per se, they clearly play a security-critical function.

## 6 CONCLUSIONS

This article has presented a review of the current state of research in usable security. This is an extremely active, fast-moving field, as evidenced that most of the cited work was performed within the last 5 years. In any such rapidly moving area, new results are always appearing; the further reading list (below) contains pointers to places to find them. Equally important to the work reviewed here is the large body of work omitted for reasons of space—for example, this review does not consider work on usable *privacy*, itself an active area of research.

Perhaps the most important lessons to be learned from this body of work are that usability is indeed key to effective security and that it is possible to design systems that are simultaneously usable and secure—as long as you think it is important enough to do so.

## REFERENCES


1. RSA. (2007). *The Untold Insider Threat: Office Workers Confess to Everyday Behavior that Places Sensitive Information at Risk*, [Online] 12 10, 2007. [Cited: 1 11, 2008.] http://www.rsa.com/press_release.aspx?id=8992.
2. Schroeder, J. H. and Salzer, M. D. (1975). The protection of information in computer systems. *Proc. IEEE* **63**, 1278–1308.
3. Smetters, D. K. and Grinter, R. E. (2002). Moving from the design of usable security technologies to the design of useful secure applications. *Proceedings of the New Security Paradigms Workshop 2002*. Virginia Beach, VA.
4. Whitten, A. and Tygar, J. D. (1999). Why Johnny can't encrypt: a usability evaluation of PGP 5.0. *Proceedings of the 8th Usenix Security Symposium*. Usenix, Washington, DC, pp. 169–183.
5. Good, N. S. and Krekelberg, A. (2003). Usability and privacy: a study of Kazaa P2P file-sharing. *CHI '03: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM Press, Lauderdale, FL, pp. 137–144.
6. McAfee Corporation and National Cyber Security Alliance. (2007). *McAfee/NCSA cyber security survey*. *McAfee Corporation*. [Online] September 25, 2007. [Cited: January 6, 2008.] http://download.mcafee.com/products/manuals/en-us/McAfeeNCSA_Analysis09-25-07.pdf?cid=36665.
7. SecuritySpace (2008). *Secure Server Survey*. SecuritySpace, [Online] January 1, 2008. [Cited: January 6, 2008.] http://www.securityspace.com/s_survey/sdata/200712/certca.html.
8. RSA. (2006). *RSA Security Research Shows Volume of Business Passwords Overwhelming End Users and Hindering IT Security Efforts*, [Online] September 12, 2006. [Cited: 1 10, 2008.] http://www.rsa.com/press_release.aspx?id=7296.
9. Adams, A. and Sasse, M. A. (1999). Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures. *Commun. ACM* **42**, 40–46.
10. Gaw, S. and Felten, E. (2006). Password management strategies for online accounts. *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*. ACM Press, Pittsburgh, PA, pp. 44–55.
11. Sasse, M. A., Brostoff, S., and Weirich, D. (2001). Transforming the "weakest link": a human-computer interaction approach to usable and effective security. *BT Tech. J.* **19**(3), 122–131.
12. Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G., and Furlong, M. (2007). Password sharing: implications for security design based on social practice. *CHI '07: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM Press, San Jose, CA, pp. 895–904. doi = http://doi.acm.org/10.1145/1240624.1240759.
13. Brostoff, S. and Sasse, M. A. (2003). Ten strikes and you're out: Increasing the number of login attempts can improve password usability. *Workshop on Human-Computer Interaction and Security Systems*, part of CHI2003, Ft. Lauderdale, FL.

14. Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2005). The memorability and security of passwords. In *Security and Usability: Designing Secure Systems that People Can Use*, L. F. Cranor and S. Garfinkel, Eds. O'Reilly & Associates, Sebastopol, CA.
15. Thorpe, J. and van Oorschot, P. C. (2004). Graphical dictionaries and the memorable space of graphical passwords. *Proceedings of the 13th Annual USENIX Security Symposium*. Usenix, San Diego, CA, pp. 135–150.
16. Chiasson, S., Biddle, R., and Oorschot, P. C. (2007). A second look at the usability of click-based graphical passwords. *ACM Symposium on Usable Privacy and Security (SOUPS 2007)*. ACM Press, Pittsburgh, PA, pp. 1–12.
17. Kuo, C., Romanosky, S., and Cranor, L. F. (2006). Human selection of mnemonic phrase-based passwords. *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*. ACM Press, Pittsburgh, PA, pp. 67–78.
18. Thorpe, J. and van Oorschot, P. C. (2007). Human-seeded attacks and exploiting hot-spots in graphical passwords. *Proceedings of the 16th Annual Usenix Security Symposium*. Usenix, Boston, MA, pp. 103–118.
19. Ahmet, E. D., Memon, N., and Birget, J.-C. (2007). Modeling user choice in the PassPoints graphical password scheme. *ACM Symposium on Usable Security and Privacy (SOUPS07)*. ACM Press, Pittsburgh, PA, pp. 20–28.
20. Yee, K.-P. and Sitaker, K. (2006). Passpet: convenient password management and phishing protection. *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*. ACM Press, Pittsburgh, PA, pp. 32–43.
21. Wu, M., Miller, R. C., and Little, G. (2006). Web wallet: preventing phishing attacks by revealing user intentions. *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*. ACM Press, Pittsburgh, PA, pp. 102–113.
22. Ross, B., Jackson, C., Miyake, N., Boneh, D., and Mitchell, J. C. (2005). Stronger password authentication using browser extensions. *Proceedings of the 14th Conference on USENIX Security Symposium—Volume 14*, (Baltimore, MD, July 31—August 05, 2005). USENIX Association, Berkeley, CA, pp. 17–32.
23. Chiasson, S., Oorschot, P. C., and Biddle, R. (2006). A usability study and critique of two password managers. *Proceedings of the 15th Annual Usenix Security Symposium*. Vancouver, BC, pp. 1–16.
24. Shehan, E. and Edwards, W. K. (2007). Home networking and HCI: what hath God wrought? *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2007)*. San Jose, CA, April 28-May 3, 2007.
25. Kandogan, E. and Eben, M. H. (2005). Security administration tools and practices. In *Security and Usability: Designing Secure Systems that People Can Use*, L. F. Cranor and S. Garfinkel, Eds. O'Reilly Media, Sebastapol, pp. 357–378. http://www.plunk.org/eben/PublishedPapers/Security-ch18.pdf.
26. Barrett, R., Kandogan, E., Maglio, P. P., Haber, E. M., Takayama, L. A., and Prabaker, M. (2004). Field studies of computer system administrators: analysis of system management tools and practices. *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*, CSCW '04. (Chicago, Illinois, USA, November 06–10, 2004). ACM, New York, pp. 388–395. DOI = http://doi.acm.org/10.1145/1031607.1031672.
27. Botta, D., Werlinger, R., Gagné, A., Beznosov, K., Iverson, L., Fels, S., and Fisher, B. (2007). Towards understanding IT security professionals and their tools. *Proceedings of the 3rd Symposium on Usable Privacy and Security*, SOUPS '07, vol. 229. (Pittsburgh, Pennsylvania, July 18–20, 2007). ACM, New York, pp. 100–111. DOI = http://doi.acm.org/10.1145/1280680.1280693.

28. Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D. K., and Stewart, P. (2004). Network-in-a-box: how to set up a secure wireless network in under a minute. *13th Usenix Security Symposium*. San Diego, CA, August, 2004.

29. Lau, S. (2003). *The Spinning Cube of Potential Doom*. *National Energy Research Scientific Computing Center*, [Online] December 10, 2003. [Cited: January 20, 2008.] http://www.nersc.gov/nusers/security/TheSpinningCube.php.

30. Stoll, J., Tashman, C., Edwards, W. K., and Spafford, K. (2008). Sesame: informing user security decisions with system visualization. *Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI 2008)*. Florence, April 5–10, 2008.

31. Zurko, M. E. and Simon, R. T. (1996). User-centered security. *Proceedings of the 1996 Workshop on New Security Paradigms*, NSPW '96. (Lake Arrowhead, California, United States, September 17–20, 1996). ACM, New York, pp. 27–33. DOI = http://doi.acm.org/10.1145/304851.304859.

32. Zurko, M. E., Simon, R., and Sanfilippo, T. (1999). A user-centered, modular authorization service built on an RBAC foundation. *Proceedings of the 1999 IEEE Symposium on Security and Privacy*. Oakland, CA, pp. 57–71.

33. Maxion, R. A. and Reeder, R. W. (2005). Improving user-interface dependability through mitigation of human error. *Int. J. Human Comp. Studies* **63**(1-2), 25–50. [DOI: 10.1016/j.ijhcs.2005.04.009]

34. Reeder, R. W., Bauer, L., Cranor, L. F., Reiter, M. K., Bacon, K., How, K., and Strong, H. (2008). Expandable grids for visualizing and authoring computer security policies. *ACM SIGCHI Conference on Human Factors in Computing Systems* (CHI '08). Florence, Italy.

35. Karat, J., Karat, C.-M. Brodie, C., and Feng, J. (2005). Privacy in information technology: designing to enable privacy policy management in organizations. *Int. J. Human Comp. Studies* **63**(1-2), 153–174.

36. Cao, X. and Iverson, L. (2006). Intentional access management: making access control usable for end-users. *Proceedings of the Second Symposium on Usable Privacy and Security*, SOUPS '06, vol. 149. (Pittsburgh, Pennsylvania, July 12–14, 2006). ACM, New York, pp. 20–31. DOI = http://doi.acm.org/10.1145/1143120.1143124.

37. Jakobsson, M. and Myers, S. A. Ed. (2006). *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*. Wiley, Hoboken, NJ.

38. Dhamija, R., Tygar, J. D., and Hearst, M. (2006). Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06. (Montréal, Québec, Canada, April 22–27, 2006). R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson, Eds. ACM, New York, pp. 581–590. DOI = http://doi.acm.org/10.1145/1124772.1124861.

39. Jackson, C., Simon, D., Tan, D., and Barth, A. (2007). An evaluation of extended validation and picture-in-picture phishing attacks. *Proceedings of the 1st International Conference in Usable Security (USEC07), part of the Proceedings of the Conference on Financial Cryptography*. Lowlands, Scarborough, Trinidad/Tobago.

40. Downs, J. S., Holbrook, M. B., and Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. *Proceedings of the Second Symposium on Usable Privacy and Security*. Pittsburgh, PA, July 12–14, 2006. ~[doi>10.1145/1143120.1143131]

41. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). Protecting people from phishing: the design and evaluation of an embedded training email system. *CHI 2007: Conference on Human Factors in Computing Systems*, San Jose, CA, April 28–May 3, 2007, pp. 905–914.

42. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., and Nunge, E. (2007). Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. *Proceedings of the 2007 Symposium On Usable Privacy and Security*. Pittsburgh, PA, July 18–20 200.

43. Wu, M., Miller, R. C., and Garfinkel, S. L. (2006). Do security toolbars actually prevent phishing attacks? *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '06. (Montréal, Québec, Canada, April 22–27, 2006). R. Grinter, T. Rodden, P. Aoki, E. Cutrell, R. Jeffries, and G. Olson, Eds. ACM, New York, pp. 601–610. DOI = http://doi.acm.org/10.1145/1124772.1124863.

44. Zhang, Y., Egelman, S., Cranor, L., and Hong, J. (2007). Phinding phish: evaluating anti-phishing tools. 2007. *Proceedings of the 14th Annual Network & Distributed System Security Symposium (NDSS 2007)*, San Diego, CA, February 28th–2nd March.

45. Zhang, Y., Hong, J., and Cranor, L. (2007). CANTINA: a content-based approach to detecting phishing web sites. 2007. *Proceedings of the 16th International World Wide Web Conference (WWW2007)*. Banff, AB, May 8–12, 2007, pp. 639–648.

46. Cook, D. L., Gurbani, V., and Daniluk, M. (2008). Phishwish: a stateless phishing filter using minimal rules. *Proceedings of Financial Crypto*, El Cozumeleno Beach Resort, Cozumel, January, 2008.

47. Provos, N., McNamee, D., Mavrommatis, P., Wang, K., and Modadugu, N. (2007). The ghost in the browser analysis of web-based malware. *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets*. (Cambridge, MA). USENIX Association, Berkeley, CA, pp. 4–4.

48. Dhamija, R. and Tygar, J. D. (2005). The battle against phishing: dynamic security skins. *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, vol. 93. (Pittsburgh, Pennsylvania, July 06–08, 2005). ACM, New York, pp. 77–88. DOI = http://doi.acm.org/10.1145/1073001.1073009.

49. Bank of America (2006). *How Bank of America SiteKey Works for Online Banking Security*. *Bank of America*, [Online] 2006. [Cited: January 19, 2008.] http://www.bankofamerica.com/privacy/sitekey/.

50. Schechter, S. E., Dhamija, R., Ozment, A., and Fischer, I. (2007). *The Emperor's New Security Indicators*. IEEE Computer Society, Washington, DC, SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy. pp. 51–65.

51. Balfanz, D., Durfee, G., Grinter, R. E., and Smetters, D. K. (2004). In search of usable security—five lessons from the field. *IEEE J. Secur. Priv.* **2**(5), 19–24.

52. Balfanz, D., Durfee, G. and Smetters, D. K. (2005). Making the Impossible easy: usable PKI. In *Security and usability: Designing Secure Systems that People Can Use*, L. F. Cranor and S. Garfinkel, Eds. O'Reilly Media, Sebastopol, CA, pp. 319–334.

53. Balfanz, D., Smetters, D. K., Stewart, P., and Wong, H. C. (2002). Talking to strangers: authentication in ad-hoc wireless networks. *Network and Distributed System Security Symposium*. Internet Society, San Diego, CA, February 6–8, 2002.

54. Stajano, F. and Anderson, R. J. (2000). The resurrecting duckling: security issues for Ad-hoc wireless networks. In *Proceedings of the 7th international Workshop on Security Protocols*, Lecture Notes In Computer Science, vol. 1796 (April 19–21, 1999). B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, Eds. Springer-Verlag, London, pp. 172–194.

55. McCune, J. M., Perrig, A., and Reiter, M. K. (2005). Seeing-Is-believing: using camera phones for human-verifiable authentication. *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, (May 08–11, 2005). IEEE Computer Society, Washington, DC, pp. 110–124. DOI = http://dx.doi.org/10.1109/SP.2005.19.

56. Balfanz, D. (2003). Usable access control for the world wide web. *Proceedings of the 19th Annual Computer Security Applications Conference*, ACSAC, (December 08–12, 2003). IEEE Computer Society, Washington, DC, p. 406.

57. Gutmann, P. (2003). Plug-and-play PKI: a PKI your mother can use. *Proceedings of the 12th Conference on USENIX Security Symposium—Volume 12*, (Washington, DC, August 04–08, 2003). USENIX Association, Berkeley, CA, pp. 4–4.

58. Gutmann, P. *Underappreciated security mechanisms*. *Peter Gutmann*, [Online] [Cited: 1 20, 2008.] http://www.cs.auckland.ac.nz/~pgut001/pubs/underappreciated.pdf.

59. Garfinkel, S. L. and Miller, R. C. (2005). Johnny 2: a user test of key continuity management with S/MIME and outlook express. *Proceedings of the 2005 Symposium on Usable Privacy and Security*, SOUPS '05, vol. 93. (Pittsburgh, Pennsylvania, July 06–08, 2005). ACM, New York, pp. 13–24. DOI=http://doi.acm.org/10.1145/1073001.1073003.

60. Parno, B., Kuo, C., and Perrig, A. (2006). Phoolproof phishing prevention. *Financial Cryptography and Data Security 10th International Conference*. British West Indies, February 27–March 2, 2006.

61. Corner, M. D. and Noble, B. D. (2002). Zero-interaction authentication. *Proceedings of the 8th Annual international Conference on Mobile Computing and Networking*, (Atlanta, Georgia, USA, September 23–28, 2002). ACM, New York, pp. 1–11. DOI=http://doi.acm.org/10.1145/570645.570647.

62. Bauer, L., Cranor, L. F., Reeder, R. W., Reiter, M. K., and Vaniea, K. (2008). A user study of policy creation in a flexible access-control system. *ACM SIGCHI Conference on Human Factors in Computing Systems* (CHI '08).

63. Smetters, D. K., Balfanz, D., Durfee, G. E., Smith, T., and Lee, K. (2006). Instant matchmaking: simple, secure virtual extensions to ubiquitous computing environments. Ubicomp 2006, *Proceedings of the 8th International Conference of Ubiquitous Computing*. Springer Verlag, Irvine, CA, September 17–21, 2006; LCS 4206: pp. 477–494.

64. Yee, K.-P. (2002). User interaction design for secure systems. In *Proceedings of the 4th International Conference on Information and Communications Security*, Lecture Notes in Computer Science 2513, R. Deng, S. Qing, F. Bao, and J. Zhou, Eds. Springer-Verlag, Heidelberg, http://zesty.ca/sid/.

65. Yee, K.-P. (2005). Guidelines and strategies for secure interaction design (Chapter 13). In *Security and Usability: Designing Secure Systems that People Can Use*, L. F. Cranor and S. Garfinkel, Eds. O'Reilly, Sebastopol, CA.

66. Chiasson, S., Biddle, R., and Somayaji, A. (2007). Even experts deserve usable security: design guidelines for security management systems. *Workshop on Usable IT Security Management (USM'07) held with the ACM Symposium on Usable Privacy and Security (SOUPS 2007)*, July 2007.

67. Mannan, M., van Oorschot, P. C. Security and usability: the gap in real-world online banking. *New Security Paradigms Workshop (NSPW)*. New Hampshire. Sept. 18–21, 2007.

## FURTHER READING

Cranor, L. F. and Garfinkel, S. *Security and Usability: Designing Secure Systems that People Can Use*. O'Reilly & Associates, 2005.

Gutmann, P. (2008). *Usable Security Fundamentals*, http://www.cs.auckland.ac.nz/~pgut001/pubs/usability.pdf.

*The HCISEC Bibliography*. http://gaudior.net/alma/biblio.html.

Yee, K.-P. *The Usable Security Blog*. http://usablesecurity.com/.

# CYBER SECURITY EDUCATION, TRAINING, AND AWARENESS

RICHARD KISSEL AND MARK WILSON
*National Institute of Standards and Technology, Gaithersburg, Maryland*

## 1 INTRODUCTION

The cyber security education, training, and awareness (ETA) program is a critical component of the cyber security program. It is *the* vehicle for disseminating security information that the workforce, including managers, need to do their jobs. In terms of the total security solution the importance of the workforce in achieving cyber security goals and the importance of learning as a countermeasure, cannot be overstated. Establishing and maintaining a robust and relevant ETA program as part of the overall cyber security program is the primary conduit for providing the workforce with the information and tools needed to protect an organization's vital information resources. These programs will ensure that personnel at all levels of the organization understand their cyber security responsibilities to properly use and protect the information and resources entrusted to them. Organizations that continually train their workforce in organizational cyber security policy and role-based cyber security responsibilities will have a higher rate of success in protecting information. As cited in audit reports, periodicals, and conference presentations, people are arguably the weakest element in the cyber security formula that is used to secure systems and networks. The *people factor*, not technology, is a critical factor that is often overlooked in the cyber security equation. Robust and enterprise-wide ETA programs are needed to address this growing concern.

## 2 EDUCATION, TRAINING, AND AWARENESS POLICY

All users have cyber security responsibilities. Although there is no mandate for formal education (provided by colleges or universities) and certification of information security professionals, they are mentioned in this section since some organizations include them as part of a comprehensive training solution for employees.

## 3 COMPONENTS: EDUCATION, TRAINING, AWARENESS, AND CERTIFICATION

An organization's cyber security program policy should contain a clear and distinct section devoted to organization-wide requirements for the ETA program. Although cyber security ETA is generally referred to as *"a"* program, many organizations consider ETA to be three distinct functions, each with separate purposes, goals, and approaches. Proper

implementation of these components (with consideration of options such as professional certification) promotes professional development, which leads to a high-performance workforce.

Requirements for the cyber security ETA program should be documented in the enterprise-level policy and should include:

- definition of cyber security roles and responsibilities;
- development of program strategy and a program plan;
- implementation of the program plan; and
- maintenance of the cyber security ETA program.

### 3.1 Education

Education integrates all of the cyber security skills and competencies of the various functional specialties into a common body of knowledge and adds a multidisciplinary study of concepts, issues, and principles (technological and social). Cyber security education strives to produce cyber security specialists and professionals who are capable of vision and proactive response. A significant and increasing number of colleges and universities provide academic programs to support the cyber security needs of the public and private sectors. Many of these schools partner with the public sector to accomplish research and development tasks to improve cyber security. The National Security Agency (NSA) and the Department of Homeland Security (DHS) have built and are maintaining a robust program called the *Centers of Academic Excellence* in Information Assurance Education. The program seeks to produce a growing number of professionals with information assurance expertise in various disciplines.

### 3.2 Training

Cyber security training strives to produce the relevant and required security knowledge and skills within the workforce. Training supports competency development and helps personnel understand and learn how to perform their cyber security role. The most important difference between training and awareness is that training seeks to teach skills that allow a person to perform a specific function, while awareness seeks to focus an individual's attention on an issue or a set of issues.

Role-based training provides cyber security modules and/or courses that are tailored to the specific needs of each group of people who have been identified as having significant responsibilities for information security in their organization. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16 provides guidance for establishing role- and performance-based cyber security training programs. Other models that can be used for developing role-based cyber security training are the Committee on National Security Systems (CNSS) Training Standards, the Office of Personnel Management (OPM) "IT Roadmap", and the DHS Essential Body of Knowledge (EBK).

Critical elements to address or consider when developing training material are:

- *Needs assessment.* A needs assessment will identify what additional cyber security training is needed or required, beyond what the organization is currently doing. Sometimes, the needs assessment takes the form of an auditor's report. The needs

assessment may identify additional people in particular roles who need training, or it may identify that people who have trained need additional training. A needs assessment will help an organization determine if a complete training course is necessary or if a module that focuses on particular topics will be sufficient.

- *Setting the bar.* "Setting the bar" means that a decision must be made as to the complexity of the material that will be developed. The complexity must be commensurate with the role and the needs of the person or people who will undergo the learning effort. Material should be developed based on two important criteria: (i) the target attendee's position within the organization, and (ii) knowledge of the cyber security skills required for that position. The complexity of the material must be determined before development begins. Setting the bar is an important aspect of the "scoping guidance" to be developed and utilized throughout the analysis, design, development, implementation, and evaluation ("Analysis, Design, Development, Implementation,and Evaluation (ADDIE)") process.
- *The ADDIE instructional design model.* The ADDIE model is a systematic instructional design model consisting of five phases: *a*nalysis, *d*esign, *d*evelopment, *i*mplementation, and *e*valuation. Each phase consists of outcomes that feed into the next phase in the model. For example, input to the Analysis Phase is the output of the needs assessment identifying the existing training gaps within the organization. As each role is analyzed, attention should be paid to the competencies or knowledge, skills, and abilities (KSAs) needed for each role as well as the particular topics, tasks, and/or elements that support the competencies or KSAs. Each competency or KSA used within each role may become a module that is suitable for use within other role-based training that may be required. For example, many cyber security roles require some level of knowledge of laws and organizational policy. A single development effort with multiple modules that can be added and removed based on the particular audience, could save significant development time.
- *Role-based training versus topic-based training.* Role-based cyber security training allows the recipient of the training to learn what he or she needs to know and be able to do, based on their current job. This is perhaps the most important distinction between role-based and topic-based training. While topic-based training is easier to develop because, for the most part, it can be developed once and for diverse audiences, it approaches being a one-size-fits-all solution. Unfortunately, an easy solution like this, to a complex issue like cyber security training, can in itself be a vulnerability as dangerous as a poorly configured operating system or firewall. Topic-based training is best employed within a role-based training framework, when a particular topic (e.g. incident response and reporting, configuration management, contingency planning) needs to be taught as a stand-alone module (or part of a training course) to people in a particular role, or to a group of people in different roles who need to know a similar amount of information about that topic.
- *Sources of cyber security training.* The first step in determining sources of training material to build a course or module is to decide if the material will be developed in-house or contracted out. If the organization has in-house expertise and can afford to allocate the necessary resources to develop training material for courses

and/or modules, there are several federal government-focused training documents or programs that can be used. These include:

- *NIST SP 800-16.* This document contains a robust role-based training methodology. The general-to-specific aspects of the methodology include a list of roles, role-specific matrices that contain responsibilities and training areas, and specific sets of cells for each role matrix that, in turn, contain cyber security topics and elements to be used to build training material for each cell.
- *CNSS training standards.* These standards are also role-based and contain sets of tasks, capabilities, and KSAs needed for those serving in each role.
- *OPM IT roadmap.* This OPM project is a web-based application based on the federal government's GS-2210 Information Technology (IT) Specialist Job Series. One of the IT Specialist subseries, the Information Security "parenthetical", has related levels of learning, competencies, expected behaviors, and recommended training courses.
- *DHS EBK.* This document is based on a number of existing federal guidelines and standards. It contains a methodology that includes roles, competency areas, responsibilities, terms, and concepts.

### 3.3 Awareness

Cyber security awareness is a blended solution of activities that promote security, establish accountability, and inform the workforce of security news. Awareness seeks to focus an individual's attention on an issue or a set of issues. Awareness is a program that continually pushes the cyber security message to users in a variety of formats.

An awareness program includes a variety of tools, communication, outreach, and metrics development.

- *Tools.* Awareness tools are used to promote cyber security and inform users of threats and vulnerabilities that impact their organization and "personal" work environment by explaining the "what" but not the "how" of security, and communicating what-is- and what-is-not-allowed. Awareness is used to explain the rules of behavior for using an organization's information and information systems and establishes a level of expectation on the acceptable use of the same. Awareness not only communicates cyber security policies and procedures that need to be followed, but also provides the foundation for any sanctions and disciplinary actions imposed for noncompliance. Types of tools include:
  - events, such as a cyber security awareness day;
  - promotional materials;
  - briefings (program- or system-specific or issue-specific); and
  - rules of behavior.
- *Communication.* A large part of an awareness effort is communication with users, managers, executives, system owners, and others. A communications plan is needed to identify stakeholders, types of information that is to be disseminated, channels for disseminating information, and the frequency of information exchanges. The plan

also identifies whether the communications are one-way or two-way. Activities that support communication include:
  - assessment (as is/to be models);
  - strategic plan; and
  - program implementation.
- *Outreach.* Outreach is critical for leveraging best practices within any organization. It has two elements for intra- and inter-organization awareness. The intraorganization element promotes internal awareness of cyber security. A Web portal that provides a one-stop shop for cyber security information can be an effective outreach tool. Policy, frequently asked questions (FAQs), cyber security e-newsletters, links to resources, and other useful information are easily accessible to all employees. This tool promotes a consistent and standard message. The interorganization element promotes sharing among organizations and is used to leverage training and awareness resources.

### 3.4 Certification

In response to the growing demand for cyber security personnel within organizations, in both the public and private sectors, there has been a movement toward increased professional standards for cyber security personnel. This "professionalization" integrates education, training, and experience with an assessment mechanism to validate knowledge and skills, resulting in the certification of a predefined level of competence.

## 4 DESIGNING, DEVELOPING, AND IMPLEMENTING AN EDUCATION, TRAINING, AND AWARENESS PROGRAM

The development of a cyber security ETA program involves three major steps:

1. *Designing* the program (including the development of the cyber security ETA program plan);
2. *Developing* the ETA material; and
3. *Implementing* the program.

Even a small amount of cyber security ETA can go a long way toward improving the cyber security posture of, and vigilance within, an organization.

### 4.1 Designing an ETA Program

ETA programs must be designed with the mission of the organization in mind. The ETA program must support the business needs of the organization and be relevant to the organization's culture and information technology architecture. The most successful programs are those that users feel are relevant to the subject matter and issues presented.

Designing an ETA program answers the question "What is our plan for developing and implementing ETA opportunities that are compliant with existing policies?" In the design step of the program, the organization's ETA needs are identified, an effective organization-wide plan is developed, organizational buy-in is sought and secured, and priorities are established.

### 4.2 Developing an ETA Program

Once the ETA program has been designed, supporting material can be developed. Material should be developed with the following in mind:

"What behavior do we want to reinforce?" (awareness);

"What skill or skills do we want the audience to learn and apply?" (training and education).

In both cases, the focus should be on specific material that the participants should integrate into their jobs. Attendees will pay attention and incorporate what they see or hear in a session if they feel that the material was developed specifically for them. Any presentation that feels so impersonal and general that it could be given to any audience, will be filed away as just another of the annual "We're here because we have to be here" sessions. An ETA program can be effective, however, if the material is interesting, current, and relevant.

The awareness audience must include all users in an organization. Users may include employees, contractors, other organization personnel, visitors, guests, and other collaborators or associates requiring access. The message to be spread through an awareness program, or campaign, should make all individuals aware of their commonly-shared cyber security responsibilities.

On the other hand, the message in a training class is directed at a specific audience. The message in training material should include everything related to cyber security that attendees need to know in order to perform their jobs. Training material is usually far more in-depth than material used in an awareness session or campaign.

An education course goes beyond the immediately practical skills taught in training sessions by presenting the underlying and related concepts, issues, and principles of particular aspects of the profession. This allows the student to understand the subject in far greater depth than is usually provided in training.

### 4.3 Implementing an ETA Program

A cyber security ETA program should be implemented only after a needs assessment has been conducted, a strategy has been developed, an ETA program plan for implementing that strategy has been completed, and ETA material has been developed.

The program's implementation must be fully explained to the organization to achieve support for its implementation and commitment of necessary resources. This explanation includes expectations of organization management and staff support, as well as expected results of the program and benefits to the organization. Funding issues must also be addressed. For example, organization managers must know if the cost to implement the ETA program will be totally funded by the Chief Information Officer (CIO) or the cyber security program budget, or if their budgets will be impacted to cover their share of the expense of implementing the program. It is essential that everyone involved in the implementation of the program understand their roles and responsibilities. In addition, schedules and completion requirements must be communicated.

Once the plan for implementing the ETA program has been explained to (and accepted by) organization management, the implementation can begin. Since there are several ways to present and disseminate ETA material throughout an organization, organizations should tailor their implementation to the size, organization, and complexity of their enterprise.

### 4.4 Postimplementation

An organization's cyber security ETA program can quickly become obsolete if sufficient attention is not paid to technological advancements, IT infrastructural changes, organizational changes, and shifts in organizational mission and priorities. CIOs and senior organization cyber security officers need to be cognizant of this potential problem and incorporate mechanisms into their strategy to ensure that the program continues to be relevant and compliant with overall objectives. Continuous improvement should always be the theme for cyber security ETA initiatives, as this is one area where *you can never do enough*. Efforts supporting this postimplementation feedback loop should be developed with respect to the cyber security organization's overall ongoing performance measures program.

### 4.5 Monitoring Compliance

Once the program has been implemented, processes should be put in place to monitor compliance and effectiveness. An automated tracking system can be designed to capture key information on program activity (e.g. courses, dates, audience, costs, sources etc.). The tracking system should capture this data at an organization level, so it can be used to provide enterprise-wide analysis and reporting regarding ETA initiatives. Tracking compliance involves assessing the status of the program as indicated by the database information, and mapping it to standards established by the organization. Reports can be generated and used to identify gaps or problems. Corrective action and necessary follow-up can then be taken. This follow-up may take the form of formal reminders to management; additional ETA offerings; and/or the establishment of a corrective plan with scheduled completion dates. A tracking system is likely to be more economically feasible in a government agency or a large company than in a small business. A small business may not be able to justify the costs of such a system, and in a small business it should be easier to track those employees needing and attending cyber security training.

### 4.6 Evaluation and Feedback

Formal evaluation and feedback mechanisms are critical components of any cyber security ETA program. Continuous improvement cannot occur without a good sense of how the existing program is working. In addition, the feedback mechanism must be designed to address objectives initially established for the program. Once the baseline requirements have been solidified, a feedback strategy can be designed and implemented. Various evaluation and feedback mechanisms that can be used to update the ETA program plan include surveys, evaluation forms, independent observation, status reports, interviews, focus groups, technology shifts, and/or benchmarking.

A feedback strategy should incorporate elements that address quality, scope, deployment method (e.g. Web-based, on-site, off-site), level of difficulty, ease of use, duration of session, relevancy, currency, and suggestions for modification.

Metrics are essential to feedback and evaluation. They can be used to:

- measure the effectiveness of the cyber security ETA program;
- provide information for many of the data requests that an organization may be required to provide with regard to compliance; and,

- provide an important gauge for demonstrating progress and identifying areas for improvement.

### 4.7 Managing Change

It is necessary to ensure that the program, as structured, continues to evolve as new technology and associated cyber security issues emerge. Training needs will shift as new skills and capabilities become necessary to respond to new architectural and technology changes. A change in the organizational mission and/or objectives can also influence ideas on how best to design training solutions and content. Emerging issues, such as homeland defense, will also impact the nature and extent of cyber security ETA activities that are necessary to keep users informed and/or trained about the latest threats, vulnerabilities, and countermeasures. New laws and court decisions may also impact organization policy that, in turn, may affect the development and/or implementation of ETA material. Finally, as cyber security policies evolve, ETA material should reflect these changes.

### 4.8 Program Success Indicators

CIOs, program officials, and organization cyber security officers should be primary advocates for ETA. Securing an organization's information and infrastructure is a team effort, requiring the dedication of capable individuals to carry out their assigned cyber security roles within the organization. Listed below are some key indicators to gauge the support for, and acceptance of, the program:

- key stakeholder demonstrates commitment and support;
- sufficient funding is budgeted and available to implement the agreed-upon ETA strategy;
- appropriate organizational placement of senior officials with key cyber security responsibilities;
- infrastructure to support broad distribution (e.g. Web, e-mail, learning management systems) and posting of cyber security ETA materials is funded and implemented;
- executive/senior-level officials deliver messages to staff regarding cyber security (e.g. staff meetings, broadcasts to all users by organization head), champion the program, and demonstrate support for training by committing financial resources to the program;
- metrics indicate improved cyber security performance by the workforce (e.g. to explain a decline in cyber security incidents or violations, indicate that the gap between existing ETA coverage and identified needs is shrinking, the percentage of users being exposed to awareness material is increasing, the percentage of users with significant cyber security responsibilities being appropriately trained is increasing);
- executives and managers do not use their status in the organization to avoid cyber security controls that are consistently adhered to by the rank and file;
- level of attendance at cyber security forums/briefings/training is consistently high.
- recognition of cyber security contributions (e.g. awards, contests) is a standard practice within an organization; and
- individuals playing key roles in managing/coordinating the cyber security program demonstrate commitment to the program and motivation to promote the program.

**REFERENCES**

1. National Institute of Standards and Technology Special Publication 800–16. (1998). *Information Technology Security Training Requirements: A Role- and Performance-Based Model*.
2. National Institute of Standards and Technology Special Publication 800–50. (2003). *Building an Information Technology Security Awareness and Training Program*.
3. National Institute of Standards and Technology Special Publication 800–55. (2003). *Security Metrics Guide for Information Technology Systems*.

# INDUSTRIAL PROCESS CONTROL SYSTEM SECURITY

IVAN SUSANTO, RICH JACKSON JR., AND DONALD L. PAUL
*Chevron Corporation, San Ramon, California*

## 1 INTRODUCTION

Process control systems or industrial automation and control systems (IACS) used in the O&G Industry are vulnerable to new threats with potentially serious consequences. Vulnerabilities come from many sources, including, but not limited to increasing access to IACS, increased digital intensity in the form of digital oil fields, smart sensors generating ever increasing amounts of data, real-time optimization, reservoir modeling, and global value chains that are highly leveraged on information and connectivity. In order to address these vulnerabilities, a public–private partnership called *Project LOGIIC* was formed to create and execute projects that address critical O&G cyber security Research and Development (R&D) needs, and produce solutions upon their completion, which can be deployed in the industry. ISA Security Compliance Institute (ISCI) also combines the talents of industry leaders from a number of major control system users and manufacturers to create a collaborative industry certification-based program.

## 2 BACKGROUND

Process control systems or IACS are used by O&G companies at their offshore platforms, pipelines, refineries, plants, and other industrial assets. IACS are collections of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process. The systems include, but are not limited to [1]:

1. Industrial control systems including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control systems and safety-instrumented system [SIS] functions, whether they are physically separate or integrated.)
2. Associated information systems such as advanced or multivariable control, on-line optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems.
3. Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

There is an increased reliance on IACS for safe, secure, and reliable operations of facilities. Historically, it was thought that IACS were secure because they relied on proprietary networks and hardware and were considered immune to network attacks that plague corporate information systems. This is no longer true.

While no solution can offer a complete solution, defense-in-depth methods can help detect and delay or even prevent breaches. Without the right information at the right time, there cannot be an appropriate response to threats.

### 2.1 The Problem

IACS used in the O&G industry are potentially vulnerable to new threats. Standardization and integration with corporate business systems have increased the potential exposure to these systems. IACS data were traditionally used in a contained environment only by those in that environment. Now, government agencies, business partners, suppliers, and others want access to the IACS data, causing more time to be spent on filling requests and less attention to monitoring for potential breaches.

Most importantly, this integration requires network connections that provide access and raise risks and threats.

### 2.2 New Threats

Most people will click on interesting links, especially when they are sent by someone known to them. Employees and vendors often use thumb drives, CDs, or DVDs to support IACS, and these portable media are readily inserted into an IACS environment without scanning for viruses first. It takes real effort to stop and think about risk; whether it is real or a cleverly disguised threat.

Removable drives and e-mail links are just two ways that these threats can be introduced. Threats to energy industry systems have expanded beyond the typical physical attacks of the past. When these physical attacks are combined with cyber attacks on the control systems, the results could be much more damaging. The changing nature of control systems means that attackers ranging from hackers through organized cyber criminals and sophisticated insiders can have physical effects through cyber means.

The new networked control systems and commercial off the shelf (COTS) technology are vulnerable to attacks that are not specifically aimed at them. For example, the Port

of Houston had to shut down operation of its control system in September, 2001. This system controlled ship movement, docking, mooring, loading, and unloading. They were affected by a "denial of service" attack, which was not aimed at them but which affected them just the same. The attack was the result of a "botnet" or robot network of computers, typical to those used by organized crime.

There are other known security incidents happening in the industries as well, such as the Maroochy Shire Sewage Spill, an IP Address change shut down chemical plant, and a slammer-infected laptop shutting down a DCS.

These are the factors that contribute to risk in the IACS environment [2]:

- Adoption of open standardized technologies susceptible to known vulnerabilities;
- Connectivity of Control Systems with other networks, including the Corporate network;
- Insecure remote connections;
- Widespread availability of technical information about control systems.

On the basis of a recent industry trend, both security risks from insiders and outsiders still continue to be of most concern, with hackers gaining a greater understanding of IACS.

### 2.3 The Solution

LOGIIC-1 Team [3] within a critical infrastructure environment, addressing security risk is a shared problem that can only be addressed and solved collaboratively. In the LOGIIC partnership, the following were the goals:

- Demonstrating a forward-looking opportunity to reduce vulnerabilities of O&G process control environments.
- Creating a working model to leverage the collective resources of the O&G industry, government agencies, and national laboratories for future cyber security projects.
- Leveraging existing SCADA cyber security knowledge and tools from the O&G industry, government, and vendors to
  - align with existing and future activities being performed in the SCADA industry, National Laboratory Testbeds, and O&G industry;
  - assist the National Laboratory Testbeds with the research and development of new solutions focused on the O&G industry, which will address existing security weaknesses (evolutionary) and breakthrough security solutions (revolutionary).

ISA Certification is one resource that promises to provide asset owners [4] a well-designed and managed product security certification process, leading to improved process reliability and safety. Certification responds to a common need for a shared security vision to be executed by suppliers, asset owners, and consultants. It also will promote better field-tested standards that are clearly followed by industry.

## 3 SCIENTIFIC STUDY

In the LOGIIC-1 Project (Event Correlation), a defense-in-depth solution can collect all raw events (data) from IACS to business/corporate network, correlate it and analyze

abnormal events to provide information to decision makers enabling them to validate threats and take appropriate action.

Monitoring is the key to building better defenses, especially for new unknown threats and vulnerabilities, but implementing even a simple perimeter intrusion detection system (IDS) can produce such volumes of data that it can become overwhelming. Too much data from an IDS would then become a hindrance rather than a help.

And as illustrated in Figure 1, for systems without layered security architecture, it only takes a single vulnerability for an attacker to bring a system down. Even for systems with layered, defense-in-depth approaches to security, an attacker can still cause damage. We need to know how many "open doors" we have left for attackers.

One answer to the problem is to have a central correlation engine that is fed with inputs from IACS to the business/corporate network.

### 3.1 Correlation Benefits

While there are many sources of security data available, the amount of data is substantial and often in incompatible formats. Both of these factors hinder transforming the raw data into useful information [5]. A best-in-class correlation system can help by gathering data from all sources and analyzing it for trends.

Some benefits of implementing such a correlation system are

- Event and log aggregation;
- Normalizing of events into a standard format;
- Categorizing and prioritizing events;

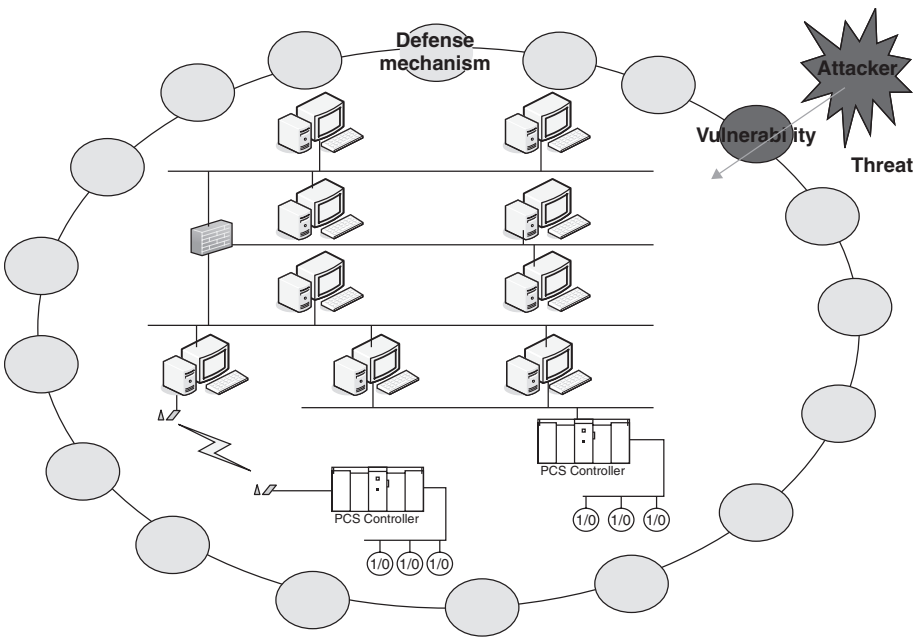



**FIGURE 1** Threats and vulnerabilities.

- Filtering extraneous events;
- Grouping similar events;
- Discovering relationships between events;
- Health monitoring from many small data points;
- Building big picture of the IACS health.

Awareness of a problem is the first step to implementing preventive or corrective measures.

### 3.2 Detection

There are four types of security events that should be detected.

In Figure 2, we let the depicted barrier abstractly to represent the perimeter defense. The four categories of events that we want to detect apply to the physical world as well as to computer systems and networks.

The probing/provocation category represents the case when attackers attempt to penetrate the defense but are unsuccessful. Examples in the cyber realm include port scanning and repeated authentication or authorization failures, such as password-guessing or file system browsing. Even though the perimeter defense works as intended, we still want to detect this kind of event because we are under attack and the attackers could eventually succeed.

Circumvention occurs when attackers find a way to reach their goal without confronting the perimeter defense. As an example, a corporation could have a strictly configured firewall protecting its corporate network from the Internet, but a badly configured wireless access point on the corporate network can allow an attacker parked on the street outside to get to the network without even going through a firewall.

Penetration occurs when vulnerability in the perimeter defense allows attackers to get through. An example of penetration is when an attacker with knowledge of software bugs can compromise the system using access that allows through well-configured firewall.

Finally, Insiders are attackers already inside the perimeter. For example, a firewall between the corporate network and the Internet does nothing to stop a disgruntled employee from stealing data from an internal database and hand-carrying it out of the building on a CD-ROM or other portable storage device. It should be noted that an

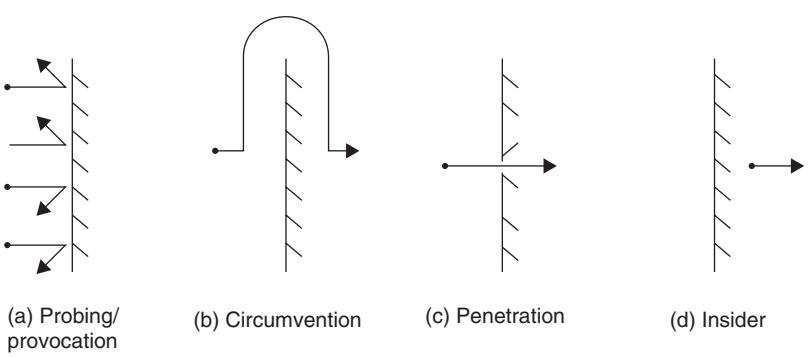



**FIGURE 2** IDS event triggered responses [6, p. 7].

attacker who has used circumvention or penetration to get inside the perimeter could also be considered an insider, from a detection perspective.

## 3.3 Technical Challenges

***3.3.1 Typical IACS Environment.*** A test bed model (Fig. 3) in LOGIIC-1 project was developed using generic DCS and SCADA system with field devices to describe typical IACS environment. Some trade-offs and assumptions were taken into account in this testing model.

***3.3.2 IACS Abnormal Events.*** There is a technical challenge in understanding the abnormal events that can be caused by an adversary in a PCSs [3]. IACS are vulnerable to the same kind of attacks experienced in a standard IT environment, but have the added vulnerability of attacks that are unique to IACS.

***3.3.3 Detecting IACS Abnormal Events.*** Another challenge is in understanding how to detect the abnormal events that can be caused by an adversary in a PCSs [3]. Standard information technology defenses can detect and defend against the same types of attacks in PCSs.

## 3.4 Implementing Defense and Detection in-Depth

The next technical challenge is to identify the layers that need to be instrumented to achieve a defensive in-depth detection [3]. The following layers were identified:

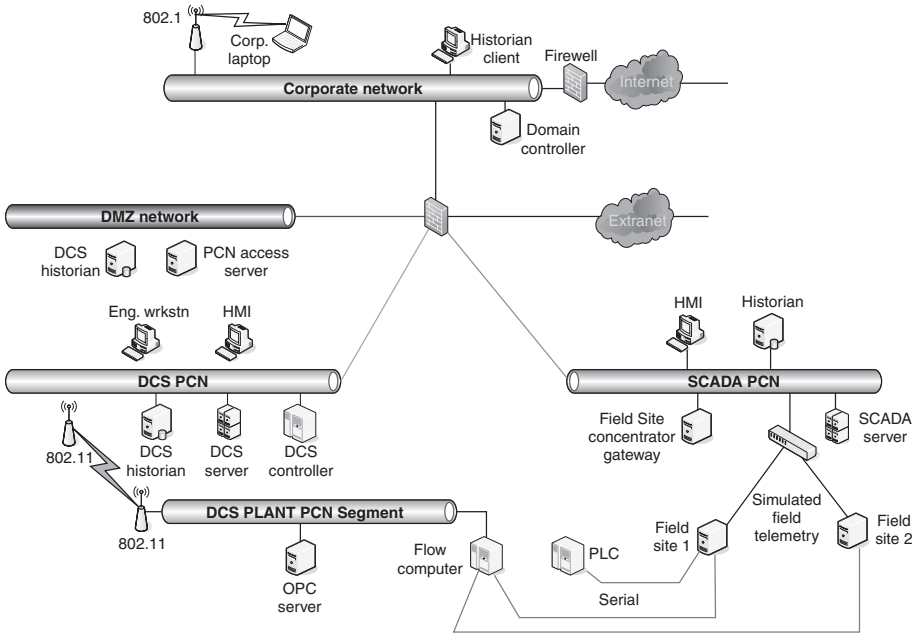



**FIGURE 3** LOGIIC-1 Baseline O&G lab environment (courtesy of DHS LOGIIC brochure).

- Network Boundary
- Host Network Connection
- Host Operating System
- Process Control Application.

The final challenge is to show that IT network devices (e.g. IDSs) can be used with IACS, as well as with their field devices such as flow computers or PLCs. Security alerts from the devices must be able to be correlated to provide the proper intrusion detection in a realistic control system environment.

### 3.5 Test Bed Operating Model

The LOGIIC-1 test bed included four individual networks: a Corporate Network, a DMZ Network, a DCS Network, and a SCADA Network. The test environment includes both a SCADA application typically used to manage pipelines as well as a DCS application used to run refineries. These applications reside on process control networks (PCNs) with other IACS-specific equipment.

The standard IT defenses selected as event sources include the following:

- Network segment firewalls (in reporting, not blocking modes);
- Host firewalls (again, in reporting, not blocking modes);
- Network IDSs;
- Network devices (wired and wireless routers).

Three sources specific to control systems are

- PCS-protocol aware IDSs on the PCNs;
- Alarms from the DCS and SCADA;
- Alarms from flow computers.

A suite of sensors was selected to implement this defense-in-depth strategy. These sensors are triggered by abnormal activity and produce security events that are collected and correlated by an Enterprise Security Management (ESM) application. It is critical to relate security events in the IT network with IACS events to provide situational awareness. This allows IACS operators to identify threats that would previously go unnoticed. These threats can now be mitigated before potentially serious process disruptions occur.

Three sets of correlation rules were developed to enable this awareness:

1. Rules that identify steps of the critical attack scenarios (e.g. moving from network segment to another).
2. Rules that implement common IACS policies. IACS is quite static compared to business/corporate networks, so violation alerts can include rogue systems, IACS configuration changes, and port scans.
3. Rules that apply a data dictionary for IACS-specific security events. This dictionary would map proprietary logged IACS events to standardized security events.

## 4 SUMMARY

In the LOGIIC-1 Project, the team was able to implement ESM application (correlation engine) in generic O&G DCS & SCADA systems within a laboratory environment and integrated them with a simulated business network [5]. As a result, the project

- Successfully developed, implemented, and tested four attack scenarios, which model new threats to IACS brought by standardization and interconnectivity;
- Implemented a PCS security data dictionary;
- Identified, correlated, and alerted the compromises to environment at and across all levels;
- Provided enhanced situational awareness;
- Built an in-depth solution for industry deployment.

IT-type sensors were placed to detect events on the IACS generated information, which was combined with events extracted from the control system applications. Attack pictures were created using events from both sources.

The IT types of sensors provided events generated by their standard IT signature set, as well as events generated by a Modbus signature set to detect PCS-specific attacks. The control system applications were also able to provide unique control system alarm events for correlation.

On the basis of the results, it was predicted that there would be a reduction in workload for a security analyst looking for attacks, since filtering reduced the number of events an analyst would need to examine. One of the attack scenarios used created over 7,000,000 low-level events from the system sensors, which were reduced to about 1000 correlated events and then further prioritized to only 130 high-priority alerts.

The LOGIIC-1 results have now been implemented by several companies in their real-world environment, proving that this LOGIIC collaboration/partnership works very effectively.

## 5 NEXT STEPS

The LOGIIC model was developed to have broad applicability within the O&G industry as well as other IACS-dependent industries and government, and the synergy from such a private–public partnership results in higher quality results, reduced R&D, and lower costs. Addressing IACS cyber security risks within any critical infrastructure environment is a shared problem and needs to be addressed through a collaborative effort. The LOGIIC model has proven to be a vehicle that provide the necessary collaborative results.

In addition to the LOGIIC model, industries can improve PCSs security by supporting other industry collaboration such as the following:

- ISA-99 Committee that establishes standards, recommended practices, technical reports, and related information that will define procedures for implementing electronically secure manufacturing and control systems and security practices and assessing electronic security performance. The Committee's focus is to improve

the confidentiality, integrity, and availability of components or systems used for manufacturing or control, and to provide criteria for procuring and implementing secure control systems. Compliance with the Committee's guidance will improve manufacturing and control system electronic security, and will help identify vulnerabilities and address them, thereby reducing the risk of compromising confidential information or causing manufacturing control systems degradation or failure [7].

- ISCI, which is an industry consortium that facilitates an efficient forum of asset owners and suppliers for proposing, reviewing, and approving security conformance requirements for products in the automation controls industry. The resulting requirements form the basis for the *ISASecure*™ compliance designation, enabling suppliers to develop secure automation control products based on industry consensus security standards (security compliance "out of the box"). The *ISASecure*™ designation creates instant recognition of automation control products and systems that comply with *ISASecure*™ technical specifications. As a result, asset owners are able to efficiently procure and deploy *ISASecure*™ products with well-known security characteristics that are in conformance with industry consensus security standards such as ISA99. [8]
- Other security collaboration/partnerships such as API and NPRA.

## 6 CONCLUSION

The Event Correlation research conducted by the LOGIIC program addresses the need for coordination at many levels if our nation's critical PCSs are going to be secure. At the technology level, security data from many disparate sources must be collected and analyzed as an integrated resource. Otherwise, a potential avalanche of events can result in valuable security information being overlooked or misinterpreted, increasing the probability of a successful attack.

At the same time, coordination at the organizational and national level is also critical. Without it, each company would be forced to proceed on its own, achieving far less in the end. Instead, the synergy generated by the private–public partnership in LOGIIC resulted in a security project with higher quality results, reduced research time, and lower costs. We believe it stands as a model for industry and government cooperation in critical infrastructure security going forward.

## ACKNOWLEDGMENTS

We would like to thank:

- Chevron Corporation, for supporting cyber security activities such as LOGIIC, ISCI, and ISA-99 in the O&G industry, and also for assistance in publishing this article.
- The members of LOGIIC-1(Correlation Project) for their participation in the project and their significant contributions to the solution (http://www.cyber.st.dhs.gov/logiic.html).

- Ulf Lindqvist, Dale Peterson, Thomas Culling, Eric J. Byres, and Linda Shaltz for their special contributions to the completion of this paper.
- The Department of Homeland Security for providing valuable information via the LOGIIC website http://www.cyber.st.dhs.gov/docs/LOGIICbrochure.pdf.

## REFERENCES

1. ANSI/ISA-99.00.01-2007 (2007). *Security for Industrial Automation and Control Systems, Part1: Terminology, Concepts, and Models*. p. 24, used with permission, ISA, www.isa.org.
2. GAO (2004). *Challenges and Efforts to Secure Control Systems* March, 2004.
3. LOGIIC-1 Team (2005). *Project Framing Document for DHS LOGIIC Project*, July, 2005.
4. ISA Security Compliance Institute (2007). *Membership Prospectus*, June, 2007.
5. Aubuchon, T. (2006). The LOGIIC correlation project. *Presented at DHS LOGIIC Cyber Security Project Conference*, Houston, September 11, 2006.
6. Ulf Lindqvist (1999). *On the Fundamentals of Analysis and Detection of Computer Misuse*. PhD Thesis, School of Electrical and Computer Engineering, Chalmers University of Technology,Göteborg, Sweden Copyright 1999 by Ulf Lindqvist, figure reprinted with permission.
7. ISA99 Purpose (1995-2007). *ISA Website*, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821, used with permission, ISA, www.isa.org.
8. ISA Insights (2008). *The ISA Security Compliance Institute, 2008 Edition, used with permission—ISA Security Compliance Institutee*.

## FURTHER READING

ANSI/ISA-TR99.00.02-2004 (2004). *Integrating Electronic Security into the Manufacturing and Control Systems Environment*.

ANSI/ISA-TR99.00.01-2007, (2007). *Security Technologies for Industrial Automation and Control Systems*.

Byres E.J., Leversage D, and Kube N. (2007). Security incidents and trends in SCADA and process industries. *Industrial Ethernet Book issue* **39**: 2.

Byres E.J. and Lowe J.. (2004). The myths and facts behind cyber security risks for industrial control systems, *VDE 2004 Congress*, VDE, Berlin, October.

http://www.us-cert.gov/control_systems/csdocuments.html#docs.

Kuipers D. and Fabro Mark. *Control Systems Cyber Security Defense-in-Depth Strategies*. (2006). Idaho National Lab, Idaho State.

NIST SP-800-53, Revision 2, NIST Recommended Security Controls for Federal Information Systems. http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf, 2007.

Permann M., Hammer J., Lee K., and Rohde K.. (2006). *"Mitigations for Security Vulnerabilities Found in Control System Networks"*, ISA.

Securing your SCADA and Industrial Control System, (2005). *U.S. DHS, ISBN 0-16-075115-2*.

*Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments version 1.0, Recommended Practice*, February (2007).

US-CERT Informational Focus Paper, *Control Systems Cyber Security Awareness*, United States Computer Emergency Readiness Team, July.

# CYBER SECURITY FOR THE BANKING AND FINANCE SECTOR

VALERIE ABEND AND BRIAN PERETTI
*Department of Treasury, Washington, D.C.*

C. WARREN AXELROD
*Bank of America, Charlotte, North Carolina*

ANDREW BACH
*NYSE Euronext, New York, New York*

KEVIN BARRY, DON DONAHUE, AND KEN WRIGHT
*Depository Trust and Clearing Corporation, New York, New York*

JOHN CARLSON
*BITS, Washington, D.C.*

FRANK CASTELLUCCIO, DAN DEWAAL, DAVID ENGALDO, AND GEORGE HENDER
*Options Clearing Corporation, Chicago, Ilinois*

DAVID LAFALCE
*The Clearing House, New York, New York*

MARK MERKOW
*American Express Company, New York, New York*

WILLIAM NELSON
*FS-ISAC, Dulles, Virginia*

JOHN PANCHERY
*Securities Industry Financial Market Association, New York, New York*

DAN SCHUTZER
*Financial Services Technology Consortium, New York, New York*

DAVID SOLO
*Corporate Technology Office, Citigroup Inc., New York, New York*

JENNIFER L. BAYUK
*Consultant, Towaco, New Jersey*

## 1 HISTORY OF COOPERATION

The US government and financial institutions have a long history of cooperation. The government recognized financial institutions as an integral part of the nation's critical

infrastructure. As such, financial institutions are highly regulated and constantly supervised by regulatory agencies to ensure that they are able to withstand the various and increasing threats they face.

Examples of cooperation between the public and private sector in the late 1990s include preparations for the Century Date Change or "Y2K", *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* (July 1998) by the President's Commission on Critical Infrastructure Protection (PCCIP) and the Critical Infrastructure Assurance Office (CIAO),[1] and Presidential Decision Directive (PDD) 63 on Critical Infrastructure Protection (CIP, May 1998). PDD 63 established the first governmental approach to protecting the nation's critical infrastructures, assigning responsibility for protecting infrastructures in different economic segments to different governmental agencies, provided each responsible agency would appoint a private sector "Sector Coordinator" to work with the agency to pursue infrastructure protection in the sector, and encouraging the sharing of infrastructure protection information between government and private industry through the formation of information sharing and analysis centers (ISACs). It also supported research and development, outreach, and vulnerability assessment. PDD 63 described "A National Goal" as follows:

> "No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from today [i.e. by May 22, 2003] *the United States shall have achieved and shall maintain the ability to protect the nation's critical infrastructures form intentional acts that would significantly diminish the abilities of*
>
> - the Federal Government to perform essential national security missions and to ensure the general public health and safety;
> - state and local governments to maintain order and to deliver minimal essential public services;
> - *the private sector to ensure the orderly functioning of the economy and the delivery of essential* telecommunications, energy, *financial* and transportation *services*." [emphasis added]

Under PDD 63, the Department of the Treasury ("Treasury") was assigned the responsibility for the banking and finance sector, and appointed Steve Katz, then Chief Information Security Officer for Citibank, as the first private sector "Sector Coordinator".

In the following years, the US Congress focused on cyber security issues as it related to privacy protection. Two significant laws governing privacy and security protections were enacted in the 1990s, the Health Insurance Portability and Accountability Act of (1996) also known as (HIPPA) and the Financial Services Modernization Act of 1999,[2] also known as the Gramm–Leach–Bliley Act (GLBA) (1999).

HIPAA[3] was enacted to restrict control of and access to patients' information and GLBA includes a provision requiring financial institutions to safeguard personal information. In 2001, regulators finalized regulations requiring financial institutions

[1]The *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures* is available at http://cipp.gmu.edu/archive/190_PCCIPCIAORandDRoadmap_0798.pdf Other pertinent documents can be found in the CIP Digital Archive in the George Mason University School of Law Critical Infrastructure Protection Program website at http://cipp.gmu.edu/clib/CIPDigitalArchive.php.

[2]Public Law No. 106–102.

[3]Public Law 104–191, 42 U.S.C. 1301 et seq.

to establish appropriate safeguards for the use, disclosure, privacy, and security of personal information, including Social Security Numbers (SSNs). The regulators applied strong enforcement tools to ensure that financial institutions complied with these security requirements. In addition, the Federal Financial Institutions Examination Council (FFIEC),[4] issued several Information Technology booklets on topics including information security, business continuity planning (BCP), and outsourcing.[5]

In January 2000, the Clinton Administration released *Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue*. This report urged the creation of public private partnerships to address cyber security issues

Shortly after the 9/11 attacks of September 11, 2001, the government and financial services industry responded. Executive Order (EO) 13228[6] *Establishing the Office of Homeland Security (HLS) and the Homeland Security Council* created the present structure for the protection of the homeland and EO 13231[7] *Critical Infrastructure Protection in the Information Age*, outlined, *inter alia*, the public partnerships context for the protection of the critical infrastructure. Private sector advisory councils were formed, including the Homeland Security Advisory Council(HSAC) (EO 13228) and the National Infrastructure Advisory Council (NIAC) (EO 13231). The Office of HLS, first headed by former Pennsylvania Governor Thomas Ridge, was formed. In addition, the President's Critical Infrastructure Protection Board (PCIPB), based on the Clinton administration's *Defending America's Cyberspace* plan, was established. The PCIPB coordinated an effort to draft a national infrastructure protection strategy that included contributions from both public and private participants. All participants were asked to comment on how this effort should evolve. In particular, the goal was to avoid legislation and regulation by means of proactive collaborative measures. Each of the critical sectors was directed to publish its own strategy.[8]

Several financial services industry organizations supported these efforts, including the Securities Industry Association (formerly SIA, now Securities Industry and Financial Markets Association [SIFMA]), BITS (the Financial Services Roundtable's technology and operations division), and the Financial Services Information Sharing and Analysis Center (FS-ISAC). This support was intended to foster closer working relationships between government and the finance sector.

The US financial regulators and the US Treasury Department were also looking at these issues. Following a series of organizational meetings in 2001, the US Treasury and financial regulators developed a process to coordinate the activities of federal and state financial services regulators by establishing the Financial and Banking Information Infrastructure Committee (FBIIC).[9]

The FBIIC, originally a standing committee of the PCIPB, but currently chartered under the President's Working Group on Financial Markets, is charged with improving coordination and communication among financial regulators, enhancing the resiliency of

[4]An interagency body with representation from the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and Office of Thrift Supervision (OTS).

[5]These Booklets are available at www.ffiec.gov/guides.htm.

[6]http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr10oc01-144.pdf.

[7]http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=fr18oc01-139.pdf.

[8]The entire list of sector plans, as well as copies of the plans, are available at the website of the Partnership for Critical Infrastructure Security (PCIS) at www.pcis.org.

[9]Membership information can be found at www.fbiic.gov.

the financial sector, and promoting the public–private partnership. Treasury's Assistant Secretary for Financial Institutions chairs the committee.

In fulfilling its mission, the FBIIC set out to:

- identify critical infrastructure assets, their locations, potential vulnerabilities, and prioritize their importance to the financial system of the US;
- establish secure communications capability among the financial regulators and protocols for communicating during an emergency; and
- ensure sufficient staff at each member agency with appropriate security clearances to handle classified information and to coordinate in the event of an emergency.

Working with appropriate members of financial institution regulatory agencies, the FBIIC has accomplished the following:

- provided key federal and state financial regulators with secure telecommunications equipment for use in a crisis, and we adding a capacity for encrypted e-mail;
- written emergency communications procedures allowing communication between financial regulators and Federal, state, and local stakeholders;
- worked to systematically identify critical financial infrastructures, assess vulnerabilities within the critical financial infrastructure, address vulnerabilities, and evaluate progress; and
- identified the infrastructure that is critical to the retail payments system, the insurance industry, and the housing finance industry.

On May 10, 2002, key leaders from the financial services industry, with the encouragement of the Treasury, established the Financial Services Sector Coordinating Council (FSSCC).[10] Rhonda MacLean, then Chief Information Security Officer at Bank of America Corporation, was appointed the second Sector Coordinator for Financial Services by Treasury, and served as the founding Chairman of the FSSCC. The banking and finance sector published its first version of the sector's critical infrastructure protection plan in May 2002. The "National Strategy for Critical Infrastructure Protection" was jointly drafted by several associations including BITS, SIA, FS-ISAC, AbA, and in consultation with the financial regulators.[11]

Members of the FSSCC and FBIIC meet three times a year for discussions and briefings.

On September 18, 2002, the Bush administration released a draft of *The National Strategy to Secure Cyberspace*. The *National Strategy* outlined the "preferred" means of interaction between the public and private sectors. After incorporating comments, the Bush administration released the final *National Strategy to Secure Cyberspace* in February 2003.[12] On March 1, 2003, the Department of Homeland Security (DHS) was formally established and many of the responsibilities of the PCIPB were transferred to DHS.

[10]Details about the FSSCC and its activities can be found at the FSSCC website at www.fsscc.org.

[11]A 2004 update of this strategy and other publications about the FSSCC's activities can be found at the FSSCC website.

[12]*The National Strategy to Secure Cyberspace*, The White House, February 2003, is available at www.whitehouse.gov/pcipb/cyberspace_strategy.pdf. This document implements a component of *The National Strategy for Homeland Security* and is complemented by *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which are available at www.whitehouse.gov/pcipb/physical_strategy.pdf.

In September 2002, several regulatory agencies released a draft paper outlining more stringent BCP requirements for certain types of large financial institutions. The *Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the US Financial System* was released for public comment by the Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Securities and Exchange Commission(SEC), and the New York State Banking Department. Several financial institutions and associations submitted detailed comment letters on the proposal and objected to several onerous proposed requirements. In April 2003, three of the original agencies (the FRB, OCC, and SEC) released the final *Sound Practices White Paper* after considering 90 comment letters from industry participants.[13] The revised final paper did not insist on a minimum distance between primary and backup sites (e.g., 300 mile mission distance between primary and backup sites). However, it does require that institutions have staff, located outside their primary sites, which can conduct business if those at the primary site cannot get to the backup facilities. This became a good precedent for how meaningful, respectful discussion can lead to a proposal that meets requirements but is not overly burdensome on industry members.

In 2003, the President released the *National Strategy to Secure Cyberspace* and *National Strategy for Physical Protection of Critical Infrastructures and Key Assets*. These documents called for Treasury, as the lead agency for the banking and finance sector, to develop a research and development agenda for the sector. Treasury, working with the FBIIC and the FSSCC, published an agenda for the sector entitled "Closing the Gap". The driving force behind the document was a desire to identify key areas where additional research dollars could be spent to make the sector more secure. This document was socialized among Federal departments and agencies, academics, and financial services participants.

On March 7 and 8, 2005, Treasury, in conjunction with the National Science Foundation (NSF), hosted a workshop entitled "Resilient Financial Information Systems". Participants from academia and the public and private sectors worked to discuss and identify research priorities to advance the resilience of the financial sector and protect the nation's critical financial infrastructure. As the issue of research and development (R&D) for the financial services sector matured, the FSSCC developed a working group to focus specifically on the issue for R&D and to coordinate its activities with respect to critical infrastructure and key resources (CI/KR) R&D. At Treasury's request, the FSSCC joined DHS in a May 2005 workshop focused on R&D priorities.

DHS published an updated version of the National Infrastructure Protection Plan (NIPP) in 2005. The role of the sector-specific agencies in coordinating the activities of the sector was again reaffirmed in the document. As DHS was finalizing the NIPP R&D plans and programs, the FSSCC formed an R&D Committee to focus on those plans and programs that would provide the most significant benefits with respect to the specific CI/KR requirements of the financial services industry. In May 2006, this committee issued a list of priority research projects. The FSSCC Research and Development Committee Research Challenges and the FSSCC Research and Development Research Agenda were issued to assist researchers in focussing research on top concerns.[14] In February 2008, the FSSCC R&D Committee began to "beta test" the Subject Matter Advisory Response Team (SMART) program. The SMART program assists research

[13]The Interagency Paper is available at www.sec.gov/news/studies/34-47638.htm.
[14]Both of these documents are available at www.fsscc.org.

and development organizations working on Critical Infrastructure Protection Projects by providing subject matter expertise for financial institutions necessary to facilitate their R&D endeavors.

## 2 ORGANIZATIONAL ROLES

### 2.1 FSSCC

The Financial Services Sector Coordinating Council (FSSCC) for critical infrastructure protection and homeland security (CIP/HLS) is a group of more than 30 private sector firms and financial trade associations that works to help reinforce the financial services sector's resilience against terrorist attacks and other threats to the nation's financial infrastructure. Formed in 2002, FSSCC works with Treasury, which has direct responsibility for infrastructure protection and HLS efforts for the financial services sector.

The mission of the FSSCC is to foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve CIP/HLS. Its objectives are to:

- provide broad industry representation for CIP/HLS and related matters for the financial services sector and for voluntary sector-wide partnership efforts;
- foster and promote coordination and cooperation among participating sector constituencies on CIP/HLS related activities and initiatives;
- identify voluntary efforts where improvements in coordination can foster sector preparedness for CIP/HLS;
- establish and promote broad sector activities and initiatives that improve CIP/HLS;
- identify barriers and recommend initiatives to improve sector-wide voluntary CIP/HLS information and knowledge sharing and the timely dissemination processes for critical information sharing among all sector constituencies; and
- improve sector awareness of CIP/HLS issues, available information, sector activities/initiatives, and opportunities for improved coordination.

As described above, the FSSCC is the private side of the public–private partnership which supports the National Infrastructure Protection Plan (NIPP). The other organizations listed in this section are all members of the FSSCC. Each organization has strengths in different areas, allowing the FSSCC to coordinate efforts of various members in support of overall infrastructure protection goals. Since the FSSCC was established, it has been chaired by distinguished and prominent members of the financial community Rhonda MacLean of Bank of America from 2002–2004, Donald Donahue of The Depository Trust and Clearing Corporation from 2004 through 2006 and George S. Hender of The Options Clearing Corporation from 2006 to 2008, and Shawn Johnson of State Street Global Advisors in 2008.

### 2.2 FSSCC Member Organizations

All FSSCC member organizations have contributed to industry goals for CIP. The organizations described below have provided the most direct focus on collaboration with respect to cyber security issues in the Banking and Finance Sector.

***2.2.1 BITS.*** In 1996, members of Bankers Roundtable (now The Financial Services Roundtable) created BITS in order to respond to significant technological changes facing the banking industry. BITS initially focused on changes in electronic commerce and the payments system, but evolved over time to focus on new threats that emerged in the areas of Internet security, fraud reduction, and CIP. Before 9/11, BITS helped to create the FS-ISAC. After 9/11, BITS helped to create the FSSCC and ChicagoFIRST.[15]

In 2001, BITS established the BITS Crisis Management Coordination Working Group (CMC-WG). This working group implemented The BITS and Financial Services Roundtable Crisis Communicator, a high-speed communications programs, that allowed the organization to connect all the key players—member CEOs and government and other business leaders—who might need to convene and determine how to address a crisis. The *BITS and Financial Services Roundtable (FSR) Crisis Management Process: Members' Manual of Procedures* was developed to provide BITS' members with the ability to communicate and coordinate with each other, government agencies, and other sectors in order to implement the emergency response and recovery process for the financial services sector.

One of the greatest lessons learned from 9/11 was the extent of the financial services sector's interdependencies and reliance on other critical sectors, specifically telecommunications and power. With the help of the Board of Governors of the Federal Reserve System, notably Steve Malphrus, BITS convened a conference in New York City in July 2002. The conference focused on ways to get tangible progress from other critical infrastructure sectors toward the goal of cooperation between government and the private sector.

One tool that resulted from the BITS Telecommunications Working Group efforts is the *BITS Guide to Business—Critical Telecommunications Services*. Completed in 2004[16], the Guide is based on extensive work by BITS members, participation by major telecommunications companies, and involvement by the National Communications System (NCS) and the President's National Security Telecommunications Advisory Council (NSTAC). The Guide is a comprehensive tool used by BITS' member institutions to better understand the risks of telecommunications interdependencies and achieve greater resiliency.

***2.2.2 ChicagoFIRST.*** Another clear lesson from 9/11 was the stunning impact an event could have on critical financial services operations that are heavily located in one regional area. Louis Rosenthal, ABN AMRO, and Ro Kumar, The Options Clearing Corporation, saw the potential risks in the Chicago area and energized their peers and a set of partners. BITS facilitated the process of forming the regional coalition. In 2003–04 the US Treasury Department founded an evaluation and guide for establishing regional coalition through the Boston Consulting Group and BITS. ChicagoFIRST, the result of these efforts, is a free-standing nonprofit organization that provides robust coordination services to maintain the resilience of the critical financial services that reside in the area. It continues to serve as a model for others, including FloridaFIRST and other regional coalitions.[17]

[15]ChicagoFIRST is a nonprofit association dedicated to addressing HLS and emergency management issues affecting financial institutions and requiring a coordinated response.

[16]The BITS Telecommunications Working Group, led by John DiNuzzo (formerly of FleetBoston/Bank of America Corporation) was a subgroup of the BITS CMC-WG.

[17]Improving Business Continuity in the Financial Services Sector: A Model for Starting Regional Coalitions (US Treasury: November, 2004). http://www.treas.gov/press/releases/reports/chicagofirst_handbook.pdf

***2.2.3 Financial Services Information Sharing and Analysis Center (FS-ISAC).*** The FS-ISAC was conceived at a meeting of Financial Industry leaders with the Treasury at the White House Conference Center in March 1999. An Information Sharing Working Group was established. The financial services industry members participating in the original Information Sharing Working Group appointed a Board of Managers, who formed FS-ISAC limited liability corporation (LLC). It was officially launched by US Treasury Secretary Lawrence A. Summers at a ceremony in the Treasury building on October 1, 1999, as a means of meeting the finance sector's information-sharing obligation under PDD 63 on CIP.

On December 9, 2003, the Treasury announced that it would purchase $2 million in services from the FS-ISAC. Treasury's contract with the FS-ISAC resulted in a new, next-generation FS-ISAC that is intended to benefit the Treasury, other financial regulators, and the private sector. In the press release, the Treasury indicated the purposes for the funding were as follows[18]

- Transform the FS-ISAC from a technology platform that serves approximately 80 financial institutions to one that serves the entire 30,000 institution financial sector, including banks, credit unions, securities firms, insurance companies, commodity futures merchants, exchanges, and others.
- Provide a secure, confidential forum for financial institutions to share information among each other as they respond in real time to particular threats.
- Add information about physical threats to the cyber threat information that the FS-ISAC currently disseminates.
- Include an advance notification service that will notify member financial institutions of threats. The primary means of notification will be by Internet. If, however, Internet traffic is disrupted, the notification will be by other means, including telephone calls and faxes.
- Include over 16 quantitative measures of the FS-ISAC's effectiveness that will enable the leadership of the FS-ISAC and Treasury to assess both the FS-ISAC's performance and the aggregate state of information sharing within the industry in response to particular threats.

The FS-ISAC was able to arrange with a managed security service provider to fund the initial development and implementation of the FS-ISAC systems and networks in return for the right to reuse the technology developed. The FS-ISAC thus succeeded in meeting its original goal of becoming a viable means for the banking and finance sector to share information about security threats, vulnerabilities, incidents, and remedies. E-mail alerts and notifications sent by the FS-ISAC give financial firms advanced notice of threats, vulnerabilities, and events so that they can proactively protect themselves. The FS-ISAC also hosts an information-sharing website, conference calls, and conferences that allow its members more interactive sharing opportunities.

In 2006, the FS-ISAC established a Survey Review Committee to provide oversight of the process of member-submitted surveys of the FS-ISAC membership. The FS-ISAC survey process allows for one live poll at a time to ensure maximum participation. The primary contact at each member organization is asked to complete each survey or route it to the appropriate area within their company to have it answered by the

[18]http://www.ustreas.gov/press/releases/reports/factsheet_js1048.pdf.

most qualified individual. Surveys conducted in 2007 included *Employee Access to HR Information*, *Data Transfer Methods*, and *Information Security Program Organization*. Once the survey is completed, a Poll Results Report is created that includes a brief summary and the final poll results. Using the survey tool link provided, members can also conduct their own detailed analysis of survey results to meet their unique needs.

Through the personal involvement of members of the FS-ISAC's Board of Managers and the FS-ISAC membership at large, the reach of the FS-ISAC members[19] quickly spread well beyond the original mandate. Early on, board members were involved in efforts such as

- participating, through the FSSCC, in drafting the finance sector's segment of Version 2.0 of the NIPP;
- assisting in, and being supportive of, the establishment of the BITS laboratory for testing and certifying security software relevant to financial services institutions;
- working with Treasury to develop an outreach and education program to increase awareness of sector security threats, vulnerabilities, and best practices, and to indicate how the FS-ISAC might assist them in these areas;
- briefing Federal agencies as to the workings of the FS-ISAC; and
- testifying before congressional committees and otherwise representing the views of the banking and finance sector on cyber security and CIP.

The FS-ISAC has been a model for a number of other ISACs in critical US sectors, such as transportation, energy and information technology, as well as ISACs in foreign countries (e.g. Canada) and in individual corporate organizations (e.g. the Worldwide ISAC). Its October 2007 biannual conference was recently coordinated in conjunction with the CIP Congress, carrying the theme "When Failure is Not an Option" and was accordingly attended by members of other ISACs.

***2.2.4 FSTC.*** The Financial Services Technology Consortium (FSTC) was established in 1993 at the dawn of the commercialization of the Internet. FSTC is a nonprofit organization with members from the financial services industry (financial services providers and vendors), government agencies, and academia, who collaborate on projects to explore and solve strategic business–technology issues through concept validation, prototype and piloting, and development of standards. Its mission is to harness technology advances and innovative thinking to help solve the problems of the financial services industry.

Early projects dealt with paper check imaging, the convergence of the payments products, and securing electronic banking, commerce, and payments over the Internet. These projects helped spur the growth of electronic commerce and paved the way for Check 21 and the electronification of the paper check through the development of important new standards and industry utilities and collaborations.

After September 11, FSTC's focus expanded to include addressing business continuity issues in addition to security, fraud management, and payments, leading to a partnership with Carnegie Mellon that developed a Resiliency Framework. FSTC also initiated a focus on enterprise architecture aimed at helping financial services firms to streamline and consolidate their siloed systems and processes, enabling the reduction of redundant

[19]The Board of Managers and members of the FS-ISAC are not restricted from other industry activities beyond the work of the FS-ISAC.

processes and systems, to provide a more efficient and flexible organization, able to more rapidly and easily accommodate new products, services, and processes needed to meet new business opportunities and threats.

FSTC thrives when the knowledge of members comes together through the formation of initiatives and projects that will better the industry as a whole. FSTC projects are its core activity and one of the key benefits of FSTC membership.

***2.2.5 SIFMA.*** SIFMA provides a forum for securities firms, exchanges, industry utilities, and regulators to share knowledge, plans, and information. It is responsible for developing and promoting industry-specific practice guidelines, for providing liaison between the securities industry and regulators and legislators, and for coordinating industry-wide initiatives. SIFMA has standing committees to coordinate industry-wide initiatives for various types of securities industry trading and operations activities.

The SIFMA BCP Committee was established as the SIA BCP in November 2001 to address and coordinate business continuity issues for the securities industry. In conjunction with the BCP Committee mission, SIFMA (and its predecessors, the SIA and the Bond Markets Association) has led an extensive on-going industry-wide business continuity testing initiative since 2002. The effort allows the industry as a whole to verify and demonstrate the resilience of the securities markets and to provide individual firms with opportunities to test their procedures with other industry participants in a way they could not do on their own. Industry tests include tabletop exercises, connectivity tests, communications tests, participation in national disaster recovery tests, and pandemic flu exercises. SIFMA in conjunction with the BCP Committee operates the Securities Industry Emergency Command Center that functions as the industry's central point of emergency communications and coordination during significant emergencies.

Initial testing efforts in 2002, 2003, and 2004 involved basic connectivity tests between individual firms and exchanges. Much more robust business continuity tests were conducted in 2005 and 2006. Over 250 firms, exchanges and industry utilities participated in these tests, which involved transmission of dummy transactions from firms' and exchanges' backup sites using backup communications links. The industry demonstrated a 95% pass rate on these tests. SIFMA also coordinates securities industry participation in the national TopOff emergency exercises and focuses heavily on planning for a potential flu pandemic and on conducting pandemic planning exercises.

SIFMA's Information Security Subcommittee, which was established in 2003, addresses and coordinates information security issues from an industry perspective and facilitates information sharing among SIFMA member firms. The Subcommittee provides comments to regulatory authorities on proposed information security rules and regulations and develops industry initiatives. The Subcommittee has focused on a variety of issues including developing guidance on the design and testing of Sarbanes Oxley controls, working with legislators on proposed Security Breach Legislation, tracking and assessing Microsoft security releases, and establishing guidance on effective means of dealing with phishing attempts.

In 2007, SIFMA formed the Information Risk Advisory Council to provide advice to SIFMA's Technology, Information Security, BCP, and Privacy Committees. The Council identifies issues of significant importance to securities firms and works with SIFMA Committee to integrate these into the committees' annual goals.

## 3 SAMPLE SIGNIFICANT EVENTS

Although cyber security-related events are a daily occurrence in the financial industry, some events are more significant than the others with respect to collaborative information sharing. The events listed below were significant in that the collaboration that occurred during the event served to strengthen the bonds of communication between public and private sector CIP organizations.

### 3.1 Russian Hacker Case

In June 1994, a Russian crime ring managed to get inside the Citibank computer system and transfer $140,000 from the Philippine National Bank to a bank in Finland. The bank in the Philippines called to complain that the transaction had not been authorized. Citibank realized something was amiss and set up a special team to start looking into transactions of similar circumstance. However, it was not given that the unauthorized transfer was the first discovery of a chain of illegal activity. By the middle of July, the team identified a similar transfer had taken place and yet a third by the end of the month. By this time, Citibank had called in the Federal Bureau of Investigation (FBI) and the investigation was in full swing. Transactions were being illegally transferred from cities as far away as Djakarta and Buenos Aires to banks in San Francisco and Israel. In total, fraudulent transactions amounted to more than $3 million; though in the end, the gang of thieves managed to abscond with only $400,000.

The system breached was called the Citibank Cash Management system. This system allowed corporate customers to transfer money automatically from their accounts to whoever they are paying. And it handled approximately 100,000 transactions a day, totaling $500 billion. The Citibank system relied on static passwords, which they intend for users to memorize. The passwords remain the same each time a user enters the system, and although they are encrypted, the crime ring was somehow able to get a password and identification numbers of some of these corporate customers. The investigation team realized that the passwords traversed through many network links that were not necessarily fully owned and operated by the bank, but many were leased from telecommunication companies in various countries which provided the bank with network links between its offices. The question the investigators faced was did the perpetrator have an insider in Citibank or was he able to get them using conventional "network-sniffing" software.

On August 5, a fraudster transferred $218,000 from a Citibank account in Djakarta and another $304,000 from a bank in Argentina to Bank of America accounts in San Francisco that had been set up by a Russian couple. They would go to the bank after the money was transferred and attempt to withdraw it. At that point, investigators identified the perpetrators. They were kept under observation by both the public and private sector through October, transferring money from and to more accounts.

The idea of computer control of funds was new to the media at that time. It was a new idea to reporters that a person could be sitting at a computer in Russia in the middle of the night keying in passwords and watching money move across a screen. The Internet was still young at the time and largely unused commercially. The transfers were done through a proprietary network managed by Citibank. But, like the Internet, these proprietary networks cross over other proprietary networks and it is at these points that

passwords become most vulnerable. Yet cooperation between the bank investigators, telecommunications administrators, and law enforcement led eventually to Vladimir Levin, a young Russian hacker. He was trapped through a traced telecommunications line performing a fraudulent transaction and was imprisoned. In the course of the investigation, several people were arrested (including half a dozen Russian citizens, for which this story is known as the "Russian Hacker Case"). Immediately after, Citibank ended the use of static passwords over its Funds Transfer networks and started issuing One Time Password tokens to customers using those networks (these tokens were a form of two factor authentication from a small company named RSA from its founders, Rivest, Shamir, and Adelman, then infrequently encountered).

### 3.2 Slammer Worm

On January 23, 2003, a structured query language (SQL) injection dubbed the "slammer worm" started to infect rapidly through computer systems throughout the world. Although a patch was released for the vulnerability, many organizations had not installed it. As a result, the worm spread very quickly, infecting, by one account, 75,000 victims within 10 min after its release.

Although financial institutions were not greatly affected by the worm, Treasury, in coordination with the FBIIC and FSSCC, convened a meeting on February 25, 2003, to discuss issues related to the worm. In addition to members of the FBIIC and FSSCC, several private sector groups attended, including Microsoft and electronic data system (EDS). At the meeting, communications protocols were developed to aid in the sharing of information in the event of another incident. The protocols were exercised during several other virus/worm attacks, including SoBig.F and BugBear.b.

### 3.3 2003 Power Outage

At approximately 4:11 pm Eastern Daylight Time (EDT) on August 14, 2003, a power outage affected a large portion of the Northeastern United States, roughly from Detroit to New York City. Although there was minimal disruption to delivery of financial services in the affected area, the incident did expose a greater need to continue to examine the backup systems institutions. For example, the American Stock Exchange had relied upon steam power to cool their trading floor. Upon reaching out to the SEC and the Treasury, a backup steam generator was located and the exchange was able to open and close on Friday, August 15, 2003.[20] Many lessons learned from that set of events. One lesson led to the *BITS Guide to Business—Critical Power*, developed in cooperation with the Critical Power Coalition and Power Management Concepts, and published in 2006. It provides financial institutions with industry business practices for understanding, evaluating, and managing the associated risks, when the predicted reliability and availability of the electrical system are disrupted—and it outlines ways by which financial institutions can enhance reliability and ensure uninterrupted backup power.

The following table, Table 1 describes a series of publications and events related to information sharing and coordination within the finance and banking sectors.

[20]The report, *Impact of the Recent Power Blackout and Hurricane Isabel on the Financial Services Sector*, can be found at http://www.treas.gov/offices/domestic-finance/financial-institution/cip.

**TABLE 1 Publications and Events**

| Date | Name of Publication/Event | Comments |
|---|---|---|
| February 1996 | CIWG (Critical Infrastructure Working Group) Report | Suggested establishing PCCIP (President's Commission on Critical Infrastructure Protection) for the longer-term view and the IPTF (Infrastructure Protection Task Force) for coordination of then existing infrastructure protection efforts. |
| July 1996 | EO (Executive Order) 13010 | Formed PCCIP, IPTF and CIAO (Critical Infrastructure Assurance Office) Available at www.fas.org/irp/offdocs/eo13010.htm |
| October 1997 | Critical Foundations: Protecting America's Infrastructures | Report issued by PCCIP suggesting a strategy incorporating research and development, information sharing, education, and awareness |
| May 1998 | PDD-63 (Presidential Decision Directive Number 63) for Critical Infrastructure Protection | By May 2003:<br>The Federal Government to perform essential national security missions and to ensure the general public health and safety<br>State and local governments to maintain order and to deliver minimum essential public services<br>The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services. |
| July 1998 | Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures | Report issued by PCCIP and CIAO as a follow-up of *Critical Foundations: Protecting America's Infrastructure*. Section 2.1 addresses the Banking and Finance sector |
| October 1999 | Official launch of the FS-ISAC (Financial Services Information Sharing and Analysis Center) | Launched by US Treasury Secretary Laurence P. Summers—available at www.fsisac.com |
| January 2000 | Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1: An Invitation to a Dialog | This report urged the creation of public private partnerships to address cyber security issues |
| January 2001 | Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities | Available at www.fas.org |

**TABLE 1 (*Continued*)**

| Date | Name of Publication/Event | Comments |
|---|---|---|
| March 2002 | Banking and Finance Sector: The National Strategy for Critical Infrastructure Protection | Available at www.pcis.org |
| May 2002 | Banking and Finance Sector National Strategy for Critical Infrastructure Assurance | Available at www.pcis.org |
| July 2002 | National Strategy for Homeland Security | Available at www.whitehouse.gov/homeland/book/nat strat hls.pdf |
| February 2003 | The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets | Available at www.whitehouse.gov/pcipb/physical.html |
| February 2003 | The National Strategy to Secure Cyberspace | Available at http://www.whitehouse.gov/pcipb/ |
| March 2003 | FFIEC IT Examination Handbook: Business Continuity Planning | Available at www.ffiec.com |
| 2003 | PCIS Industry Compendium to the National Strategy to Secure Cyberspace | Analysis of plans and summary of commonalities. Available at www.pcis.org |
| July 2003 | Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, Bank for International Settlements | Available at www.bis.org/publ/bcbs98.pdf |
| December 2003 | Homeland Security Presidential Directive (HSPD)—7 on Critical Infrastructure Identification, Prioritization, and Protection | Covers policy, roles and responsibilities of Secretary of Homeland Security, other offices, and so on, coordination with the private sector. Note: Consistent with Homeland Security Act of 2002, produce "National Plan for Critical Infrastructure and Key Resources Protection" within one year, that is, by December 2004. www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html |
| May 2004 | Homeland Security Strategy for Critical Infrastructure Protection in the Financial Services Sector: Version 2 | Objectives of Financial Services Strategy:<br>Identifying and reducing vulnerabilities in the financial services infrastructure to such attacks<br>Ensuring the resiliency of the nation's financial services infrastructure to minimize the damage and expedite the recovery from attacks that do occur, and |

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| Date | Name of Publication/Event | Comments |
|---|---|---|
| | | Promoting public trust and confidence in the financial services sector's ability to withstand and recover from attacks that do occur. Available at www.fsscc.org |
| February 2005 | National Infrastructure Protection Plan (Interim) | Superseded by June 2006 NIPP http://cipp.gmu.edu/archive/Interim NIPP Feb 05.pdf |
| 2005 | FFIEC IT Examination Handbook: Information Security | Available at www.ffiec.com |
| April 2003 | Interagency Sound Practices to Strengthen the Resilience of the US Financial System | Available at www.sec.gov/news/studies/34-47638.htm |
| April 2006 | FSSCC Research Challenges Booklet | Available at www.fsscc.org |
| June 2006 | National Infrastructure Protection Plan | Available at www.dhs.gov |
| October 2006 | FSSCC R & D Agenda | Available at www.fsscc.org |
| December 2006 | FSSCC Annual Report | FSSCC published the Banking and Finance Sector-Specific Plan as their annual report. Available at www.fsscc.org |
| May 2007 | Sector-Specific Plan: Banking and Finance Sector for Critical Infrastructure Protection | http://www.dhs.gov/xlibrary/assets/nipp-ssp-banking.pdf |
| 2005 (–2007) | Protecting the US Critical Infrastructure: 2004 (–2006) in Review | Annual reports, expected to continue, available at www.fsscc.org |

### 3.4 Pandemic Planning

In September and October 2007, SIFMA, in partnership with the FSSCC, the FBIIC, and the Treasury, conducted a multiweek pandemic flu exercise for the full financial services sector. This was the largest most ambitious financial services exercise to date that addressed business process recovery as a sector in communication with its sector-specific agency. The exercise offered a realistic simulation of the spread of a pandemic wave in the United States. It was designed to identify how a pandemic could affect the financial markets and to provide participants with an opportunity to examine their pandemic business recovery plans under a demanding scenario. Over 2700 financial services organizations participated.

### 3.5 Operation Firewall

On October 28, 2004, the US Department of Justice, in coordination with the United States Secret Service (USSS), executed over 28 search and arrest warrants in connect

with Operation Firewall,[21] an undercover investigation designed to stop the flow of stolen credit card numbers and other personal information. This operation lured criminals into a false sense of security by creating a fake website for buying and selling purloined credit card information. The main target was a group that called itself Shadowcrew, whose sole purpose was to defraud the financial services sector.

The operation, which lasted over an 18 month period, ended with the seizure of over 100 computers and the arrest of 28 individuals—21 in the United States and seven in Europe and Russia. Through the cooperation of several major financial services sector entities, the underground "carding" scene was dealt a major blow from which it is still attempting to recover.

## 4 FUTURE CHALLENGES

The examples above demonstrate high levels of collaboration among dedicated individuals representatives financial institutions, associations, and government agencies. For this collaboration to continue, it will require proactive engagement, open communications, and trust. The industry needs to cooperatively work with the respective agencies to develop rules and regulations that best meet the requirements of government while maintaining a strong finance sector and not overburdening financial institutions.

Since 9/11, government has proven its willingness to reach out and ensure the consensus of the financial community in its efforts to strengthen the infrastructure. It has also demonstrated increased trust on the part of the private side of the financial sector of government's intent and a willingness to work with the various agencies, and to persuade others that cooperation is ultimately the best approach where each side can achieve its goals.

## FURTHER READING

The FSSCC Research and Development Committee. (2006). *The FSSCC Research and Development Committee Research Challenges*, April 2006, http://www.fsscc.org.

The FSSCC Research and Development Committee. (2006). *The FSSCC Research and Development Committee Research Agenda*, October 2006, http://www.fsscc.org.

[21] http://www.secretservice.gov/press/pub2304.pdf.

# SYSTEM AND SECTOR INTERDEPENDENCIES

# SYSTEM AND SECTOR INTERDEPENDENCIES: AN OVERVIEW

JAMES P. PEERENBOOM AND RONALD E. FISHER
*Argonne National Laboratory, Argonne, Illinois*

## 1 INTRODUCTION

The importance of infrastructure interdependencies was first highlighted at the national level in 1997 when the President's Commission on Critical Infrastructure Protection (CIP) released its landmark report, *Critical Foundations: Protecting America's Infrastructures* [1]. The report pointed out that the security, economic prosperity, and social well-being of the nation depend on the reliable functioning of our increasingly complex and interdependent infrastructures.

In defining its case for action, the Commission noted that interdependency between and among our infrastructures increases the possibility that a rather minor and routine disturbance could cascade into regional or national problems. The Commission further concluded that technical complexity could also permit interdependencies and associated vulnerabilities to go unrecognized until a major failure occurs. The blackout on August 14, 2003, in which large portions of the Midwest and Northeast United States and Ontario, Canada, experienced an electric power outage, dramatically illustrated the enormously complex technical challenge that we face in preventing cascading impacts [2].

In the nearly 10 years since the release of the *Critical Foundations* report, much has been written about identifying, understanding, and analyzing infrastructure interdependencies, and significant progress has been made [3]. This progress has been the result of a number of interrelated factors, including the following:

- the emergence of a risk-based national strategy for all-hazards infrastructure protection that explicitly addresses dependencies and interdependencies;
- focused national Research and Development (R&D) efforts that address both physical and cyber infrastructures and their interdependencies in a more integrated manner;
- new analytical techniques that capture complex system response and human behavior;
- a growing awareness of interdependencies issues and increased interest by local and regional stakeholder groups who have held interdependencies-related exercises,

captured lessons learned from natural and man-made infrastructure disruptions, and been proactive in addressing interdependencies-related needs; and
- a new generation of professionals who have the requisite educational backgrounds and skill sets to address infrastructure and interdependencies.

These factors are briefly discussed in the following sections of this article and in more detail in the subsequent articles of this handbook.

## 2 CONCEPTS AND TERMINOLOGY

The release, over the past several years, of national strategy and policy documents, such as *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection* (HSPD-7), *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, *The National Strategy to Secure Cyberspace*, and the *National Infrastructure Protection Plan* (NIPP), have reshaped the definition of critical infrastructure and key resources (CIKR) in the United States [4–7]. These documents define 18 CIKR as follows: agriculture and food, water, health care and public health, emergency services, defense industrial base, energy, information technology, banking and finance, telecommunications, dams, transportation systems, chemical, postal and shipping, national monuments and icons, government facilities, commercial facilities, and commercial nuclear reactors critical manufacturing was added in 2008 as the 18th sector. Although other countries may aggregate differently (e.g. Canada identifies 10 critical infrastructures), significant similarities can be found in terms of capturing the assets, systems, and networks that, if lost or degraded to varying degrees, would have a debilitating impact on national security, public health and safety, the economy, and other dimensions of concern.

A variety of concepts and definitions can be used to describe interdependencies among the CIKR sectors [8, 9]. The NIPP defines interdependency as the "multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly" [7]. Infrastructure interdependencies are characterized in terms of four general categories:

- physical (e.g. the material output of one infrastructure is used by another);
- cyber (e.g. infrastructures utilize electronic information and control systems);
- geographic (e.g. infrastructures are co-located in a common corridor); and
- logical (e.g. infrastructures are linked through financial markets).

The proliferation of information technology, along with the widespread use of automated monitoring and control systems and increased reliance on the open marketplace for purchasing and selling infrastructure commodities and services (e.g. electric power), has intensified the prevalence and importance of cyber and logical interdependencies.

Physical, cyber, geographic, and logical infrastructure interdependencies transcend individual infrastructure sectors (by definition) and generally transcend individual public and private-sector companies. Further, they vary significantly in scale and complexity, ranging from local linkages (e.g. municipal water-supply systems and local emergency services), to regional linkages (e.g. electric power coordinating councils), to national

linkages (e.g. interstate natural gas and transportation systems), to international linkages (e.g. telecommunications and banking and finance systems). These scale and complexity differences create a variety of spatial, temporal, and system representation issues that are difficult to identify and analyze.

To facilitate analysis, infrastructure interdependencies must be viewed from a "system of systems," or holistic, perspective. Failures affecting interdependent infrastructures can be described in terms of three general categories:

- *Cascading failure.* A disruption in one infrastructure causes a disruption in a second infrastructure (e.g. the August 2003 blackout led to communications and water-supply outages, air traffic disruptions, chemical plant shutdowns, and other interdependency-related impacts).
- *Escalating failure.* A disruption in one infrastructure exacerbates an independent disruption of a second infrastructure (e.g. the time for recovery or restoration of an infrastructure increases because another infrastructure is not available).
- *Common cause failure.* A disruption of two or more infrastructures at the same time results from a common cause (e.g. Hurricane Katrina simultaneously impacted electric power, natural gas, petroleum, water supply, emergency services, telecommunications, and other infrastructures).

As an illustration of cascading and escalating failures, consider the disruption of a microwave communications network that is used for the supervisory control and data acquisition (SCADA) system in an electric power network. The lack of monitoring and control capabilities by the SCADA system could cause generating units to be taken off-line, which, in turn, could cause a loss of power at a distribution substation. This loss could lead to blackouts for the area served by the substation.

The electricity outages could affect multiple dependent infrastructures (depending on the availability of backup systems), such as transportation and water systems, commercial office buildings, schools, chemical facilities, banking and financial institutions, and many others. These disruptions could lead to delays in repair and restoration activities (i.e. an escalating failure) because of logistics, communications, business services, and other interdependency-related problems.

This simplified example reinforces the notion that understanding and analyzing cascading and escalating failures require a systems perspective and a broad set of interdisciplinary skills.

The state of operation of an infrastructure—which can range from normal operation to various levels of stress, disruption, or repair and restoration—must also be considered in examining interdependencies. Further, it is necessary to understand backup systems, other mitigation mechanisms that reduce interdependency-related problems, and the change in interdependencies as they relate to outage duration and frequency. Such considerations add complexity to the process of quantifying infrastructure interdependencies.

### 2.1 Lessons Learned

Analytical studies and real-world events have highlighted the importance of the characteristics and complexities described above. A number of lessons have been learned that have broad implications for interdependencies planning and analysis:

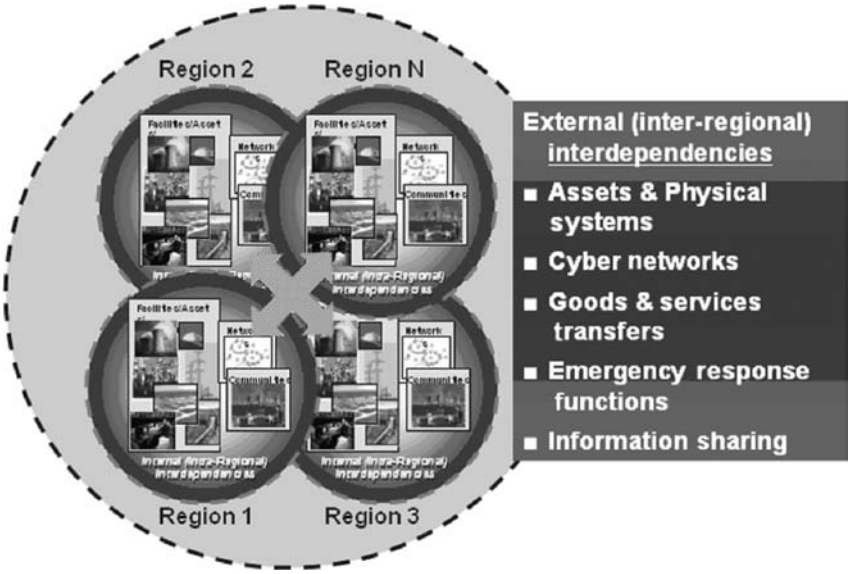



**FIGURE 1** Intra- and interregional interdependencies.

- *Interdependencies have no borders.* Infrastructure systems and supply chains transcend geographic and geopolitical boundaries, allowing disruptions to cascade in ways that are not well documented or well understood.
- *Interdependencies can be considered at multiple levels.* Different perspectives can be applied in analyzing interdependencies, ranging from an asset- or facility-level perspective to a network-, community-, region-, systems-, or CIKR sector-level perspective.
- *Intra- and interregional interdependencies are fundamental to ensuring regional resilience.* Analysts must examine interdependencies that are internal to a region (intraregional interdependencies), as well as the interconnections with other regions (interregional interdependencies), which could include backbone infrastructure systems and networks, transfers of goods and services, and shared emergency response capabilities (Fig. 1).
- *Interdependencies can influence all components of risk.* Interdependencies can act as a "risk multiplier" in that they can influence all components of risk. For example, interdependencies can (i) amplify the consequences of a disruption because of cascading and escalating impacts, (ii) expand the set of vulnerabilities because CIKR can be affected indirectly, and (iii) in the case of terrorism, change the threat (intent) through innovative targeting to specifically exploit interdependencies.
- *Interdependencies change during events.* Pre-event interdependencies, which are a function of system operations and topologies, change during an event (trans-event) depending on the specific assets affected, the use of backup systems, and the implementation of contingency plans. Post-event interdependencies may be different from pre-event interdependencies depending on how infrastructure systems are reconstituted, how supply chains are reconfigured, and how operational procedures and contingency plans are modified.

Given these considerations, key questions—from an owner/operator viewpoint—that facilitate discovery of interdependencies information and help determine the importance of interdependencies impacts include the following:

- Do you know what CIKR you depend on and who are your suppliers?
  - direct reliance on infrastructures;
  - indirect reliance through supply chains; and
  - reliance on vendors (goods and services).
- Do you know what cascading impacts might result from disruptions?
- Do you know what backup systems are in place and how long they are likely to last?
- Do you know where to get information about infrastructure restoration priorities and time lines?

### 2.2 Research and Development Needs

Consistent with the new national strategy described in the NIPP, *The National Plan for Research and Development in Support of Critical Infrastructure Protection* (NCIP R&D Plan)—prepared by the Office of Science and Technology Policy and the Department of Homeland Security (DHS) Directorate for Science and Technology—recognizes that physical and cyber infrastructures must be addressed in an integrated manner because these two areas are interdependent in all sectors, and each can disrupt or disable the other [10]. The NCIP R&D Plan represents an important shift in philosophy in that past R&D roadmaps for CIP tended to separate physical and cyber considerations.

As described more fully in later articles of this handbook, the NCIP R&D Plan notes that "critical infrastructure systems are complex, interconnected physical and cyber networks that include nodes and links with multiple components. Analysis and decision support methods help decision makers make informed choices involving these complex systems using structured, analytic approaches that incorporate controlling factors and detailed knowledge relevant to the critical infrastructure systems and their interconnectivity and reliance on one another."

Among the many R&D needs described in the Plan, decision and analysis R&D work is needed to achieve the following:

- Develop risk-informed prioritization and investment strategies to fund research, to address the most serious issues first, and to achieve the best return from the limited funding resources available.
- Develop precision vulnerability analysis tools to quantitatively predict the performance of critical infrastructure network elements if attacked, and advance these engineering tools to include new materials, innovative network design concepts, and emerging computational methods.
- Develop high-fidelity modeling and simulation capabilities to quantitatively represent the sectors and their interconnectivity and to identify realistic, science-based consequences if attacked.
- Develop integrated, multi-infrastructure advanced action and response plans for a range of threat/hazard scenarios, and "war-game" these actions and plans to anticipate problems and prepare in advance the most effective combinations and sequences of protection measures before an event occurs.

The emphasis on developing modeling and simulation capabilities and making risk-informed decisions underscores the need to (i) devise new approaches for addressing CIKR as a "system of systems" and (ii) explicitly include interdependencies considerations. Difficult issues related to spatial and temporal modeling resolution, propagation pathways for cascading disruptions, system complexity and nonlinear behavior, uncertainty, and human factors remain largely unanswered (although, as described below, progress is being made).

## 3 MODELING OF INFRASTRUCTURE INTERDEPENDENCIES

The "science" of interdependencies is still relatively new, although new modeling and simulation tools are beginning to address selected dimensions of interdependency (Fig. 2). A variety of models and computer simulations have been developed to analyze the operational aspects of individual infrastructures (e.g. load flow and stability programs for electric power networks, connectivity and hydraulic analyses for pipeline systems, traffic management models for transportation networks). In addition, simulation frameworks that allow the coupling of multiple, interdependent infrastructures are beginning to emerge.

For example, the DHS National Infrastructure Simulation and Analysis Center (NISAC)—built around a core partnership of Los Alamos National Laboratory and Sandia National Laboratories and chartered to develop advanced modeling, simulation, and analysis capabilities for the nation's CIKR—has developed tools to address physical and cyber dependencies and interdependencies in an all-hazards context [7]. Actor-based

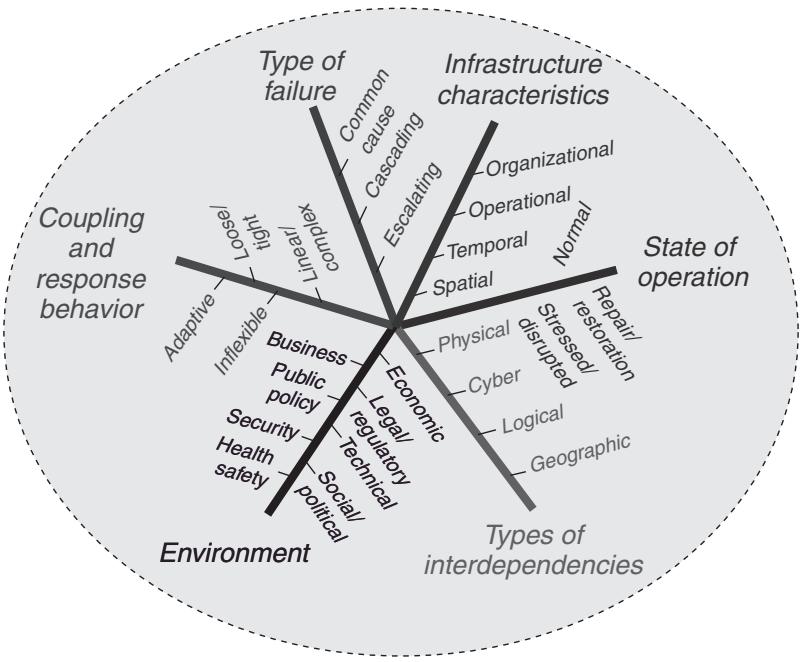



**FIGURE 2** Dimensions of interdependencies [3].

infrastructure modeling, simulation, and analysis tools, such as the Interdependent Energy Infrastructure Simulation System (IEISS), have been developed to assist individuals in analyzing and understanding interdependent energy infrastructures [11]. Dynamic systems and agent-based models also are being developed to capture economic interactions between the decision makers in infrastructure networks [12].

NISAC also has developed tools such as N-ABLE, a large-scale microeconomic simulation tool that captures the complex supply chain and market dynamics of businesses in the US economy, and the Fast Analysis Infrastructure Tool, which provides information on infrastructure assets, including their interrelationships with other infrastructure assets. Other interdependencies-related tools include the Urban Infrastructure Suite, a set of seven interoperable modules that employ advanced modeling and simulation methodologies to represent urban infrastructures and their interdependencies, as well as populations [13].

In a joint effort, Argonne, Los Alamos, and Sandia national laboratories, under the sponsorship of the DHS Science and Technology Directorate, are developing a risk-informed decision support system (DSS)—the Critical Infrastructure Protection/Decision Support System (CIP/DSS)—that provides insights for making CIP decisions by considering all CIKR sectors and their primary interdependencies [14]. CIP/DSS will assist decision makers in making informed choices by functionally representing the CIKR sectors and their interdependencies; computing human health and safety, economic, public confidence, national security, and environmental impacts; and synthesizing a methodology that is technically sound, defensible, and extendable.

CIP/DSS will address questions such as the following:

- What are the consequences of attacks on infrastructure in terms of national security, economic impact, public health, and conduct of government, including the consequences that propagate to other infrastructures?
- Are there choke points in our nation's infrastructures (i.e. areas where one or two attacks could have the largest impact)? What and where are the choke points?
- What are the highest-risk areas when consequence, vulnerability, and threat information are incorporated into an overall risk assessment?
- What investment strategies can the United States make that will have the most impact in reducing overall risk?

CIP/DSS has been applied to problems involving an agricultural pathogen that affected the food chain and involved regional transportation quarantines, as well as a telecommunications disruption that degraded the operation of other infrastructure sectors. Using CIP/DSS, analysts computed decision metrics and utility values for several investment alternatives that would mitigate the impact of the incidents.

Argonne National Laboratory has developed a series of modeling and simulation tools to address various facets of infrastructure assurance and interdependencies. These tools include the Electricity Market Complex Adaptive Systems (EMCAS) model, which is designed to provide new insights into today's dynamic electricity markets [15–17]. EMCAS uses agent-based modeling techniques that represent multiple and diverse market participants or "agents," each with its own unique set of business and bidding strategies, risk preferences, objectives, and decision rules. The success of an agent is a function not only of its own decisions and actions, but also of the decisions and actions of other market participants. Because minimal amounts of local information are shared among

participants, agent decisions in EMCAS are made without either perfect knowledge or certainty.

The model's complex adaptive systems (CAS) approach empowers market agents to learn from past experience and change and adapt their behavior when future opportunities arise. With EMCAS, analysts can capture and investigate the complex interactions between the physical infrastructures (i.e. generation, transmission, and distribution) and the economic behaviors of market participants, which are a trademark of the newly emerging markets. The model does this by representing the transmission grid in detail and simulating the market operation on a chronological, hourly basis. This feature is particularly important when trying to assess the issue of market power.

Other CAS models, such as SMART II+ and SymSuite, have been developed to analyze large-scale, interconnected infrastructures with complex physical architectures [18, 19]. These models emphasize the specific evolution of integrated infrastructures and their participants' behavior, not just simple trends or end states. Argonne is also developing a next-generation drag-and-drop simulation-building platform that offers a unique, comprehensive, and unified modeling environment with capabilities for developing and integrating dynamic physical systems models, agent-based simulations, real-time data flows, advanced visualization, and postprocessing tools.

Another tool, called Restore, was developed at Argonne to address the postdisruption elements of interdependencies. Through Monte Carlo simulation, Restore estimates the time and/or cost to restore a given infrastructure component, a specific infrastructure system, or an interdependent set of infrastructures to an operational state [20]. The tool allows users to create a representative model of recovery and restoration activities. Graphical and tabular results allow analysts to better quantify the impact of infrastructure disruptions. Restore also provides a framework for incorporating uncertainty into the analysis of critical infrastructures.

Considerable research and model development are also underway at academic institutions and research centers throughout the world. For example, a Critical Infrastructure Simulation by Interdependent Agents (CISIA) simulator was developed at the Universita Roma Tre using CAS techniques to analyze the short-term effects of infrastructure failures in terms of fault propagation and performance degradation [21]. An interoperability input–output Model was developed at the University of Virginia Center for Risk Management of Engineering Systems to analyze the impacts of an attack on an infrastructure and the cascading effects (in economic and inoperability terms) on all other interconnected and interdependent infrastructures [22]. Although it is not possible to cite all relevant researches, an inventory and analysis of protection policies in 20 countries and 6 international organizations was published in 2006 by the Center for Security Studies in Zurich, Switzerland [23].

## 4 EDUCATION AND SKILL REQUIREMENTS

Multiple viewpoints and a broad set of interdisciplinary skills are required to understand, analyze, and sustain the robustness and resilience of our interdependent infrastructures [9]. For example, engineers (e.g. chemical, civil, electrical, industrial, mechanical, nuclear, structural, and systems) are needed to understand the technological underpinnings of

the infrastructures, as well as the complex physical architectures and dynamic feedback mechanisms that govern their operation and response (e.g. response to stresses and natural and man-made disruptions). Supply-chain analysts are needed to unravel and analyze, from an interdependencies perspective, the local, regional, national, and international flows of goods and services that support the functioning of our infrastructures.

Computer scientists, information technology specialists, and network and telecommunications experts are needed to understand the electronic and informational (cyber) linkages among the infrastructures. Information security and information assurance professionals are needed to ensure cyber security.

Economists are needed to understand the myriad marketplace and financial considerations that shape the business environment for public and private-sector infrastructure owners and operators. Expertise in estimating the direct and indirect economic consequences of infrastructure disruptions and building the necessary business cases for action is critical.

Social scientists are needed to understand the behaviors of infrastructure service providers, brokers, consumers, and other organizational entities that compete in the new economy. Health physicists and safety professionals are needed to quantify the public health and safety consequences of various disruption events that involve a wide range of threats (e.g. chemical, biological, radiological, nuclear, and explosive sources).

Lawyers, regulatory analysts, and public policy experts are needed to understand the legal, regulatory, and policy environment within which the infrastructures operate. Security and risk management experts are needed to perform vulnerability assessments (physical and cyber) and develop strategies to protect against, mitigate the effects of, respond to, and recover from infrastructure disruptions.

Software engineers, along with appropriate infrastructure domain and interdependencies experts, are needed to develop modeling and simulation tools to assess the technical, economic, psychological, and national security implications of technology and policy decisions designed to ensure the reliability and security of the nation's interdependent infrastructures. Insights from such tools will inform policy and decision-making processes.

Most important, risk and decision analysts are needed to help government officials at all levels, as well as private-sector infrastructure owners and operators, make cost-effective operation, protection, and risk management decisions. Such skills are also required to make defensible public policy, R&D, and resource-allocation decisions—and to effectively communicate those decisions.

## 5 PATH FORWARD

Important progress is being made in developing analytical approaches and modeling and simulation tools to address various facets of interdependencies. However, much remains to be accomplished, particularly because of the complexity and pervasive nature of interdependencies, and because they influence—in complex and uncertain ways—each component of the risk equation (threat, vulnerability, and consequence). A wide range of interdisciplinary skills are clearly required for comprehensive interdependencies analysis. This creates an additional challenge in terms of training across the diverse range of skill sets (e.g. software engineers, economists, and social scientists) and developing integrated

analyses and assessments. Exercises, such as the Blue Cascades exercises undertaken in the Pacific Northwest, provide a forum for discussing such issues and uncovering critical concerns at both the local and regional levels [24]. Information captured in responding to accidents and natural disasters, such as the August 2003 blackout and the recent hurricanes along the Gulf Coast, also provide valuable insights.

The following actions provide a foundation and path forward for understanding and analyzing interdependencies:

- Identify internal and external infrastructure assets, systems, and networks that, if lost or degraded, could adversely affect the facility, sector, or region of interest.
- Study natural disasters and incidents to gain insight into interdependencies problems and solutions.
- Develop contingency plans to deal with cascading outages.
- Identify how backup systems and other mitigation mechanisms can reduce interdependencies problems (and implement these mechanisms, as appropriate).
- Address interdependencies-related security through contractual arrangements with suppliers and distributors.
- Develop effective and secure procedures to share sensitive information, as appropriate, and tools to analyze interdependencies-related impacts.
- Collaborate, cooperate, and participate with supply/security partners; avoid failure of imagination in terms of "what if" events that could lead to infrastructure disruptions and associated interdependencies-related impacts.

## REFERENCES

1. President's Commission on Critical Infrastructure Protection (1997). *Critical Foundations: Protecting America's Infrastructures*. Available at http://fas.org/library/pccip.pdf.
2. U.S.-Canada Power System Outage Task Force (2004). *Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations*, April.
3. Rinaldi, S., Peerenboom, J. P., and Kelly, T. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Syst. Mag*. pp 11–25.
4. The White House (2003). *Homeland Security Presidential Directive/HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection*. Available at http://www.dhs.gov/xabout/laws/gc_121459789952.sthm#1. Department of Homeland Security, Washington, DC.
5. The White House (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. Available at http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf. Department of Homeland Security, Washington, DC.
6. The White House (2003). *The National Strategy to Secure Cyberspace*. Washington, DC.
7. U.S. Department of Homeland Security (2006). *National Infrastructure Protection Plan*. Department of Homeland Security, Washington, DC.
8. Peerenboom, J. P., Fisher, R. E., Rinaldi, S., and Kelly, T. (2002). Studying the Chain Reaction. *Electr. Perspect*. 22–35.
9. Peerenboom, J. P. (2001). Infrastructure Interdependencies: Overview of Concepts and Terminology, invited paper, *National Science Foundation/Office of Science and Technology Policy Workshop on Critical Infrastructure: Needs in Interdisciplinary Research and Graduate Training*, June 14–15, 2001, Washington, DC.

10. The Executive Office of the President, Office of Science and Technology Policy, and the Department of Homeland Security Science and Technology Directorate (2004). *The National Plan for Research and Development in Support of Critical Infrastructure Protection*.
11. Visarraga, D., Bush, B., Linger, S. P., and McPherson, T. N. (2005). Development of a JAVA Based Water Distribution Simulation Capability for Infrastructure Interdependency Analyses. *World Water Congress 2005: Impacts of Global Climate Change*, May 15–19, Anchorage, Alaska, p. 14.
12. Brown, T., Beyeler, W., and Barton, D. (2004). Assessing Infrastructure Interdependencies: The Challenge of Risk Analysis for Complex Adaptive Systems. *Int. J. Crit. Infr*. **1**(1),pp. 108–117.
13. See the Los Alamos National Laboratory web site (http://www.lanl.gov) and Sandia National Laboratories web site (http://www.sandia.gov/mission/homeland/programs/critical/nisac.html) for more detailed descriptions of tools and capabilities.
14. Bush, B., Dauelsberg, L., Ivey, A., LeClaire, R., Powell, D., DeLand, S., and Samsa, M. (2005). Critical Infrastructure Protection Decision Support System (CIP/DSS) Project Overview, LA-UR-05-1870, *3rd International Conference of the System Dynamics Society*, July 17–21, 2005, Boston, MA.
15. Veselka, T., Boyd, G., Conzelmann, G., Koritarov, V., Macal, C., North, M., Schoepfle, B., and Thimmapuram, P. (2002). Simulating the Behavior of Electricity Markets with an Agent-Based Methodology: The Electricity Market Complex Adaptive System (EMCAS) Model. *22nd International Association for Energy Economics International Conference*, October 2002 Vancouver, BC, Canada.
16. North, M. J., Thimmapuram, P. R., Macal, C. Cirillo, R., Conzelmann, G., Koritarov, V., and Veselka, T. (2003). EMCAS: An Agent-Based Tool for Modeling Electricity Markets. *Proceedings of the Agent 2003 Conference on Challenges in Social Simulation*, October 2003, Argonne National Laboratory/The University of Chicago, Chicago, IL.
17. Macal, C., Boyd, G., Cirillo, R., Conzelmann, G., North, M., Thimmapuram, P., and Veselka, T. (2004). Modeling the Restructured Illinois Electricity Market as a Complex Adaptive System. *24th Annual North American Conference of the USAEE/IAEE: Energy*, July 8–10, 2004, *Environment and Economics in a New Era*, Washington, DC.
18. North, M. J. (2000). SMART II+: The Spot Market Agent Research Tool Version 2.0 Plus Natural Gas *Proceedings of the Computational Analysis of Social and Organizational Science Conference 2000*, Carnegie Mellon University, Pittsburgh, PA, pp. 161–162.
19. Thomas, W. H., North, M. J., Macal, C. M., and Peerenboom, J. P. (2003). From Physics to Finances: Complex Adaptive Systems Representation of Infrastructure Interdependencies, *Naval Surface Warfare Center Technical Digest*, Naval Surface Warfare Center, Dahlgren, VA, pp. 58–67.
20. Peerenboom, J. P., Fisher, R. E., and Whitfield, R. (2001). Recovering from Disruptions of Interdependent Critical Infrastructures presented at *the CRIS/DRM/IIIT/NSF Workshop*, September 10–11, 2001, Alexandria, VA.
21. Panzieri, S., Setola, R., and Ulivi, G. (2004). An Agent Based Simulator for Critical Interdependent Infrastructures. *Proceedings of the 2nd International Conference on Critical Infrastructures*, October 24–27, 2004.
22. Haimes, Y. Y., Horowitz, B.M., Lambert, J.H., Santos, J.R., Lian, C., and Crowther, K.G. (2005). et al. Inoperability Input-Output Model for Interdependent Infrastructure Sectors: Theory and Methodology. *J. Infr. Sys*. **11**(2), 67–79.
23. See the *International Critical Information Infrastructure Protection (CIIP) Handbook*, available at *the Crisis and Risk Network* web site http://www.crn.ethz.ch/.
24. See *Pacific NorthWest Economic Region* web site for *Blue Cascades information* http://www.pnwer.org.

# SYSTEM AND SECTOR INTERDEPENDENCIES: AN OVERVIEW OF RESEARCH AND DEVELOPMENT

PAUL D. DOMICH
*CIP Consulting, Inc., Boulder, Colorado*

## 1 INTRODUCTION

This article will address the National Critical Infrastructure Protection Research and Development (NCIP R&D) Plan, the National Infrastructure Protection Plan (NIPP) and sector-specific agencies' (SSAs) R&D efforts.

## 2 HIGH-LEVEL R&D PRIORITIES FOR CRITICAL INFRASTRUCTURE/KEY RESOURCE

As recognized in the *National Strategy for Homeland Security*, "The Nation's advantage in science and technology is a key to securing the homeland." Research and development in modeling complex systems, data analysis, information sharing, threat identification and the detection of attacks, and the development of effective countermeasures will help prevent or limit the damage from disasters both man-made and naturally occurring. A systematic national effort has been created to leverage science and technology capabilities in support of national homeland security goals that involve private sector companies, universities, research institutes, and government laboratories involved in research and development on a very broad range of issues.

## 3 MOTIVATION FOR A NATIONAL R&D PLAN

Achieving this potential to field important new capabilities and focus new efforts in support of homeland security is a major undertaking. The Department of Homeland Security (DHS) and other federal agencies have been given responsibility to work with private and public entities to ensure that our homeland security research and development efforts are of sufficient size and sophistication to counter the threats posed by natural disasters and terrorism. The goal of this national R&D effort is to develop the desired new capabilities through "an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructures (CIs) and key assets from terrorist attack."[1]

[1]Homeland Security Presidential Directive 7/HSPD-7.

## 4 NATIONAL STRATEGIES, PRESIDENTIAL DIRECTIVES, AND AUTHORIZING LEGISLATION

The roles and responsibilities related to critical infrastructure/key resource (CIKR) research and development follow from a series of authorities, including the Homeland Security Act of 2002, CIKR protection-related legislation, Presidential Executive Orders, Homeland Security Presidential Directives, and National Strategies. These current authorities and directives have built upon those previously issued including Presidential Decision Directive 63—Protecting America's Critical Infrastructures (PDD-63) released in May of 1998 and spanning the broad homeland security landscape. The most significant authorities related to CIKR research and development are the Homeland Security Act of 2002 and Homeland Security Presidential Directive/HSPD-7.

*Critical infrastructures as defined include food and water systems, agriculture, health systems and emergency services, information technology, telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, and dams), transportation (air, highways, rail, ports, and waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons. Key resources refer to publicly or privately controlled resources essential to the minimal operations of the economy or government.*

The Homeland Security Act of 2002 provides the basis for the roles and responsibilities of the US Department of Homeland Security (DHS) in the protection of the nation's CIKR. This act defined the DHS mission as that of "reducing the nation's vulnerability to terrorist attacks," major disasters, and other emergencies, and charged the department with the responsibility of evaluating vulnerabilities and ensuring that steps are implemented to protect the high-risk elements of America's CIKR. The Homeland Security Act created the DHS Science and Technology Directorate and assigned it the responsibility to perform research and development in these areas in support of the broad DHS mission. Title II, Section 201 of the Act also assigned primary responsibility to the DHS to develop a comprehensive national plan for securing CIKR and for recommending "measures necessary to protect the key resources and CI of the United States in coordination with other agencies of the Federal Government and in cooperation with state and local government agencies and authorities, the private sector, and other entities."

Similarly, Homeland Security Presidential Directive/HSPD-7 established the official US policy for "enhancing protection of the Nation's CIKR" and mandated a national plan. This directive sets forth additional roles and responsibilities for DHS, sector-specific agencies (SSAs), other federal departments and agencies, state, local, and tribal governments, the private sector, and other security partners to fulfill HSPD requirements and calls for the collaborative development of the NIPP. HSPD-7 designates Federal Government SSAs for each of the CIKR sectors and requires development of an annual plan for each sector. HSPD-7 also directed the Secretary of DHS in coordination with the Director of the Office of Science and Technology Policy to prepare on an annual basis, a federal research and development plan in support of critical infrastructure identification, prioritization, and protection. This plan is the National Plan for Research and Development in support of National Critical Infrastructure Protection (NCIP R&D) and was first released in 2005 (www.dhs.gov).

## 5 NATIONAL INFRASTRUCTURE PROTECTION PLAN

The NIPP is a multiyear plan describing mechanisms for sustaining the nation's steady-state protective posture. The NIPP and its component sector-specific plans (SSPs) (see below) include a process for annual review, periodic interim updates as required, and regularly scheduled partial reviews and reissuance every 3 years, or more frequently, if directed by the Secretary of the DHS.

In accordance with HSPD-7, the NIPP defines the framework for security partners to identify, prioritize, and protect the nation's CIKR from terrorist attacks emphasizing protection against catastrophic health effects and mass casualties. The NIPP coordinates the activities for both public and private security partners in carrying out CIKR protection activities while respecting and integrating the authorities, jurisdictions, and prerogatives of each. While DHS has overall responsibility for developing the NIPP, the SSAs and their public and private sector counterparts are active partners in its development.

The goal of the NIPP, to achieve a safer, more secure, and more resilient America, consists of the following principal objectives:

- understanding and sharing information about terrorist threats and other hazards;
- building security partnerships to share information and implement CIKR protection programs;
- implementing a long-term risk management program that includes:
  - hardening and ensuring the resiliency of CIKR against known threats and hazards, as well as other potential contingencies;
  - processes to interdict human threats to prevent potential attacks;
  - planning for rapid response to CIKR disruptions to limit the impacts on public health and safety, the economy, and government functions;
  - planning for rapid CIKR restoration and recovery for those events that are not preventable; and
- maximizing efficient use of resources for CIKR protection.

The NIPP comprehensive risk management framework clearly defines CIP roles and responsibilities for the DHS; federal SSAs; and other federal, state, local, territorial, tribal, and private sector security partners.

The NIPP risk management framework is applied on an asset, system, network, or function basis, depending on the fundamental characteristics of the individual CIKR sectors. As illustrated in Figure 1, the framework relies on a continuous improvement cycle

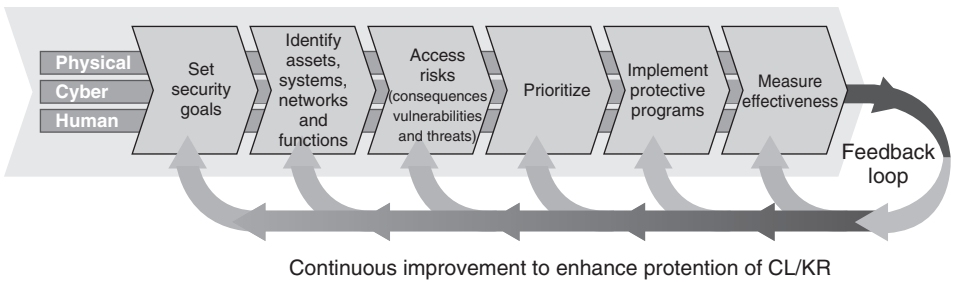



**FIGURE 1** NIPP risk management framework.

| Sector-Specific Agency | Critical Infrastructure/Key Resources Sector |
|---|---|
| Department of Agriculture<br>Department of Health and Human Services | Agriculture and food |
| Department of Defense | Defense industrial base |
| Department of Energy | Energy |
| Department of Health and Human Services | Public health and healthcare |
| Department of the Interior | National monuments and icons |
| Department of the Treasury | Banking and finance |
| Environmental Protection Agency | Drinking water and water treatment systems |
| Department of Homeland Security<br>Office of Infrastructure Protection | Chemical<br>Commercial facilities<br>Dams<br>Emergency services<br>Commercial nuclear reactors, materials, and waste |
| Office of Cyber Security and Telecommunications | Information technology<br>Telecommunications |
| Transportation Security Administration | Postal and shipping |
| Transportation Security Administration, US Coast Guard | Transportation systems |
| Immigration and Customs Enforcement, Federal Protective Service | Government facilities |

**FIGURE 2** Sector Specific Agencies.

so as to address the ever-changing homeland security landscape. The NIPP also provides the coordinated approach needed to establish national CIKR priorities, goals, and requirements for infrastructure protection, including related short-term R&D requirements. The NIPP was first released in June 2006 (www.dhs.gov).

## 6 SECTOR-SPECIFIC PLANS

Annual SSPs are required from each of the federal SSAs (See Fig. 2). These plans provide a common vehicle across all CIKR sectors to communicate CIKR protection performance and progress to security partners and other government entities and focuses on: priorities and annual goals for CIKR protection and associated gaps; sector-specific requirements for CIKR protection activities and programs based on risk and need; and projected CIKR-related resource requirements for the sector. Emphasis is placed on anticipated gaps or shortfalls in funding for sector-level CIKR protection and/or for protection efforts related to national-level CIKR that exists within the sector. The SSP plans address R&D requirements and activities relevant to the sector and include a description of future capabilities and R&D needed for that sector. These R&D sections align with the high

level federal CIKR R&D priorities but may also contain desired capabilities unique to the sector requirements and, therefore, not included in the broader and prioritized NIPP and NCIP R&D strategies and plans.

*The sector coordinating councils (SCCs) are self-organized and self-governed forums comprised of private sector owners and operators with specific membership varying from sector to sector, reflecting the demographics of each sector. The SCCs serve as principal sector policy coordination and planning entities for CIKR issues.*

*The government coordinating councils (GCCs) are the government counterpart for each SCC established to facilitate interagency and cross-jurisdictional coordination. The GCC is comprised of representatives across various levels of government (federal, state, local, or tribal) as appropriate to the individual sector.*

SSPs are developed by a designated lead federal agency in close collaboration with the corresponding SCCs, GCCs, and their state, local, territorial, and tribal homeland security partners. These plans address the unique characteristics and risk for each sector while coordinating their activities with other sector and national priorities. The SSPs for each sector must be completed and submitted to DHS within 180 days of issuance of the NIPP.

The SSPs serve to clearly define sector security partners and their authorities, regulatory bases, and roles and responsibilities. The plans address sector interdependencies and identify existing procedures for sector interaction, information sharing, coordination, and partnership as is appropriate. The SSAs and the various security partners identify and agree upon the goals and objectives for the sector as well as the desired protective posture for that sector. Consistent with the NIPP, the SSPs independently define the methodology used for assessing the risks and vulnerabilities of the sector and the mitigation strategy used.

Specifically, the SSPs identify priority CIKR and functions within the sector, including cyber considerations; assess sector risks including potential consequences, vulnerabilities, and threats; assess and prioritize assets, systems, networks, and functions of national-level significance within the sector; and develop risk-mitigation programs based on detailed knowledge of sector operations and risk landscape. The plans also develop the protocols to transition between steady-state CIKR protection and incident response in an all-hazards environment and define the performance metrics to measure the effectiveness of the approaches employed. The SSP concurrence process includes a formal review process for GCC member departments and agencies, as well as demonstrated or documented collaboration and coordination within the SCC, which may include letters of endorsement or statements of concurrence.

## 7 NATIONAL PLAN FOR RESEARCH AND DEVELOPMENT IN SUPPORT OF CRITICAL INFRASTRUCTURE PROTECTION

The research and development plan for protecting CIKR mandated by HSPD-7 is the NCIP R&D. This plan focuses on (i) creating a baseline that identifies major research

and technology development efforts within federal agencies and (ii) articulating a vision that takes into account future needs and identifies threat-based research gaps. The NCIP R&D Plan is developed through an intensive, collaborative, interagency effort and is coordinated with the R&D requirements coming from the NIPP and the associated SSPs. This public document highlights the longer-term targeted investments needed to help secure and protect the nation's key infrastructures and resources from acts of terrorism, natural disasters, or other emergencies. The plan is organized around nine major focus areas or themes that impact all CIs, identifies three high level goals for protecting CIKR, and prioritizes key R&D areas needed for CIKR protection. Additional details on the NCIP R&D plan are described below.

## 8 RELATIONSHIP BETWEEN THE THREE CIKR PLANS FROM AN R&D PERSPECTIVE

The NIPP Plan and SSPs together provide key elements to the operationally focused CIKR protection strategy applicable within and across all sectors. The SSPs also address the unique needs, vulnerabilities, and methodologies associated with each sector while the NIPP provides the high level strategies and overall coordination of these activities. The SSP and NIPP plans encourage alignment with other homeland security plans and strategies at the state, local, territorial, and tribal levels, providing for coordinated CIKR protection responsibilities appropriate within each of the respective jurisdictions. The strategy outlined in the NIPP processes is also intended to provide the coordination, cooperation, and collaboration among private sector security partners within and across sectors to synchronize efforts and avoid duplicative security requirements.

From an R&D perspective, each of the three national plans has wholly, or as a key component, the requirement to identify and prioritize new capabilities and future CIKR R&D needs. Proper coordination and alignment of these three plans are essential to making intelligent and effective investments in those R&D areas deemed most critical in the presence of limited R&D resources (both monetary and human).

The proper coordination of these R&D activities takes into account the effective planning horizon for each plan, the stakeholder focus, and national R&D priorities established for protecting CIKR. With respect to R&D requirements, the NCIP R&D Plan represents the longer-term comprehensive strategy for research and development across all sectors, focusing on new and ongoing federal R&D. In contrast, the annual NIPP and SSP reports include R&D requirements over a 1- and 3-year planning horizon respectively and address the most pressing capabilities needed immediately.

Stakeholder input is central to an effective short- and long-term R&D strategy. Similar to the NIPP, the NCIP R&D Plan provides for the coordination, cooperation, and collaboration among other federal agencies, and private sector security partners within and across sectors to synchronize related R&D efforts and avoid duplicative programs. Asset owners and operators across all sectors, public and private sector commercial service providers and product developers, professional and trade associations, and the broad national research and development community including academia, federal agencies and National Laboratories, and private sector groups, all provide valuable input to the R&D agenda for CIKR. The NCIP R&D working with these stakeholder groups develops the long-term R&D strategy for CIKR.

## 9 CYCLICAL DEVELOPMENT

The NCIP R&D plan includes a survey of current top-priority CIKR research and development underway at federal agencies and National Laboratories. This baseline represents current R&D in support of homeland security as well as other traditional agency mission areas impacting CIKR. The future capabilities identified in each of these three plans assume a cyclical development cycle where current technology is successively evolved building upon existing applications and capabilities. This development approach provides security providers with interim technologies while maintaining focus on longer-term national CIKR priority R&D goals and objectives.

## 10 MOTIVATION FOR CROSS-CUTTING R&D THEMES FOR ALL SECTORS AND INFRASTRUCTURES

Previous efforts to develop the R&D requirements for infrastructure protection were typically assembled along individual sector categories. In particular, directed planning activities to be organized along sector lines. Following the extensive work to implement PDD 63, it was apparent that this sector orientation challenged our ability to cost-effectively and efficiently address key factors related to the R&D. Relevant factors identified in the 2005 National Plan for Research and Development in Support of Critical Infrastructure Protection include the following:

- Many different sectors contain infrastructure systems that are vulnerable to the same threats.
- Combined planning of related sectors more directly addresses the inherent and broadly applicable interconnections and interdependencies among infrastructure sectors.
- Past efforts had a tendency to separately consider cyber and physical, which are interdependent in all sectors.
- The efforts to reduce vulnerability were separate from the efforts to design new infrastructure for higher performance and quality. Efforts to reduce vulnerability are more effective if they are incorporated into new designs.
- The challenge of evaluating cross-cutting new threats against opportunities coming from new technological advances has not been adequately addressed. Cross-cutting observations of threats and opportunities could potentially be incorporated by designers into future specialized systems.

The NIPP together with the accompanying SSPs provide detailed sector plans essential for operational-level focus and for strategic and resource prioritization. However for R&D planning purposes, important cross-sector synergies can be realized and funding better leveraged by grouping the sector R&D requirements across common themes. Due to the functional and operational requirements, the sector focus though is retained in the NIPP together with the SSPs for obvious reasons.

## 11 NINE COMMON THEMES

The NCIP R&D Plan is structured around nine themes in the fields of science, engineering, and technology that support all CI sectors, encompass both cyber and physical

concerns, and are strongly integrated into an overall security strategy. The basis for selection of these nine themes was their repeated occurrence in the expressed concerns of infrastructure owners and operators, industry representatives, academia and government officials. The nine themes identified in the NCIP R&D plan are as follows:

1. Detection and sensor systems;
2. Protection and prevention;
3. Entry and access portals;
4. Insider threats;
5. Analysis and decision support systems;
6. Response, recovery, and reconstitution;
7. New and emerging threats and vulnerabilities;
8. Advanced infrastructure architectures and systems design; and
9. Human and social issues.

Through a broad interagency collaborative effort, federal agency experts and others have confirmed the completeness of nine themes and identified three broad long-term strategic goals for CIKR. The three overarching CIKR strategic goals identified are as follows:

- Goal 1: A national common operating picture for CI
- Goal 2: A next-generation computing and communications network with security "designed-in" and inherent in all elements and
- Goal 3: A resilient, self-diagnosing, and self-healing physical and cyber infrastructure system.

The nines themes of the NCIP R&D Plan map directly onto each of the three long-term strategic goals and contain both long-term and short-term priority research and development areas. Figure 3 below which appears in the 2005 National Plan for Research and Development in Support of Critical Infrastructure Protection, illustrates a mapping of a single theme area priority onto a strategic goal.

These high level goals and their associated high priority R&D areas were vetted with stakeholder groups from the private sector, academia, and the National Laboratories, and serve to drive future R&D efforts and ensure that new and effective technologies will be available for the future security of the Nation's CIKR.

## 12 NCIP R&D PLAN THEME AREA: ANALYSIS AND DECISION SUPPORT SYSTEMS

This section describes the analysis and decision support system theme of the NCIP R&D Plan. This development is representative of the conclusions identified and serves to illustrate the range of R&D activities inherent in each theme area. Two examples are provided: The critical infrastructure protection decision support system and the interdependency models used to analyze the collapse of the World Trade Center (WTC) towers resulting from a terrorist attack.

Examination of trade-offs between the benefits of risk reduction and the costs of protective action require analysis and decision support systems that incorporate threat

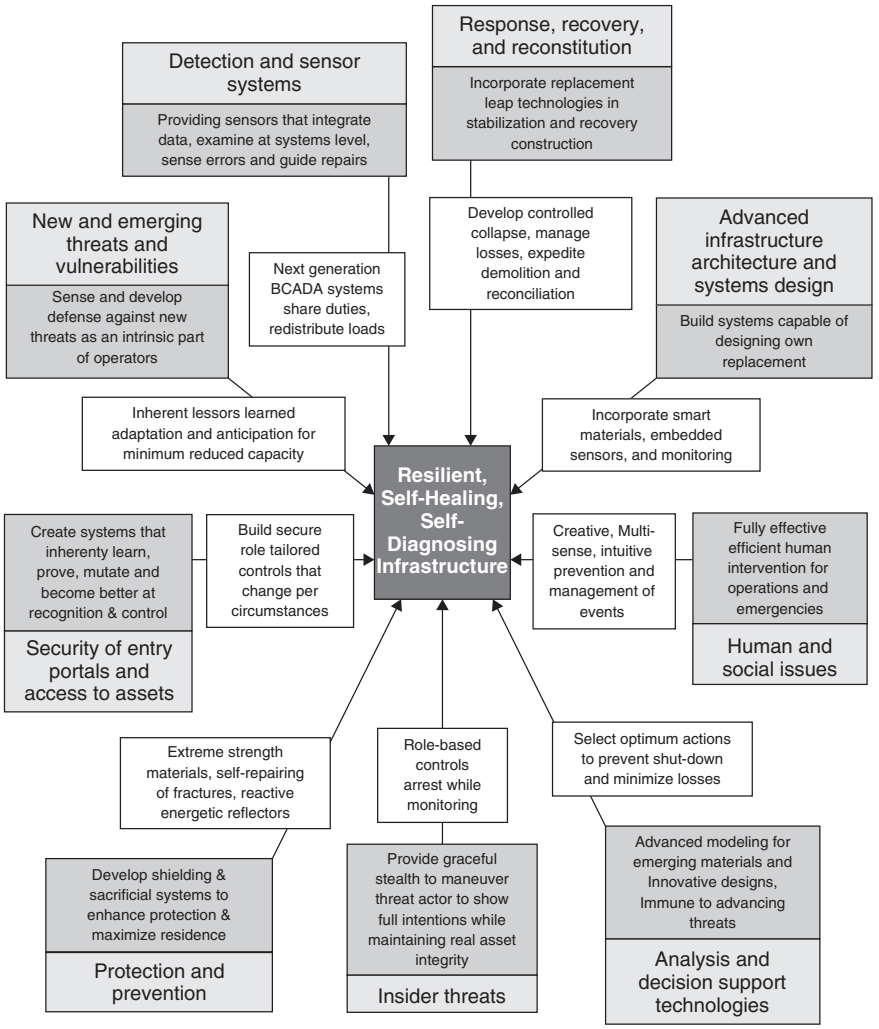



**FIGURE 3** Relationship of NCIP R&D goals and themes.

information, vulnerability assessments, and disruption consequences in quantitative analyses through advanced modeling and simulation. Broadly interpreted, the analysis and decision support technologies area addresses future R&D needs in

- risk analysis and decision theory for evaluating strategies and prioritizing CIP investments;
- threat evaluation;
- vulnerability and performance evaluation and design of upgrades;
- forensic analysis and reconstruction;
- consequence analysis and modeling of interconnected CI sectors, and;
- integrated systems modeling.

Of the existing systems and technologies available presently, many are focused on military applications and are classified or otherwise restricted and have not been examined within the broad, integrated context necessary for homeland security in a domestic setting. As such, future work is needed to transform Department of Defense-focused technologies to homeland security applications were possible and to develop new technologies where gaps in current capabilities exist.

Many of these topic areas are ripe for future research and development opportunities. Future R&D in analysis and decision support should be cognizant of, and attempt to address the major challenges in this field of study are as follows:

- the increasing size and complexity of the models under examination;
- the vast size and complexity of the sectors being modeled;
- the need to tightly couple or integrate multiple models across disciplines and across sectors;
- the absence of standardized analysis metrics and measures across sectors; and
- the need for more agile, robust, and high confidence systems.

Future advances in the analysis and decision support approaches will change how analyses are performed and informed decisions are made. Together with improvements in graphical and computational capabilities and improved communication capability, accurate and timely decision information will transform how the nation responds to man-made and natural disasters. Central to all three of the strategic goals for CIKR is the development of effective and validated analysis and decision support systems.

## 13 OVERVIEW OF CONSEQUENCE ANALYSIS AND MODELING OF INTERCONNECTED CRITICAL INFRASTRUCTURE SECTORS

Of particular interest for this section is decision support through consequence analysis and the analytical modeling of interconnected and interdependent CIs. These consequence and impact analyses are central to quantifying the severity of disasters and are used in decision support systems by decision makers both for planning purposes and for *real-time* protection, response, and recovery activities. Decision- makers must have the capability to understand the causes of disruptions to infrastructures (e.g. cascading failures), the consequences of decisions, and the trade-offs between alternative actions in the decision-making process.

Through HSPD-7, 13 CI sectors have been identified: Agriculture and Food, Public Health/Health Care, Drinking Water and Wastewater Treatment Systems, Energy, Banking and Finance, National Monuments and Icons, Defense Industrial Base, Information Technology, Telecommunications, Chemical, Transportation Systems, Emergency Services, and Postal and Shipping. Analytical models of these CIs must possess sufficient accuracy to accurately represent their normal behavior and the effects of disruptions due to a range of threats. The inherent interconnectivity and interdependencies of these systems make this modeling effort a long-term monumental challenge.

## 14 OVERVIEW OF MODELS

There has been considerable effort put forth in providing analytical models for select infrastructure sectors. For energy and the telecommunications sectors, for example,

detailed models have been previously developed by Department of Energy (DOE), National Communications System, and private sector organizations from these sectors. As mentioned previously, the DOE National Laboratories and the DHS National Infrastructure Simulation and Analysis Center (NISAC) have developed and/or extended the number of infrastructure models to include interdependencies and to enhance model fidelity and breadth of application. Models for agriculture, food, banking and finance, government facilities, are either less mature or not well understood or characterized. For specific biological events, such as pandemic/avian flu, the US Department of Health and Human Services and DHS have developed detailed models to analyze the spread and impact of a major biological disease outbreak.

## 15 INFRASTRUCTURE SYSTEM AND SECTOR INTERDEPENDENCY R&D PRIORITIES

Current infrastructure system and sector interdependency development at three DOE National Laboratories are focusing on new tools for interdependency modeling and simulation of the CI sectors. These models use a system dynamics approach to analyze changes in supplies and demands within and between infrastructures. These models study disasters ranging from major hurricane impacts to biological/agriculture disease outbreaks to failures in key components of the telecommunication system. These studies use existing knowledge and understanding of the systems and sectors under examination and verify model behaviors-—where possible—using past disaster events to confirm that the predicted interdependencies and computational results were realistic.

Other efforts such as those of NISAC seek to develop higher fidelity models with comparable vulnerability and consequence analyses for select CI sectors. These focused sector models provide detailed understanding of the progression and impact of disruptions to the associated infrastructures though they embody more limited interdependencies with other infrastructures. Important advances in vulnerability assessments will include new integrated physics-based models for analyzing highly complex and integrated systems such as those that were developed for the fire dynamics and structural failure analyses of the WTC towers. Advances are still needed in the development of practical tools for quantifying the full spectrum of the consequence metrics identified in HSPD-7 in order to inform investment decisions for all-hazards risk management and emergency preparedness.

These types of models must be developed to address the needs for CIP with data and results that are compatible and interoperable with other sector models. These systems must be flexible and responsive to evolving requirements and conditions imposed by decision makers and changes in the physical and cyber environments. Data for these systems must remain current and contain sufficient granularity to provide adequate specification to the models to be useful in detailed analyses. And there is a need for improved modeling and simulation methods that will make it easier to predict the behavior of complex generic computer networks under various scenarios, and to perform ”what-if” analyses. This latter development will be analogous to a virtual experiment performed on a computer network under a range of different conditions. Integration of such cyber network models into larger infrastructure models will contribute to the understanding that is gained from interdependency modeling for the CI sectors.

Example 1: The Critical Infrastructure Protection-Decision Support System (CIP-DSS)

The Critical Infrastructure Protection-Decision Support System (CIP-DSS), developed by the DOE National Laboratories at Sandia, Los Alamos, and Argonne through funding from the DHS, is a risk-informed decision analysis tool using a suite of mathematical models for assessing the consequences of CI disruption at both the metropolitan and national levels. This modeling effort is the first of its kind to incorporate infrastructure interdependencies along with workforce or population, and geographical influences, in a unified decision support system.

The CIP-DSS modeling system comprises a wide range of mathematical models, tools, and associated data. Included are system dynamics models that: represent each of the 17 relevant sectors/assets; include geographical influences that interact with each sector component in the model; represent the primary interdependencies among infrastructures and primary processes, activities and interactions of each infrastructure; provide for important feedback mechanisms and all critical inputs and outputs across infrastructures; and have the capability to handle major substitution effects. The data for the models comes from a range of sources and include, for example, industry production reports, published literature, and data from the Census Bureau and Bureau of Labor Statistics.

This system is used to simulate the steady-state conditions simultaneously across all infrastructures and the effects of disruptions to steady state, caused by specific threat scenarios in a Monte Carlo simulation setting. The outputs to the consequence modeling are used in a decision-support methodology to analyze and evaluate alternative strategies and their related impacts.

Examples of questions that this decision support system is designed to answer include the following:[2]

- What are the consequences of attacks on infrastructure in terms of national security, economic impact, public health, and conduct of government, including the consequences that propagate to other infrastructures?
- Are there choke points in our nation's infrastructures (i.e. areas where one or two attacks could have the largest impact)? What and where are the choke points?
- Incorporating consequence, vulnerability, and threat information into an overall risk assessment, what are the highest risk areas?
- What investment strategies can the United States make such that it will have the most impact in reducing overall risk?

To develop the CIP-DSS decision support methodology, the system developers conducted a series of formal and informal interviews of CIKR decision makers and stakeholders in order to identify requirements for the decision support system, define the decision environment, and quantify the prioritization of consequences. The taxonomy of decision metrics derived from this research involves six categories: (i) sector-specific, (ii) human health and safety, (iii) economic, (iv) environmental, (v) sociopolitical, and (vi) national security. The risk-related preferences for the decision

[2]CIP-DSS Documentation.

makers were encoded to arrive at multi-attribute utility functions consistent with the output of the consequence models and applicable to the scenarios under consideration. These multi-attribute utility functions describe the preferences of the decision maker as a function of the frequency of the disaster and its consequences relative to the decision metrics previously defined.

Currently, the CIP-DSS system is fully operational. The model has been used to produce detailed analyses of both simulated and real-life disasters providing analysis and insights to decision makers and strategic planners. The initial model representations provide broad infrastructure coverage and are iteratively being refined and enhanced. Significant efforts are underway to analyze specific threat scenarios as defined by stakeholders and program sponsors. The system requires continuous testing and refinement as a result of insights developed in the threat scenario build-out.

The CIP-DSS system has provided a valuable understanding of the infrastructures and their dynamics, developed insight into infrastructures viewed as dynamic systems, and provided analyses that can identify high leverage points and suggest mitigation strategies. This simulation and assessment capability allows decision makers to understand the CI of the United States including its components, their coupling, and their vulnerabilities. This capability can be used in a crisis response mode as well as in an analysis and assessment mode to provide decision makers with a better basis to make prudent, strategic investments, and policy resolutions needed to improve the security of our infrastructure.

Example 2: Integrated high-fidelity models—NIST Analysis of the WTC tower Collapse

The second example area of the analysis and decision support system is the National Institute of Standards and Technology (NIST) Analysis of the WTC tower collapse. A complex and broad suite of software models were used in the analysis that led to a series of recommendations for changes in design and material requirements for tall buildings. These tools together with detailed laboratory forensic analysis provided an extensive and comprehensive list of recommended changes to building codes and standards.

Following the terrorist attacks on September 11, 2001, NIST was authorized by the US Congress to conduct a multiyear building and fire safety investigation into the collapse of the WTC Towers (WTC 1 and 2) and WTC 7. The analysis studied the factors contributing to the probable cause of post-impact collapse and required a thorough examination of the planes' impact, fire dynamics and structural failures, the effectiveness of resistance design and retrofit of the structures, and the effectiveness of the fire resistive coatings on structural steel. The subsequent analysis resulted in the most detailed study of a complex system/structure ever performed and was successful in integrating the dynamical effects within multiple software-based mathematical models. Model outputs were combined to provide a thorough understanding of the effects of the explosion and resulting fire, and the effects of superheated steel on the structural integrity of a steel structure.

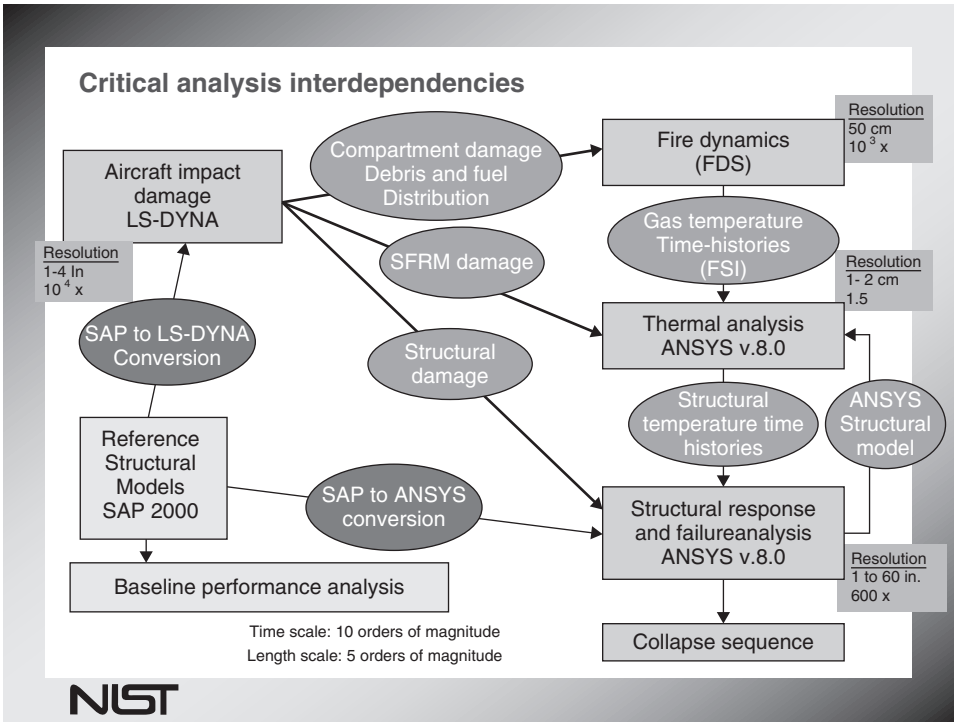



**FIGURE 4** Model interdependencies from the NIST WTC collapse investigation.

The analysis of probable collapse sequences for the WTC required analyzing a variety of factors. This included the effects of the aircraft impact on the structures, the spread of jet-fuel and the resulting fire on multiple floors, the thermal weakening of structural components, and the progression of local structural failures that initiated the catastrophic collapse of the WTC Towers 1 and 2. The mathematical analysis was supported by laboratory-based experiments, visual and physical evidence acquired from multiple sources. The following Figure (Fig. 4) depicts the models and their interdependencies that were used in the NIST analysis.[3]

[3]Taken from the US Federal Building and Fire Safety Investigation of the World Trade Center Disaster to the 4th Annual Congress on Infrastructure Security for the Built Environment, October 19, 2005, Dr. James E. Hill, Director, Building and Fire Research Laboratory, NIST.

Also modeled in this investigation was the occupant evacuation of the towers, the condition of stairwells and the flow of evacuees from the buildings. The results of the modeling effort combined with a thorough laboratory analysis provided the key insights needed to accurately describe the factors that led to the collapse of the WTC towers in New York City on September 11, 2001. The key findings from the entire WTC study, as a result of the 3-year effort, can be found at http://wtc.nist.gov/.

### 16 FUTURE DIRECTIONS FOR SECTOR AND SYSTEM INTERDEPENDENCY R&D, PARTNERSHIP FOR CRITICAL INFRASTRUCTURE SECURITY

The previous examples illustrate just two areas where analysis and decision support techniques have been advanced significantly. These are exemplary of the R&D required to address the complex systems and infrastructures currently present. Many new areas of research exist in analyzing the complex interdependencies of CIKR as well as development of accurate high-fidelity analysis models for specific infrastructures.

# PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION

DAVID A. JONES AND JAMES P. PEERENBOOM
*Argonne National Laboratory, Argonne, Illinois*
BRENTON C. GREENE
*Northrop Grumman Corporation, McLean, Virginia*
IRWIN M. PIKUS
*Consultant, Bethesda, Maryland*

## 1 INTRODUCTION

Following is a brief history that led to the creation of the President's Commission on Critical Infrastructure Protection (PCCIP), selected details of the Commission's inner-workings, an overview of the Presidential Decision Directive (PDD) promulgated as a result of the PCCIP report, and six research and development (R&D) areas targeted for further exploration.

It is important to fully understand the concepts of infrastructure *dependency* and *interdependency*. Figure 1 depicts illustrative infrastructure dependencies for electric power, while Figure 2 depicts examples of interdependent infrastructures. In Figure 1 examples of dependencies of other infrastructures are shown for the electric power infrastructure operation. A problem with any function can adversely affect the operation of the infrastructure. In Figure 2 the interaction of two or more functions is shown. The definition of

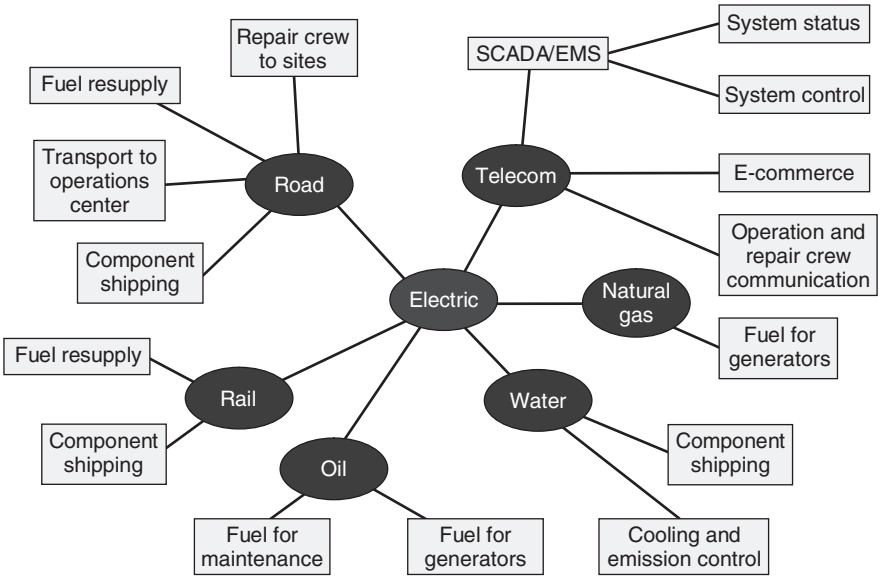



**FIGURE 1** Illustrative infrastructure dependencies for electric power.

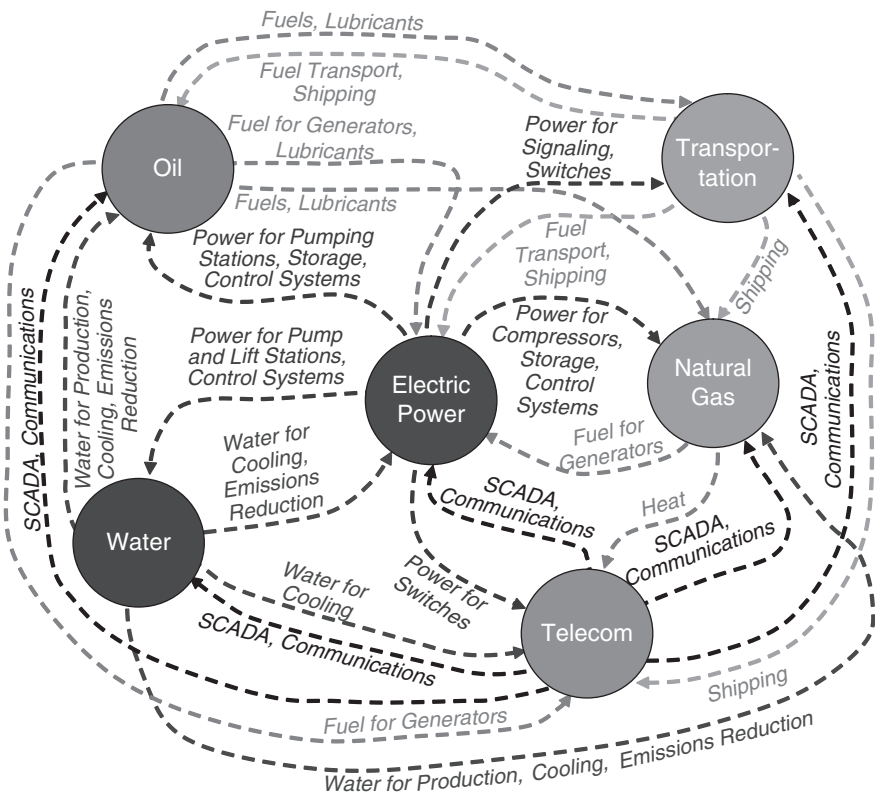



**FIGURE 2** Examples of interdependent infrastructures.

*interdependency* can be found in the Glossary of Key Terms in the National Infrastructure Protection Plan—"The multi- or bi-directional reliance of an asset, system, network, or collection thereof, within or across sectors, on input, interaction, or other requirement from other sources in order to function properly." The key to *interdependency* is that two or more assets depend on one another.

Even though research on interdependencies in the United States began many years ago with efforts in the Department of Defense (DoD), the broader federal government effort began with the PCCIP in 1996–1997.

## 2 PROLOGUE—PRECURSOR EVENTS TO THE PCCIP

Early critical infrastructure efforts began with military strategic targeting, as databases of key potential targets were assembled. Initiatives to identify the most critical targets drew on strategic insights from system experts who identified such targets as vital bridges and other transportation hubs, critical industrial capabilities, and similar strategic sites. In the 1980s, such approaches were further advanced by bringing in civilian engineers with greater insights as to how particular infrastructures functioned and how they might depend on external needs such as power or water. With the dynamic growth of computer processing capability and the creation of infrastructure databases, coupled with knowledge of how particular systems functioned, engineers began to model the performance of particular infrastructures. Though initially challenging, modeling became a vital tool for improving a particular infrastructure's reliability, robustness, and recoverability in an emergency. As the models matured, they became more valuable for assessing system performance and predicting how systems would respond during particular events or in case of casualties. However, these models usually focused only on a specific system or infrastructure segment; they did not incorporate other infrastructure sectors. Thus, computer models of infrastructures had not yet begun to consider and model interdependencies.

Consideration of interdependencies began in the late 1980s, whereby models of one particular infrastructure, such as electric power, could be considered alongside another infrastructure sector, such as telecommunications, thus beginning to explore where one infrastructure depended on signals, communications, or other processes within a separate infrastructure. This interdependency raised the possibility that an infrastructure could be attacked through its dependent elements; that is, something could be attacked without ever touching the obvious components within that infrastructure. However, while models of individual sectors were becoming increasingly mature, models of other sectors were often not compatible (i.e., in format, protocols, or input/outputs), and the merging of models to achieve interdependency modeling became a real challenge. With a significant increase of available open-source information on infrastructures in the 1990s, the ability to consider and assess infrastructure performance and interdependency improved. Thus, in the military targeting world, critical infrastructure targeting was continuing to advance. Targeting techniques were exploiting technology to render a particular infrastructure more vulnerable. In some ways, therefore, the more dependent a particular nation or system was on technology potentially increased the vulnerability of its critical infrastructures. Within DoD, these concepts advanced significantly, within an organization that evolved to become the Joint Warfare Analysis Center in Dahlgren, Virginia, and within the Joint Program Office for Special Technology Countermeasures, also in Dahlgren.

In 1992–1993, the maturation of critical node targeting led to discussions (within DoD's Office of the Under Secretary for Policy) concerning the need to explore the potential vulnerability of our nation to similar targeting approaches. As indicated above, interdependencies rendered particular infrastructures potentially more vulnerable. This possibility was countered in part by another factor: the increasing complexity of our infrastructures—how they interconnected, what software systems operated them, and what security tools were in place to enhance both physical and cyber security. This complexity could make it more difficult to attack a particular infrastructure. Even though increased complexity of our infrastructures may reduce some vulnerabilities, new ones could also be introduced that need to be examined and understood. Some infrastructure sectors began to consider interdependency issues long before others. Among the earliest infrastructure sectors to begin building reliability and security into their systems were the telecommunications and the banking and finance sectors. The early efforts to assure telecommunications functionality and survivability were born following the Cuban Missile Crisis (1962) with the establishment of the National Communications System, which focused on building national security and emergency preparedness features into the nation's communications infrastructure. Similarly, though for different reasons, banking and finance led most infrastructure sectors in building security into their facilities by asking such questions and answers as "Why do people rob banks?" "Because that is where the money is." The industry's concern over security was similarly advanced as they developed information technology processes that linked banking systems.

Other policy efforts across government to consider potential vulnerabilities in our nation came to light—efforts often unknown to other branches of government. For example, a senate-directed study of infrastructure vulnerability was undertaken in the 1989–1990 time frame. Led by a Secret Service agent, this study produced a sensitive report that was delivered to both Senate leadership and the National Security Council (NSC). Similarly, the Center for Strategic and International Studies conducted a review of infrastructure vulnerability. All these efforts came to a similar conclusion: the potential vulnerability of critical infrastructure was an issue that warranted a more detailed study and possible actions to bolster our national security. Following the first World Trade Center bombing in 1993, New York City government established a committee on counterterrorism, with several subgroups that focused on infrastructure and emergency response issues. As a result, New York City bolstered its emergency operations center and developed very comprehensive planning on emergency response.

As concerns for infrastructure vulnerability gained momentum within the national security policy community, a series of briefings were held in 1994–1995 to highlight potential critical infrastructure vulnerabilities and to assess terrorist threats that could potentially exploit such vulnerabilities. In late 1995, the Department of Justice and the DoD cosigned a document directing the establishment of a working group to explore critical infrastructure vulnerabilities in this light. The group, called the *Critical Infrastructure Working Group* (CIWG), was under the leadership and guidance of Ms Jamie Gorelick, Deputy Attorney General at that time. The CIWG consisted of eight members, including five subject-matter experts from the Defense, Justice, and Intelligence communities. Curiously, because many interagency legal issues began to surface in these discussions, the CIWG included three representatives from the offices of various general counsels. The tasking for the CIWG was to explore the concept of domestic vulnerability and, from that, recommend a possible course of action for the nation's security. Following delivery of the CIWG report to the White House in January 1996, the CIWG was

reconvened to prepare a draft Executive Order, which established the PCCIP to explore critical infrastructure.

## 3 PCCIP REPORT OVERVIEW

### 3.1 Executive Order 13010, Critical Infrastructure Protection: Scope and Key Sections

On July 15, 1996, President Clinton signed Executive Order 13010, titled *Critical Infrastructure Protection*, which focused on protecting those national infrastructures vital to the defense and economic security of the United States. The Order named eight specific infrastructures as critical to the United States and identified both physical and cyber threats to these infrastructures. The infrastructures were telecommunications, electric power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. The Order also noted that many infrastructure enterprises are owned and/or operated by the private sector. Thus, a partnership between the government and the private sector was considered essential.

The Order established a Presidential Commission to, among other things, assess the nature and scope of threats and the vulnerabilities of these critical infrastructures and recommend a comprehensive national policy and implementation strategy for assuring their continued operation.

The Commission was to consist of a full-time chair, appointed by the president, and up to 20 full-time commissioners, no more than 2 of whom were to be nominated by each of 10 named departments and agencies. The departments and agencies directed to nominate commissioners were Treasury, Justice, Defense, Commerce, Transportation, Energy, Central Intelligence Agency, Federal Emergency Management Agency, Federal Bureau of Investigation (FBI), and National Security Agency. The Commission had authorized staff and contracting authority. Anticipating the sensitive nature of the information to be dealt with, each commissioner and many of the staff held high-level security clearances.

Nothing in the Order explicitly cited the importance of interdependencies among the infrastructures, but interactions among the infrastructures was an implicit priority in the interdisciplinary structure of the Commission and the Order's mandate to assess the scope and nature of the wide-ranging vulnerabilities of and threats to critical infrastructures.

### 3.2 Commission Structure

One of the first tasks in the operation of the Commission was the development of a work plan. To help simplify the effort and rationalize work assignments, the Commission adopted a structure focused on five infrastructure sectors that incorporated the eight critical infrastructures named in the Executive Order and allowed for some necessary amplification. The five sectors were as follows:

1. *Information and communications.* Recognized the intimate and necessary connection between telecommunications and the entire range of information technology. The original scope was expanded to include the threats to and vulnerabilities of the full range of information systems, including, but not limited to, the telecommunications links. The sector included the Public Telecommunications Network, the

Internet, and millions of computers and related equipment in homes, businesses, academe, and other organizations across the nation.

2. *Energy.* Included both the entire electric power infrastructure and portions of the oil and gas infrastructure. Both the Department of Energy (DOE) and Department of Transportation (DOT) have statutory authority pertaining to aspects of the oil and gas infrastructure. The DOE has responsibilities in the production and storage elements, while the DOT has responsibilities in the pipeline and transportation elements.
3. *Physical distribution.* Included air, water, surface (including rail, road, and pipeline), and subsurface transportation subsectors—systems that facilitate the movement of people and goods. It also included navigation systems such as global positioning systems.
4. *Banking and finance.* Included all infrastructure elements relating to financial transactions, including various financial institutions, financial markets, and the companies that service and work with them.
5. *Vital human services.* Included water supply, emergency services, and government services at all levels (such as Social Security, weather forecasting, and aid to dependent children). The original mandate to include continuity of government was changed, with the approval of the White House, to focus on services provided by the government since issues of continuity of government were being addressed in other forums. The Commission explored the possibility of expanding the scope of this sector to include agriculture and public health but because of the limited time and resources available, decided that such expansion should be considered in the next phase of the government effort following the work of this Commission.

### 3.3 Commission Process

After establishing the sectors and assigning lead and supporting commissioners and staff, the Commission, through the five sector teams, turned to developing a detailed characterization of each sector. This exercise served as a basis for understanding the nature of the vulnerabilities of the infrastructure, the threats it might face, and the potential consequences that might be expected from a successful attack. The work plan then called for the Commission to develop a national policy and a strategy for implementation. At every stage of the effort, the Commission took extraordinary measures to ensure that it acquired a solid base of information and that it vetted the work and thinking with a wide range of experts and stakeholders.

Each sector arranged briefings (in many cases for the entire Commission) on the structure of the sector; its operations, dependencies on other sectors, particular weaknesses, and critical vulnerabilities; and potential consequences of failure, not only for customers but also for the broader community. Among the experts from whom briefings were requested were owners/operators of infrastructure organizations, trade associations, professional societies, community leaders, government officials, and subject-matter experts. Some briefings were classified, and nearly all were treated as highly sensitive even if not officially classified under national security procedures.

Each sector group developed a thorough characterization of its respective infrastructure. In some cases, contractors were hired to develop the product—under the guidance of and with assistance from the commissioners. In other cases, the sector staff did the

bulk of the work with assistance from contractors. In at least one sector, a series of meetings across the nation in cooperation with the American Public Works Association elicited the views and concerns about infrastructure protection from local private and government groups.

The Commission conducted several open "town meetings" at locations across the country (e.g., Boston and Houston), both to raise the level of awareness among the general public about critical infrastructure protection and to elicit information and perspectives concerning the issues.

The Commission's final report, *Critical Foundations: Protecting America's Infrastructures*, was released publicly in October 1997. Much of the documentation developed by the Commission, however, has not been released to the public and is exempt from such release under statutes and executive orders.

## 3.4 Selected Case Studies of Infrastructures

***3.4.1 Water Infrastructure.*** The water infrastructure was part of the vital human services sector, a varied collection of critical infrastructures that did not fit into the other four sectors. The Commissioner from the Department of Commerce was chosen to lead this sector, and several other commissioners were appointed to the team. In contradistinction from some other sectors, this team decided against contracting with an outside firm to help characterize the infrastructure and probe its vulnerabilities. Rather, this team hired a few staff to be responsible for the effort and several outside consultants to address specific problems.

The team conducted a characterization of the water infrastructure through a series of discussions with the US Environmental Protection Agency, the US Geological Survey, the US Army Corps of Engineers, the Department of Health and Human Services, the American Water Works Association, and a number of individual water utilities across the country. In addition, facts and data provided by the organizations and utilities interviewed were analyzed and included in the characterization. These results were documented in the sector report, which, to date, has not been publicly released because of their sensitivity.

The major security concerns that emerged were the potential for

- large-scale impacts on public health through purposeful contamination of the water supply with toxins and/or pathogens and
- disruption of the water supply through destruction of assets such as pumps, pipes, valves, control systems (including supervisory control and data acquisition [SCADA]), and treatment facilities that would not only cause some challenges to public health but would also cause serious economic damage through the disruption of activities that depend on water supply.

Both contamination and physical destruction of system assets are physical threats. The primary cyber threat relevant directly to water supply is through the SCADA system. While in principle, it is possible for a cyber attack to have serious consequences, even more dramatic and extensive impacts would be achievable more easily through the use of physical attacks, such as explosives and contaminants. The primary advantages of a cyber attack on water supply would be that, in many cases, an adversary could gain sufficient access, while maintaining a physical distance far from the target, and would have a better chance at disguising or hiding his or her identity.

At the time, opinion within the water sector concerning the importance of a threat of water contamination was divided, and no definitive studies had been conducted. The Commission team tasked one of the national laboratories to undertake a definitive study aimed at determining whether there were any chemical or biological agents, reasonably available to terrorists, in quantities that could be carried by one or two people that could cause thousands of deaths when introduced into a municipal water supply system. The study, which was not exhaustive, identified several such agents. This alerted the Commission to the extraordinary importance of preventing, detecting, and mitigating such potential contamination.

The team also addressed several interdependencies of water supply systems. For example, water utilities use large quantities of chemical disinfectants such as chlorine or chloramine to kill a number of biological contaminants. Utilities generally have limited storage capacity for these materials and depend on timely delivery through either rail or truck transport. In addition, many water utilities run their SCADA systems over the public switched network, and disruption in those communication elements could wreak havoc on the operation of dependent utilities. Finally, with regard to dependencies of water on other infrastructures, most utilities require externally provided electric power to operate pumps and automatic controls, including valves and monitoring equipment.

Other sectors, of course, depend on water. For example, illnesses and death caused by contaminated water would affect the workforce and strain resources needed for dealing with other emergencies. Few hospitals have alternate supplies of clean water, so a disruption could seriously affect their ability to care for patients. Many industries require clean water for their manufacturing processes. Most municipalities access water for fighting fires from the water supply utility. Therefore, a disruption in the supply of clean water could also affect fire fighting. In some cases, disruption in the flow of source waters could impair hydro-generation of electricity.

The Commission found no indications of interdependencies leading from an attack on water supply to cascading (singularity) failures in other infrastructures in the near term. If longer term outages were encountered, the potential for such cascading failures seemed intuitively to be increased.

***3.4.2 Energy Infrastructure.*** The Commission established an Energy team to lead the effort for the electric and oil and gas sectors. A DOE commissioner led a team consisting of several commissioners with supplemental help from DOE national laboratory experts in the electric power and the oil and natural gas infrastructures, as well as cyber security. The team generated two detailed reports that characterized the sectors, current trends, impacts from significant outages, threats and vulnerabilities, issues, risk management, interdependencies, protective measures, Commission outreach, and strategies and recommendations. Significant physical security information was drawn from previous reports because of terrorist concerns in the late 1980s [1, 2]. Organizations providing a wealth of reference material included DOE, Energy Information Administration, North American Electric Reliability Council (NERC), and Federal Energy Regulatory Commission.

In addition, the Energy team conducted an extensive outreach program to many sector organizations (NERC, Edison Electric Institute, National Petroleum Council, American Petroleum Institute), and leading companies within the sectors. This effort collected the ideas and concerns of the owners/operators and invited review and comment of their thoughts on the subject.

Several vulnerability concerns emerged as listed below:

- more reliance on computer networks and telecommunication systems not designed for secure operations;
- control systems (including SCADA) using commercial off-the-shelf hardware and software;
- proliferation of modems;
- sabotage of critical parts and difficulty of replacement;
- insufficient effort to correct previously identified physical security vulnerabilities; and
- availability of vulnerability information.

As stated in the Commission's report, interdependencies were a key concern of the energy sector. "The security, economic prosperity, and social well being of the US depend on a complex system of interdependent infrastructures. The life blood of these interdependent infrastructures is energy ... [3]." The power outages of July and August 1996 in the western United States clearly demonstrated the extensive impact to all of the other critical infrastructures. Telecommunications, water supply systems, transportation, emergency services, government services, and banking were all significantly affected by the blackouts, which covered most of that region.

### 3.5 The Nature of Interdependencies

The Commission dealt with interdependencies as an integral part of the work of each infrastructure group. The final report did not deal with the subject separately but did recognize the overarching importance in connection with several strategic objectives and policy initiatives.

There are two main sources of interdependency: geographic proximity (in which an attack on one element causes damage to proximate elements of other infrastructures) and functional interdependency (in which other infrastructure elements depend on the functioning of the attacked element in order to perform adequately). One of the most serious concerns due to the interdependencies among infrastructures is that the effects of an attack on one might, under certain conditions, cause cascading failures among other infrastructures, which in turn might amplify the effect on the originally attacked infrastructure and cause disproportionately high levels of damage on a wide geographic and functional scale. It is unlikely that an adversary would unknowingly choose such a critical target; however, the potential consequences call for special protective efforts for those specific assets.

It became clear to the Commission that the degree of interdependency throughout the critical infrastructures was much higher than was first apparent on the surface. Energy and communications/information clearly underlie virtually everything else. But, in fact, significant outages in any of the critical infrastructures could be expected to seriously affect at least several other infrastructures. While the initial effects of a particular attack would be localized to the target assets, the degree of interconnectedness would, in many cases, lead well beyond the initial locale. The specific consequences of an event would be a function of the detailed nature of the interdependencies on an enterprise level.

In addition to noting the extensive nature of interdependencies among the critical infrastructures, and therefore the need for wide-ranging partnership between government

and many elements of the private sector, the Commission considered a number of specific examples of interdependencies. For example, the loss of electric power would prevent the pumps at gasoline stations from operating, which would prevent vehicles from delivering products and services, which would cripple other infrastructure services and hamper repairs to the electric power infrastructure, thus compounding the cycle of consequences.

During its limited life, the Commission was not able to delve more deeply into the nature and characterization of failure modes through interdependencies. It was clear that the real failure events unfolded through the effects on specific interdependent individual enterprises. That realization, however, would not lead to a generalized approach to understanding the phenomenon. On the other hand, integrating or averaging over entire sectors could provide a more workable approach because data would be more readily available, but would lose the reality of what actually causes the interlinked failures, and thus would likely lead to incorrect conclusions. Moreover, an averaged approach would not illuminate specific needs for protective measures. This clearly was an area in need of more research.

### 3.6 Partnership between Government and Industry

The Commission noted as a fundamental requirement that a wide-ranging partnership among governmental organizations and industrial entities was key to the success in protecting the nation's critical infrastructures for the following reasons:

- the infrastructure enterprises were largely owned and/or operated by the private sector;
- the owners/operators were in a better position to assess their vulnerabilities and design protective measures;
- the large-scale consequences of an event affect the broad community, beyond the specific business responsibilities of the infrastructure enterprise;
- the government has regulatory and law enforcement responsibilities and authority and can also provide a mechanism for spreading the risk/costs; and
- the government can bring unique resources, such as intelligence and analysis capabilities, as well as diplomacy, to bear.

The Commission identified seven specific areas of responsibility for the owners/operators of critical infrastructure (paraphrased here):

1. provide and manage the assets needed to ensure the delivery of infrastructure services efficiently and effectively;
2. meet customer expectations for quality and reliability;
3. manage risks effectively:
   (a) identify threats and vulnerabilities,
   (b) mitigate risks cost-effectively,
   (c) maintain emergency response and management capability;
4. give special consideration to vulnerabilities in information systems;
5. cooperate with others in the sector to identify the best reliability and security practices;

6. report criminal activities to law enforcement and cooperate with investigations;and
7. build working relationships with intelligence and law enforcement.

State and local governments play several roles: regulation, law enforcement, administration of justice, response to incidents, and ownership/operation of certain infrastructures.

The federal government has overarching responsibilities for national security, public health and safety, and the general welfare of the nation. Thus, unique resources are available, such as collection and analysis of intelligence, training and equipment for first responders, and relations with other countries and international organizations.

The Commission recommended the establishment of national structures to facilitate the partnership and to address matters of policy formulation, planning for critical infrastructure protection, and the design and implementation of specific programs. The pros and cons were weighed for establishing a new department to protect the nation's critical infrastructures, but it was decided that the political costs and barriers would render such a recommendation impossible to implement. Instead, the Commission recommended a small office in the White House (called the Critical Infrastructure Assurance Office [CIAO]) located in the Department of Commerce. In the aftermath of the terrorist attacks of September 11, 2001, the government did establish the Department of Homeland Security (DHS) with responsibilities that encompass most of the elements of critical infrastructure protection. These functions have been transferred to the DHS.

Each of the infrastructure sectors was to have a lead government agency that would be responsible for identifying and working with sector coordinators from within the infrastructure community and for ensuring that the sector was tied in to the entire government activity in critical infrastructure protection.

The indispensable step to establishing the partnership is ***information sharing***. Chapter 5 of the PCCIP report, *Establishing the Partnership*, discusses the reluctance of private sector entities to share sensitive information with the government because of their concern about the government's inability to protect the information. To address this concern, the Commission recommended that the government establish appropriate measures to protect private sector information. Also, the private sector noted that the limited information available from the government (e.g., specific threat information). However, on the other hand, elements of the government were frustrated by the perceived lack of information flow from the private sector.

Among the innovative mechanisms recommended by the Commission was the establishment of Information Sharing and Analysis Centers (ISACs) in each sector. Their primary functions were

- to provide a forum for the infrastructure enterprises to share information and experiences concerning threats to and vulnerabilities of their sector as well as various problems encountered and possible solutions and
- to provide a mechanism for the federal government to disseminate information and advice throughout the sector.

Another innovative suggestion was that communication and cooperation among the ISA Cs could be very helpful in identifying and dealing with sector interdependencies. ISACs have now been established in most of the critical infrastructure sectors with varying results. It is a valuable mechanism that is still evolving in its implementation. However, the private sector business model has only worked for a few of

them. All of the new sectors and some of the PDD 63 sectors no longer have ISACs. Most of them did have the capacity to do real analysis but acted as "pass-throughs" for information. Now each sector coordinating council (which replaced the PDD 63 sector coordinator) has the option to identify an ISAC to be their sector information sharing mechanism.

### 3.7 Risks in the Information Age

The Commission anticipated that the threat of cyber attacks would grow rapidly to become a dominant concern for infrastructure assurance. The increasing reliance of all the nation's sectors on the information and communications infrastructure suggested that one of the major risks would soon be that of a cyber attack. Such an attack would cause extraordinary damage and loss of capability through large-scale interdependencies with devastating effects on the United States.

While the direction of the threat trend was correctly predicted, it has not yet reached the magnitude or urgency foreseen. The major threats to critical infrastructure remain physical—mostly kinetic—attacks. As an instrument of terror, an explosion is far more impressive than a cyber attack. When the attackers turn toward creating economic impacts instead of terrorizing populations, the role of cyber threats will undoubtedly increase.

## 4 PRESIDENTIAL DECISION DIRECTIVE 63 OVERVIEW

PDD 63 institutionalized many of the recommendations from the PCCIP report [3]. Initially, PDD 63 noted a "growing potential vulnerability" and stated that "[m]any of the nation's critical infrastructures have historically been physically and logically separate systems that had little *interdependence*. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and *interlinked*" [4].

PDD 63 set a national goal that "any interruptions or manipulations of these critical infrastructures must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States" [5].

The President directed elements of the federal government to implement activities and encouraged the private sector to take steps to improve the protection of the US critical infrastructures as reported on by the PCCIP. The following three sections summarize his direction.

### 4.1 Federal Government

PDD 63 established an organizational structure within the Executive Branch of the federal government to implement the Directive. Lead agencies were designated for each critical infrastructure with an appointed sector liaison official, as well as lead agencies and officials for special functions (national defense, foreign affairs, intelligence, and law enforcement). Also established was the position of national coordinator to chair an interagency group (Critical Infrastructure Coordination Group) to coordinate the overall implementation activities. The national coordinator would be supported by the National Plan coordination staff (Table 1).

To strengthen the protection of critical infrastructures within the jurisdiction of the federal government, each department/agency was directed to appoint a senior-level official

**TABLE 1 Presidential Directive Directive 63 Federal Government Organization, Annex A**

**National Coordinator**—Chair of Critical Infrastructure Coordination Group and supported by National Plan Coordination staff

| **Lead Agency** | **Sector Liaison** |
|---|---|
| Commerce | Information and communications |
| Energy | Electric power |
| | Oil and gas production and storage |
| Environmental Protection Agency | Water supply |
| Federal Emergency Management Administration | Emergency fire services<br>Continuity of government services |
| Health and Human Services | Public health services, including prevention, surveillance, laboratory services, and personal health services |
| Justice/FBI | Emergency law enforcement services |
| Transportation | Aviation, Highways, Mass transit, Pipelines, Rail, Waterborne commerce |
| Treasury | Banking and finance |
| **Lead Agency** | **Special Functions** |
| Central Intelligence Agency | Foreign intelligence |
| Defense | National defense |
| Justice/FBI | Law enforcement and internal security |
| State | Foreign affairs |
| Office of Science and Technology Policy | R&D coordination |

to be the Critical Infrastructure Assurance Officer. The existing Chief Information Officer would be responsible for information assurance, while the Critical Infrastructure Assurance Officer would be responsible for protecting all other aspects of the department's/agency's critical infrastructure. To facilitate gathering of threat information and rapid distribution of such information, "the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC) [6]."

### 4.2 Private Sector

For the private sector, a National Infrastructure Assurance Council was to be established. It consisted of "a panel of major infrastructure providers and state and local government officials" appointed by the President to provide him advice. Periodic meetings were "to be held to enhance the partnership of the public and private sectors" [7]. Subsequently, the Council was established as the National Infrastructure Advisory Council by Executive Order 13231, and amended by EO 13286 and EO 13385.

A private-sector coordinator to represent each sector was to be identified as the counterpart to the federal government's sector liaison official.

Owners/operators were "strongly encouraged" to create ISACs. "Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC" [8].

### 4.3 Research and Development

The Directive established a formal R&D program with guidelines and specific tasking.

- *Section V, Guidelines.* "The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection."
- *Section VIII, Tasks.* The President requested the Principal's Committee to submit to him a National Infrastructure Assurance Plan with milestones. R&D was one of the subordinate and related tasks:
  - "*Research and Development*: Federally sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable."
- *Annex A, Structure and Organization.* "In addition, OSTP (*Office of Science and Technology Policy*) shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council."

### 4.4 Problems and Major Shortfalls of PDD 63

***4.4.1 Lack of Partnership.*** There was significant resistance to the new concept of Critical Infrastructure Protection, both in the private sector and in many elements of the government. Also, many government departments and agencies were not familiar with the concept of a partnership with the private sector. Building the "partnership" would be a long-term process that would need to be developed over time (years), starting with personal relationships established on trust, followed by awareness and education efforts, and the active participation of partners with leadership skills with the ability to focus on outcomes of mutual benefit.

The Directive was promulgated with minimal collaboration between the government and private sector. PDD 63 was written within the federal government. A senior official in the NSC led the effort to draft the document, relying on their support organization and an interagency group of senior representatives selected from the agencies involved.

There was a need to stimulate dialogue across and within particular infrastructure sectors to drive and accelerate more collaboration on critical infrastructure thinking within infrastructure sector leadership. Part of the challenge is that many sectors had not previously engaged in critical infrastructure dialogues among themselves to consider opinions and develop conclusions toward their approach to critical infrastructure. While PDD 63 encouraged such efforts, little was done to bring together the leadership to stimulate such efforts. Fortunately, both the CIAO and the Partnership for Critical Infrastructure Security (PCIS) caused much of the internal sector dialogues to begin, though these successes took several years to begin consolidating effectively.

Similarly, once a dialogue began within a particular sector, it took further effort (and time) to generate trusted dialogue between that sector and government. In some cases, this dialogue moved ahead very effectively while in some sectors, it still struggles a decade after the PCCIP. Further, many superb efforts are driven primarily by several very effective individuals leading their particular sector, though broad acceptance and understanding of CIP issues remain a challenge—thus, if that person ceased driving

leadership, many initiatives could potentially fade or be weakened. The need for sector CIP dialogues was vitally important at three levels: (i) within and across the sector; (ii) between the sector and other sectors, many of which had interdependent elements; and (iii) between the sector and government. While PDD 63 was ineffective in successfully achieving these ends, the CIAO and PCIS made significant strides prior to the establishment of DHS.

***4.4.2 Lack of Resources for Implementation.*** To initiate a new program, the departments and agencies realized that the resources had to be taken out of existing funds. No new funds were available! Although the agencies submitted budget requests through their normal channels, and they were accepted by the Office of Management and Budget to some extent, the White House did not develop or present a unified set of supporting arguments to the congressional oversight committees involved. Because of the need to make Congress aware of the critical infrastructure issues and concerns, there was no clear idea of the need or magnitude of the undertaking. Thus, the implementation of PDD 63 began with a long-term effort of awareness and education. A key lesson learned in the government sphere is that central coordination of a distributed program is an essential element in its success.

***4.4.3 Lack of Emphasis on Interdependencies.*** Even though interdependencies were stressed throughout the PCCIP report, PDD 63 gave it minimal emphasis. The most significant reference came at the end of Section IV: "During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies" [9]. No single agency or department was given a lead role for interdependencies.

Interdependency was one example of a crosscutting issue that could have been addressed by the Critical Infrastructure Coordination Group. However, the "unfunded mandate" problem made performance of the sector lead agency responsibilities too spotty and inconsistent to allow the different agencies to work on common issues.

## 5 CASE AND STRATEGY FOR ACTION IN TERMS OF INFRASTRUCTURE INTERDEPENDENCIES

The tremendous explosion of technologies, including computers, processing, and communications processes, led to a complex mosaic of technology in every infrastructure sector. The reliance on other infrastructures continued to grow, led in large part by a markedly increased reliance on communications and control systems, providing signals and feedback mechanisms by which infrastructures are monitored and operated to include an expanded range of remote operations. Although experts in each of these processes are fluent as to how their particular systems interact dynamically to control and operate segments of the infrastructure, their insights are often limited to the narrow scope of their particular system or functional role. With the expanded complexity of technology, individual infrastructure sectors have advanced modeling and simulation processes that can mimic and, in some cases, function predictively in the operational control of an infrastructure sector, especially in localized or regional operations. However, it becomes far

more difficult for managers and decision makers to fully understand the broad range of detailed interactions and nuances by which their entire infrastructure functions technologically and operationally, especially during crises or emergency scenarios where dynamic changes occur more rapidly within the sector. This challenge becomes even greater when the scope of interdependencies upon other infrastructure sectors is considered.

Each infrastructure sector's consideration of critical infrastructure issues has advanced at its own pace; some sectors are further along the path of understanding and are taking appropriate actions to better assure resilience, recoverability, and robustness. This disparity becomes more obvious as we consider infrastructure outage events that occur periodically during any given year. In some cases, a sector's response is impressively swift, mitigating the damaging effects of an outage and accelerating a return-to-normal operation. In other cases, a flawed response leads to open criticism, causing either governmental or privately led efforts to force improvements in emergency response-and-recovery processes and driving greater investments toward greater assurance of acceptable sector performance. The point is that different sectors, and sometimes varying management elements within the same sector, often are at different levels of technological and operational maturity in the understanding and response within their sector. This is further exacerbated when the issue of infrastructure interdependency is considered.

Even sectors with mature processes for operations and recovery often have given limited consideration to developing predictive means for assessing their systematic reactions to emergency events occurring in other sectors on which they rely. In their defense, given (i) the difference in modeling and simulation maturity within each sector; (ii) the reliance on different and often incompatible technologies; and (iii) the variety of signal and protocol formats, the interoperability of modeling processes between infrastructure sectors is both complex and very limited. Furthermore, the best way to coordinate the operations among multiple infrastructures is often through leveraging preexisting relationships among the leaders, managers, and operators of those separate infrastructures.

The more interdependent our infrastructures become—and their interdependence continues to grow year after year—the more urgent it becomes for our nation and its critical infrastructure owners/operators to more thoroughly consider critical infrastructure interdependencies. Operational processes, service-level agreements, emergency response systems, and organizational interactions and procedures must better address interdependencies to assure critical infrastructure protection. To do so will require many types of investments to help assure critical infrastructure performance for the future.

## 6 SUMMARY OF COMMISSION'S CONCLUSIONS ON RESEARCH AND DEVELOPMENT NEEDS

Consistent with the scope of its charter and in recognition of the importance of interdependencies, the Commission addressed R&D needs not only for the eight specific infrastructures identified in Executive Order 13010, but also explicitly for the crosscutting interdependency issues that affect more than one infrastructure. The goal was to provide a road map for the development of technologies that will counter threats (physical, cyber, and other threats that arise from the complexity of automated systems and from increasing interdependencies among infrastructures) and reduce the vulnerabilities in those areas with the potential for causing "significant" national security, economic, and/or social impacts.

Basic research requiring long-term government investment was emphasized. However, it was recognized that this research must be accompanied by the development of technology within the private sector. As broadly defined by the Commission, technology includes processes, systems, models and simulations, and hardware and software. Strong involvement from infrastructure owners/operators was deemed essential to ensure the development of useful and usable products.

The Commission concluded that federal R&D efforts were inadequate for the size of the R&D challenge presented by emerging cyber threats. They further noted that real-time detection, identification, and response tools were urgently needed and that R&D for infrastructure protection requires partnership among government, industry, and academia to ensure a successful and focused research and technology development effort.

The Commission proposed a substantial increase in federal investment in infrastructure assurance research, targeting R&D and focusing on six R&D areas:

1. *Information assurance.* Assurance of vital information is increasingly a key component for the functioning of our interdependent infrastructures. The urgent need to develop new, affordable means of protection is apparent, given the increasing rate of incidents, the expanding list of known vulnerabilities, and the inadequate set of solutions available.
2. *Intrusion monitoring and detection.* Reliable automated monitoring and detection systems, timely and effective information collection technologies, and efficient data reduction and analysis tools are needed to identify and characterize structured attacks against infrastructure.
3. *Vulnerability assessment and systems analysis.* Advanced methods and tools for vulnerability assessment and systems analysis are needed to identify critical nodes within infrastructures, examine interdependencies, and help understand the behavior of these complex systems. Modeling and simulation tools and test beds for studying infrastructure-related problems are essential for understanding the interdependent infrastructures.
4. *Risk management decision support.* Decision support system methodologies and tools are needed to help government and private-sector decision makers effectively prioritize the use of finite resources to reduce risk.
5. *Protection and mitigation.* Real-time system control, infrastructure hardening, and containment and isolation technologies are needed to protect infrastructure systems against the entire threat spectrum.
6. *Incident response and recovery.* A wide range of new technologies and tools is needed for effective planning, response, and recovery from physical and cyber incidents that affect critical infrastructures.

The fundamental R&D issue for critical infrastructure protection was framed by the Commission in terms of three interrelated questions:

- What R&D is needed to achieve the nation's infrastructure assurance objectives?
- What level of corresponding investment is required?
- Who should make this investment?

These questions remain relevant and must be answered within a partnership between government and the private sector. The Commission noted that both entities must recognize that (i) infrastructure assurance risks cut across the public and private sectors; (ii) the private sector holds much of the relevant technical and empirical data on infrastructure operations, vulnerabilities, and interdependencies; and (iii) the private sector develops technology only when it identifies a market for it. The Commission concluded that successful implementation of technologies developed from government-funded research efforts requires close cooperation from private-sector owners and operators of our nation's infrastructures.

## 7 CLOSING STATEMENT

The PCCIP set the stage and Presidential Decision Directive 63 initiated the path forward. As stated in the *Onward* section of the PCCIP report—the Commission's effort was "the prologue to a new era of infrastructure assurance (p. 101)."

## REFERENCES

1. (a) Congress of the United States, Office of Technology Assessment (1990) *Physical Vulnerability of Electric Systems to Natural Disasters and Sabotage*, OTA-E-453, (NTIS order #PB90-253287, GPO stock # 052-003-01197-2) (June 1990); see also (b) Charles, L., *Draft Report for the Committee on Government Affairs*, US∼Senate hearings.
2. *The White House (1989). Vulnerability of Telecommunications and Energy Resources to Terrorism*, Hearings before the Committee on Government Affairs, U.S. Senate, One Hundred First Congress, First Session, S. Hrg 101-73 (Feb. 7–8, 1989).
3. The White House (1997). President's Commission on Critical Infrastructure Protection, *Critical Foundations—Protecting America's Infrastructures*, Appendix A, p. A-24 (October 1997).
4. The White House (1998). Presidential Decision Directive-63, Section I, *A Growing Potential Vulnerability* (May 1998).
5. The White House (1998). Presidential Decision Directive-63, Section III, *A National Goal* (May 1998).
6. The White House (1998). Presidential Decision Directive-63, Annex A, *Warning and Information Centers* (May 1998).
7. The White House (1998). Presidential Decision Directive-63, Section VI-4, *National Infrastructure Assurance Council* (May 1998).
8. The White House (1998). Presidential Decision Directive-63, Annex A, *Information Sharing and Analysis Center (ISAC)* (May 1998).
9. The White House (1998). Presidential Decision Directive-63, Section IV, *A Public-Private Partnership to Reduce Vulnerability* (May 1998).

## FURTHER READING

Brown, K. A. (2006). *Critical Path: A Brief History of Critical Infrastructure Protection in the United States*. George Mason University Press, Arlington, VA.

The White House (1998). *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, White Paper (May 22, 1998).

# INPUT–OUTPUT MODELING FOR INTERDEPENDENT INFRASTRUCTURE SECTORS

JOOST R. SANTOS AND YACOV Y. HAIMES
*Center for Risk Management of Engineering Systems, University of Virginia, Charlottesville, Virginia*

## 1 BACKGROUND: LEONTIEF INPUT–OUTPUT MODEL

No literature survey on interdependency analysis is complete without mentioning the input–output (I–O) model, for which Wassily Leontief received the 1973 Nobel Prize in Economics. This model is useful for studying the effects of consumption shocks on interdependent sectors of the economy [1, 2]. Miller and Blair [3] provide a comprehensive introduction of the model and its applications. Leontief's I–O model describes the equilibrium behavior of both regional and national economies [4, 5] and presents a framework capable of describing the interactive nature of economic systems. Extensions and current frontiers of I–O analysis can be found in Lahr and Dietzenbacher [6] and Dietzenbacher and Lahr [7]. It is worth noting that the traditional use of input–output analysis for estimating the effects of economic shifts (e.g. changes in consumption) has been extended to other applications, such as disaster risk management, environmental impact analysis, and energy consumption, among others. Various studies for estimating losses pursuant to disasters have employed traditional I–O analysis and extended approaches such as computable general equilibrium (CGE) models. Rose and Liao [8] conducted a case study of water-supply disruption scenarios in Portland using CGE to account for resilience factors (e.g. substitution and conservation) that business sectors typically consider in order to minimize potential losses. (Note that Rose [9] states that CGE is an extension rather than a replacement of the traditional I–O model). Cho et al. [10] identified the I–O model as a useful tool for estimating the economic costs associated with major earthquakes in urban areas. Lenzen et al. [11] implemented a multiregion environmental input–output analysis to determine $CO_2$ multipliers based on international trade data for commodities that emit greenhouse gas by-products. Alcántara and Padilla [12] developed an I–O-based methodology that considers energy demand elasticities for determining the key sectors that are involved in the final consumption of energy.

The formulation of the basic Leontief I–O model is shown in Eq. (1). The notation $x_i$ refers to the total production output of industry $i$. The Leontief technical coefficient $a_{ij}$ indicates the ratio of the input of industry $i$ to industry $j$, with respect to the total production requirements of industry $j$. Thus, given $n$ industries, $a_{ij}$ can tell the distribution of inputs contributed by various industries $i = 1, 2, \ldots, n$ to the total inputs required by industry $j$. Finally, the notation $c_i$ refers to the final demand for the $i^{th}$ industry—the portion of industry $i$'s total output for final consumption by end users (i.e. the excess of all intermediate consumptions by various industries $j = 1, 2, \ldots, n$).

$$\mathbf{x} = \mathbf{A}\mathbf{x} + \mathbf{c} \Leftrightarrow \left\{ x_i = \sum_j a_{ij} x_j + c_i \right\} \forall\, i \tag{1}$$

## 2 INOPERABILITY INPUT–OUTPUT MODEL (IIM)

Today, the infrastructure sectors in the United States (and the entire global economy) are highly interdependent—making them more vulnerable to natural- and human-caused disruptive events. Such events upset the "business-as-usual" production levels of the affected systems and lead to a variety of economic losses, such as demand/supply reductions. Interdependency analysis applies to ripple effects triggered by various sources of disruption, including terrorism, natural calamities, and accidents, among others.

On the basis of Leontief's work, Haimes and Jiang [13] developed the inoperability input–output model (IIM) for interconnected systems. One of the metrics offered by the IIM is *inoperability*, which is defined as the inability of a system to perform its intended functions. In the IIM, inoperability can denote the level of the system's dysfunction, expressed as a percentage of the system's intended production level. Inoperability can be caused by internal failures or external perturbations, which adversely affect the delivery of a system's intended output. The IIM was later expanded by Santos and Haimes [14] to quantify the economic losses triggered by terrorism and other disruptive events to economic systems (or industry sectors). The analysis of economic impacts associated with such events is made possible through the economic I–O data published by the Bureau of Economic Analysis (BEA) [15, 16].

The formulation of the IIM is as follows:

$$\mathbf{q} = \mathbf{A}^*\mathbf{q} + \mathbf{c}^* \tag{2}$$

The details of model derivation and an extensive discussion of model components are found in Santos and Haimes [14]. In a nutshell, the terms in the IIM formulation in Eq. (2) are defined as follows:

- $\mathbf{q}$ is the inoperability vector expressed in terms of normalized economic loss. The elements of $\mathbf{q}$ represent the ratio of unrealized production (i.e. "business-as-usual" production minus degraded production) with respect to the "business-as-usual" production level of the industry sectors.
- $\mathbf{A}^*$ is the interdependency matrix, which indicates the degree of coupling of the industry sectors. The elements in a particular row of this matrix can tell how much additional inoperability is contributed by a column industry to the row industry.
- $\mathbf{c}^*$ is a demand-side perturbation vector expressed in terms of normalized degraded final demand (i.e. "business-as-usual" final demand minus actual final demand, divided by the "business-as-usual" production level).

Previous IIM-based works on infrastructure interdependencies and risks of terrorism include Haimes [17], Jiang and Haimes [18], Crowther and Haimes [19], Haimes et al. [20, 21], Lian and Haimes [22], and Santos [23]. Other quantitative research on modeling terrorism risks has emerged in recent years because of sustained threats to homeland security. Apostolakis and Lemon [24] proposed the use of graph theory for modeling infrastructure interconnectedness and employed multiattribute utility theory for setting priorities to vulnerabilities. Paté-Cornell and Guikema [25] employed probabilistic risk analysis (PRA), decision analysis, and game theory for prioritizing vulnerabilities and their associated countermeasures. Bier and Abhichandani [26] proposed a game theory approach to model the way defenders and offenders determine optimal strategies for achieving their respective objectives of protecting or destroying a system.

## 3 APPLICATIONS OF THE IIM

This section discusses representative applications of the IIM that resulted from three government-commissioned projects: (i) high-altitude electromagnetic pulse (HEMP) impact on interconnected sectors; (ii) economic impact of homeland security advisory system (HSAS) threat levels; and (iii) Virginia Department of Transportation (VDOT) interdependencies.

### 3.1 High-Altitude Electromagnetic Pulse (HEMP) Impact on Interconnected Sectors

HEMP is defined as intense electromagnetic blasts induced by high-elevation nuclear explosions, which can potentially cause damage to electronic and electrical systems. National- and regional-level case studies have been conducted in this study to analyze the impacts of HEMP on the electric power, electromagnetic pulse (EMP) vulnerable equipment, workforce, and health services sectors. The EMP Commission's guidance has been solicited to generate the perturbation scenarios employed in the case studies. Systemic parametric and sensitivity analyses of HEMP attack scenarios are achieved via consideration of various sources of uncertainties relating to (a) geographic scope and detail (e.g. national versus regional); (b) intensity of perturbation to an initial set of affected sectors (e.g. electric power, EMP-vulnerable equipment, and workforce); and (c) temporal characteristics surrounding sector recoveries (e.g. 60-day versus 1-year recovery rates). Trade-off analyses have been performed to analyze the effectiveness of resource allocation strategies associated with restoring diversely affected sectors. Recommendations from this study include developing cost-benefit-risk-balanced policies and solutions for managing disruptions and expediting recovery time from potential terrorist attacks [see [16] for details]. For a 60-day exponential electric power outage in the Greater Northeastern Region (GNR), as shown in Figure 1, the resulting direct and indirect sector impacts were ranked and classified according to two types of metrics: economic loss and inoperability. Approximately $14 billion in losses are incurred for this scenario, of which about 80% is realized within the first 20 days.

### 3.2 Economic Impact of Homeland Security Advisory System (HSAS) Threat Levels

The IIM was used to estimate the economic impact of heightened HSAS threat levels and the corresponding courses of actions relating to the period of implementation and the regional scope of the alert. A system for generating the direct-sector impacts associated with various HSAS courses of actions was developed, along with a process for visualizing the results. Parametric analyses were conducted to address critical factors, such as impacted sectors, nature of impact (productivity loss versus demand reduction), and duration of effects. Input–output datasets for the Greater New York Metropolitan Region and the Newark Statistical Area (a subset consisting of six counties contiguous to Newark) were obtained from the BEA. These datasets enabled us to estimate the magnitude of economic impacts associated with the specified HSAS scenarios. National IIM analysis was also implemented to estimate the psychological response of the general public to HSAS alert modifications. In particular, we studied the sensitivity of recreation and other discretionary sectors to demand reductions potentially caused by increasing alert levels. The results show that economic repercussions of a red alert are large and are highly sensitive to the definition of nonessential businesses (i.e. discretionary vs. fundamental

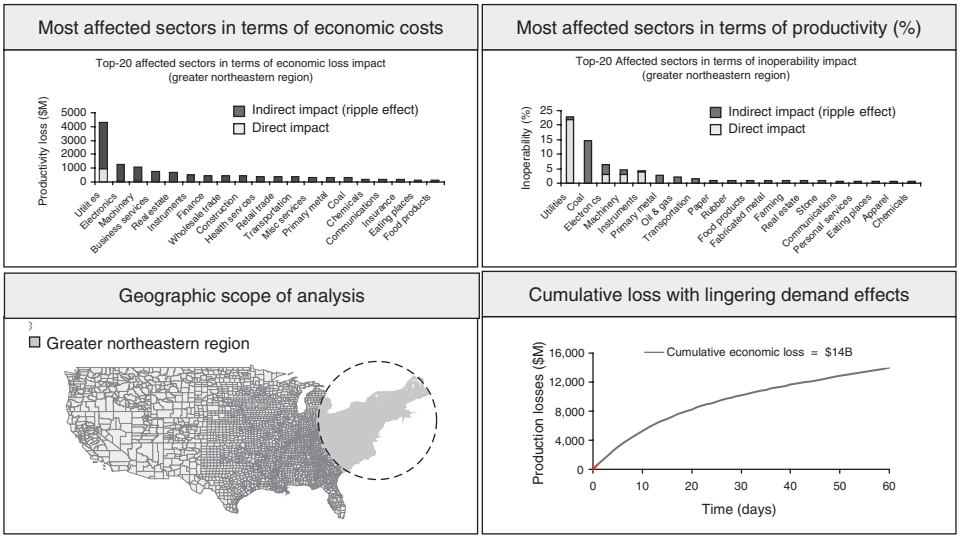



**FIGURE 1** Sample IIM results for a regional HEMP attack scenario.

sectors). On the basis of the assumption that approximately 10% of the businesses are nonessential, red alerts would likely result in $210 billion losses for the nation, $50 billion for the Greater New York Metropolitan Region, and $6.3 billion for the Newark Statistical Area. These losses are based on a one-week red alert followed by one year of consumption losses due to lingering public fear. Lingering demand effects have substantial economic impacts and should not be ignored—IIM results indicate that these losses are approximately 3 times the losses incurred during the first week of a red alert. Also, losses incurred in smaller regions are proportionately higher compared to overall domestic production. This observation may be attributable to the greater effort required to manage security and/or more focused public reaction when the red alert is local.

### 3.3 Virginia Department of Transportation (VDOT) Interdependencies

The transportation network, being a lifeline infrastructure, is designed to support other infrastructures and systems. This symbiotic relationship creates vulnerabilities that affect not only the highway system but also all other systems dependent on transportation modes and facilities. The IIM was used for modeling and analysis of transportation interdependencies, which requires investigation of various transportation elements, such as road network structure, flow, and capacity, as well as the type of economic activities they support [27]. Mobility is an important aspect of recovery and can be assured through availability of transportation modes and facilities. Furthermore, workforce mobility is an important consideration during recovery to ensure uninterrupted availability of essential services other than transportation (health care, food supply, electric power, communication, etc.). The focus of the case study is to understand how a terrorist attack (or other disruption) on a highway system element (bridge, overpass, tunnel, road, etc.) propagates to other physical and economic sectors within Virginia and its contiguous region, so that management policies can be implemented to reduce the consequences of the event. These sectors include utilities, commerce, communication, and providers of basic necessities (food, water, and health care), among others.

## REFERENCES


1. Leontief, W. W. (1951a). *Input–Output Economics*. Scientific American, pp. 15–21.
2. Leontief, W. W. (1951b). *The Structure of the American Economy, 1919–1939: An Empirical Application of Equilibrium Analysis*, 2nd ed., International Arts and Sciences Press, New York.
3. Miller, R. E., and Blair, P. D. (1985). *Input–Output Analysis: Foundations and Extensions*. Prentice-Hall, Englewood Cliffs, NJ.
4. Isard, W. (1960). *Methods of Regional Analysis: An Introduction to Regional Science*. MIT Press, Cambridge, MA.
5. Lahr, M. L., and Stevens, B. H. (2002). A study of regionalization in the generation of aggregation error in regional input-output models. *J. Reg. Sci.* **42**, 477–507.
6. Lahr, M. L., and Dietzenbacher, E. (2001). *Input–Output Analysis: Frontiers and Extensions*. Palgrave, New York.
7. Dietzenbacher, E., and Lahr, M. L. (2004). *Wassily Leontief and Input–Output Economics*. Cambridge University Press, Cambridge.
8. Rose, A., and Liao, S. (2005). Modeling regional economic resilience to disasters: a computable general equilibrium analysis of water service disruptions. *J. Reg. Sci.* **45**, 75–112.
9. Rose, A. (2004). Economic principles, issues, and research priorities in hazard loss estimation. In *Modeling Spatial and Economic Impacts of Disasters*, Y. Okuyama, and S. Chang, Eds. Springer-Verlag, New York, pp. 13–36.
10. Cho, S., Gordon, P., Moore, J. E. II, Richardson, H. W., Shinozuka, M., and Chang, S. (2001). Integrating transportation network and regional economic models to estimate the costs of a large urban earthquake. *J. Reg. Sci.* **41**, 39–65.
11. Lenzen, M., Pade, L., and Munksgaard, J. (2004). $CO_2$ multipliers in multi-region input-output models. *Econ. Syst. Res.* **16**, 391–412.
12. Alcántara, V., and Padilla, E. (2003). Key sectors in final energy consumption: an input–output application to the Spanish case. *Energy Policy* **31**, 1673–1678.
13. Haimes, Y. Y., and Jiang, P. (2001). Leontief-based model of risk in complex interconnected infrastructures. *J. Infrastruct. Syst.* **7**, 1–12.
14. Santos, J. R., and Haimes, Y. Y. (2004). Modeling the demand reduction input–output (I–O) inoperability due to terrorism of interconnected infrastructures. *Risk Anal.* **24**, 1437–1451.
15. Bureau of Economic Analysis (BEA). (1997). *Regional Multipliers: A User Handbook for the Regional Input-Output Modeling System (RIMS II)*. US Department of Commerce, Washington, DC.
16. Bureau of Economic Analysis (BEA). (1998). *Benchmark Input-Output Accounts of the United States for 1992*. US Department of Commerce, Washington, DC.
17. Haimes, Y. Y. (2004). *Risk Modeling, Assessment, and Management*, 2nd ed. John Wiley & Sons, New York.
18. Jiang, P., and Haimes, Y. Y. (2004). Risk management for Leontief-based interdependent systems. *Risk Anal.* **24**, 1215–1229.
19. Crowther, K. G., and Haimes, Y. Y. (2005). Application of the inoperability input–output model (IIM) for systemic risk assessment and management of interdependent infrastructures. *Syst. Eng.* **8**, 323–341.
20. Haimes, Y. Y., Horowitz, B. M., Lambert, J. H., Santos, J. R., Lian, C., and Crowther, K. G. (2005a). Inoperability input-output model (IIM) for interdependent infrastructure sectors: theory and methodology. *J. Infrastruct. Syst.* **11**, 67–79.
21. Haimes, Y. Y., Horowitz, B. M., Lambert, J. H., Santos, J. R., Crowther, K. G., and Lian, C. (2005b). Inoperability input-output model (IIM) for interdependent infrastructure sectors: case study. *J. Infrastruct. Syst.* **11**, 80–92.

22. Lian, C., and Haimes, Y. Y. (2006). Managing the risk of terrorism to interdependent infrastructure systems through the dynamic inoperability input-output model. *Syst. Eng.* **9**, 241–258.
23. Santos, J. R. (2006). Inoperability input-output modeling of disruptions to interdependent economic systems. *Syst. Eng.* **9**, 20–34.
24. Apostolakis, G. E., and Lemon, D. M. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Anal.* **25**, 361–376.
25. Paté-Cornell, M. E., and Guikema, S. (2002). Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. *Mil. Oper. Res.* **7**, 5–20.
26. Bier, V. M., and V. Abhichandani (2003). Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries. *ASCE Proc. Risk Based Decisionmaking Resour.* **10**, 59–76.
27. Haimes, Y. Y., Santos, J. R., and Williams, G. M. (2006). Assessing and managing the inoperability of virginia's interdependent transportation systems. *Int. J. Risk Assessment Manag.* **4**, 489–510.

# APPLICATION OF A CONDITIONAL RISK ASSESSMENT METHODOLOGY FOR PRIORITIZATION OF CRITICAL INFRASTRUCTURE

EDWARD J. HECKER AND YAZMIN SEDA-SANABRIA
*U.S. Army Corps of Engineers, Washington, D.C.*
ENRIQUE E. MATHEU
*U.S. Department of Homeland Security, Washington, D.C.*
JAMES D. MORGESON AND M. ANTHONY FAINBERG
*Institute for Defense Analyses, Alexandria, Virginia*

## 1 INTRODUCTION

The Dams Sector comprises dams, navigation locks, levees, flood damage reduction systems, hurricane protection systems, mine tailings impoundments, and other similar water retention and/or control facilities. There are over 82,000 dams in the United States;

approximately 65% are privately owned and more than 85% are regulated by State Dam Safety Offices. The Dams Sector is a vital part of the nation's infrastructure, and continually provides a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, flood control, and recreation. The potential impacts associated with damage or destruction of dams could include significant loss of life, massive property damage, and severe long-term consequences. Many of these infrastructures were built before man-made threats were recognized as a possibility and their implications were fully understood. While many differences exist between the needs of individual dam owners and operators, the Dams Sector shares a collective goal of incorporating appropriate and practical protective measures to improve awareness, prevention, protection, response, and recovery. Meaningful assessment of risks and systematic prioritization of risk mitigation measures are critical elements to accomplish this goal.

## 2 RISK METHODOLOGY COMPARISON STUDY

In 2006, the US Army Corps of Engineers (USACE) initiated a risk methodology comparison study for civil infrastructure projects. The initial phase of this study (see Figure 1) focused on a review of the state-of-practice of critical infrastructure security risk assessments, which could be applied to Corps civil works infrastructure projects. This study [1] identified a significant opportunity for collaboration with other Dams Sector partners, based on a clearer, more comprehensive understanding of requirements for a consistently applied, sector-wide risk assessment approach. The development of a framework that enables a sector-wide risk assessment is the primary goal of the Dams Sector-Specific Agency (SSA) within the Office of Infrastructure Protection in the US Department of Homeland Security (DHS). As a continuation to the comparison study effort, and through the auspices of an interagency agreement between USACE and DHS, the study was further expanded to establish the comparative advantages and limitations of a number of risk assessment methodologies. In this second phase, a technical review led by an external panel of experts was conducted to assess the technical approach and implementation of the selected methodologies.

As a final phase, a select set of owners and operators conducted an analysis of requirements that provided a more detailed understanding of how well each methodology compared to the needs of organizations responsible for assessing security risks. Each of these phases is covered in additional detail below.

### 2.1 Phase 1—Site Assessments

This phase primarily involved a literature review of risk analysis methodologies currently in use for security assessments of critical infrastructure, to assist in the identification of existing state-of-practice approaches with most applicability to dams. The term *state-of-practice* was used to denote those approaches currently in use that can provide useful input to decisions on managing risks associated with various threat scenarios. From this research, a preliminary screening of existing assessment methodologies was conducted and five methodologies were identified for application at two typical USACE projects; a navigation lock and dam, and a combined flood control, hydropower, and

navigation lock project. The five methodologies were: Dam Assessment Matrix for Security and Vulnerability Risk (DAMSVR), developed by the Federal Energy Regulatory Commission; Risk Assessment Methodology for Dams (RAM-D), developed by Sandia National Laboratories; Critical Asset and Portfolio Risk Analysis (CAPRA), developed by the University of Maryland; Reclamation's Risk Quantification Methodology (RRQUM) and Matrix Security Risk Analysis (MSRA), both developed by the US Bureau of Reclamation, and Joint Antiterrorism (JAT) Risk Assessment Methodology, developed by the US Department of Defense (DoD). It must be pointed out that some of these methodologies and approaches have continued evolving over time, and therefore their current versions may show differences with respect to those used in the initial phase of this effort.

Technical teams with representatives from each of the risk assessment methodologies under consideration conducted site assessment visits at select dam sites during the November 2006 time frame. Each team conducted an independent evaluation of the sites, and collected the information required for the application of the corresponding assessment methodology. In advance of the site assessments, each methodology team was provided with the same read-ahead package, consisting of site information and descriptions of the functions and components of the project, including pictures, drawings, and other relevant information. For the purpose of this effort, a definition of threat scenarios was also provided. After the site assessment, each team provided a technical report summarizing the analysis resulting from the application of the risk assessment methodology to each site.

### 2.2 Phase II—Panel Reviews

Phase II was initiated during 2007 by an external panel of experts who reviewed the risk assessment reports and evaluated the application of the corresponding methodologies to the two sites selected for the study. The objective was to establish comparative advantages and limitations of the technical approaches, as well as to identify any challenges encountered during the implementation process.

The panel developed a systematic approach that included a comprehensive set of criteria to evaluate the results arising from Phase I of the study. The criteria established by the panel took into consideration the requirements from the National Infrastructure Protection Plan (NIPP) developed in 2006 [2] and updated in 2009. The NIPP provides a coordinated approach for the protection of critical infrastructure and key resources (CIKR). Other provisions in the NIPP include a risk management framework for systematically combining consequence, vulnerability, and threat information. The 2006 NIPP included specifications for baseline criteria that risk assessment methodologies should meet in order to enable comparative analyses between multiple sectors. The purpose of these baseline criteria was to assist in the use of assessments previously performed by owners and operators. These baseline criteria aimed to ensure that a given methodology is credible and comparable with other methods. The challenge of comparing results from multiple risk methodologies is significant since there is wide variation among methodologies on aspects such as assumptions, comprehensiveness, objectivity, inclusion of threat and consequence considerations, physical and cyber dependencies, and other characteristics.

In addition to the 2006 NIPP baseline criteria, the expert panel considered some additional basic elements that are relevant to the types of infrastructures included within the Dams Sector. These sector-specific considerations were used to augment the 2006 NIPP baseline criteria. Table 1 shows the entire set of criteria used to facilitate the comparative evaluation by the panel.

**TABLE 1 Evaluation Criteria**

**NIPP-related criteria**

1. Is the methodology based on documented risk analysis and security vulnerability analysis?
2. Does it specifically address consequences? Vulnerability? Threat?
3. Does the methodology provide reasonably complete results via a quantitative, systematic and rigorous process that
   (a) provides numerical values for estimated consequences, vulnerability and threat whenever possible, or uses scales when numerical values are not practical?
   (b) specifically addresses both public health and safety and direct economic consequences?
   (c) considers existing protective measures and their effects on vulnerabilities as a baseline?
   (d) examines physical, cyber, and human vulnerabilities?
   (e) applies the worst-reasonable-case standard when assessing consequences and choosing threat scenarios?
   (f) uses threat-based vulnerability assessments?
4. Is the methodology thorough and does it use the recognized methods of the professional disciplines relevant to the analysis?
5. Does it adequately address the relevant concerns of government, the CIKR workforce, and the public?
6. Does the methodology provide clear and sufficient documentation of the analysis process and the products that result from its use?
7. Is the methodology easily understandable to others as to assumptions used, key definitions, units of measurement, and implementation?
8. Does the methodology provide results that are reproducible or verifiable by equivalently experienced or knowledgeable personnel?
9. Is the methodology free from significant errors or omissions so that the results are suitable for decision-making?

**Dams Sector-specific criteria**

1. Is the methodology able to conduct comparisons between assets and comparisons with other sectors?
2. Is the process Six Sigma friendly to allow for trend analysis involving similar structures or regional groupings of structures?
3. Can the methodology be used to identify security and protection measures that will result in quantifiable risk reduction?
4. Will implementation of the methodology result in distinguishing characteristics that can be used for meaningful prioritization and are important for decision-making?
5. Is the theoretical/analytical/mathematical formulation logically sound, consistently carried over across the whole methodology and reasonable/practical in terms of data/input requirements?
6. Does the method clearly identify and consider direct and indirect consequences associated with damage/failure of the facility and/or disruption of its functions? Does it consider potential effects on downstream population (population at risk, number of fatalities, and number of injuries)? Does it consider economic impacts (facility replacement and repair cost, direct property damage, business interruption costs and loss of benefits, emergency response impacts, search and rescue costs, short- and/or long-term environmental remediation and restoration costs, indirect effects on other infrastructure)?

(*continued overleaf*)

**TABLE 1 (*Continued*)**

7. Does the method identify a process for aggregating losses across various consequence types to allow an assessment of the cumulative loss of an attack?
8. Does the method clearly identify and quantify interdependency impacts?
9. Does the method effectively address economic impacts on regional interdependencies as many of these dams affect numerous entities upstream, downstream, and across state lines?
10. Does the threat assessment portion of the methodology have an "intelligence quality" process for identifying, quantifying, and qualifying intelligence and information from both public and private sectors, leading to a formal threat estimate that identifies the most credible threats to a facility, activity, organization, or region?
11. Does the method identify a process for allocating the threat for the entire Dams Sector down to the threat for a specific dam?
12. Does the methodology consider the structural condition and maintenance state of the facility or asset when evaluating the vulnerabilities?
13. Does the methodology consider the response effectiveness (time for arrival of first responders) when evaluating the vulnerabilities, or their effects on their resulting risk?
14. Is the methodology sensitive enough to capture the influence of alternative security/protection/response measures on the vulnerabilities and/or the resulting risk?

In August 2007, the expert panel convened to complete the review of the application of the five methodologies. The panel, facilitated by the Oak Ridge Institute for Science and Education, met for 3 days to share findings arising from their evaluation and to identify desirable features or limitations in current approaches. Results from the discussions were documented; some of the key highlights are as follows:

- The baseline criteria for risk assessment methodologies can identify desirable overall characteristics, but are inadequate to ensure that the results of methodologies will be compatible or their resulting data consistent. For the Dams Sector to produce comparable risk estimates, the basic criteria must be augmented with additional sector-specific technical considerations.
- In some cases, the expert panel evaluation criteria required "yes" or "no" answers, yet many panelists felt that the most accurate answer lay in between. This led to disagreements among panelists, which were not capable of being resolved within the limitations of the evaluation criteria. Where possible, ordinal scales (e.g. "low, moderately low, moderate, moderately high, and high") should be developed that would permit panelists to estimate the "degree" to which a methodology met a required criterion. Alternatively, questions which permitted panelists to provide somewhat open-ended descriptions that described and defended the panelist's assessment were deemed desirable in some cases.
- The evaluation lacked benchmarks or defined standards for best practices against which methods could be compared; thus, evaluators tended to evaluate each method against their own undefined "best practice" standards.
- Experts agreed on the need to develop rational methods for transforming threat information and intelligence into comparative estimates (e.g. rank order or probabilities) for different attack scenarios (i.e. threat vector and target combinations) within the sector.

- To obtain credible vulnerability results, expressed as a probability of attacker success given an attack, it is necessary to develop rational models that appropriately account for all layers of protection (including passive and active detection, assessment, and interdiction features).
- It is necessary to establish a method for aggregating consequences across various consequence categories (human impacts, economic impacts, etc.), including cascading impacts and indirect effects arising from long-term project disruptions.
- The methodology has to include a clear communication strategy for documenting attack-target predictions in a way that accounts for model limitations and data uncertainty.
- Development of a sector-wide risk assessment approach will require a set of tools that can integrate information available from asset-specific assessments conducted at the facility level.

### 2.3 Phase III—Independent Analysis

The third phase of the study was initiated in June 2008. Additional analysis of the requirements defined by the Dams Sector was conducted to develop a more detailed understanding of the results of the prior phases of the study. The primary objective of this phase was to further analyze the outcomes from Phase II, which included making a more detailed evaluation of the advantages and limitations of the representative methodologies considered. The desired end-state of the final phase of the study was to provide additional recommendation on the desired attributes that an effective risk assessment methodology should have, and to take additional steps toward achieving risk analysis interoperability across the Dams Sector.

SRA International was funded to facilitate this phase of the study and develop an objective framework of common requirements and features for security risk analysis methodologies. Noting that much of the Phase II panel analysis generated agreement on "yes" and "no" answers while demonstrating significant differences in the open-ended comments, it was perceived that a more discriminating scale such as an ordinal scale could generate greater clarity. The result of this enabling step was the development of a methodology evaluation tool that could facilitate comparison of risk assessment methodologies on a more detailed and objective basis. This process identified a set of measurable requirements and preferences commonly associated with security risk analysis methodologies.

This phase of the study relied on additional data elicited from a number of security risk experts affiliated with organizations with large portfolios of high-consequence dams. The interviews were conducted in September 2008. Each interview lasted between 1 and 2 h, and they were conducted via teleconference.

First, the facilitators intentionally focused questions toward sector-wide needs and requirements, given likely resources and time constraints. Recognizing that most of the participants could identify many improvements to current security risk analysis that may be beyond current budget and resources, participants were directed to consider the best methodology achievable in the near term. The acronym BMAN ("best methodology available now") was coined by the SRA team to identify this target methodology. The features of this benchmark methodology were explicitly defined based on the set of measurable requirements and preferences incorporated in the methodology evaluation tool.

Second, participants were also asked to give a narrative response for a set of open-ended questions. The open-ended responses were particularly important because they allowed participants to reflect upon overarching risk methodology issues in a narrative format. It also permitted interviewees to express a more detailed and contextual perspective about methodology features for the Dams Sector. A systematic process was followed to capture these methodological requirements and preferences.

In Phase II, in the absence of a thorough understanding of requirements and preferences, expert reviewers had little choice but to evaluate methods against a notional "ideal methodology," without consideration of capabilities or resources needed to develop such an elusive perfect solution. The incorporation of a practical benchmark allows the objective comparison of methodologies through a set of technical requirements, while incorporating additional elements such as measures of their fitness with respect to practical capabilities and available resources. The study succeeded in identifying a wealth of critical issues and observations for further research. The final consolidation into a comprehensive requirements document however, would require additional development and approval across formal Dams Sector collaboration channels (Sector Coordinating Council and Government Coordinating Council). Once completed, the Dams Sector could be in a better position to evaluate, develop, or modify methodologies to bring them in line with sector-accepted requirements and preferences.

## 3 FINDINGS AND OBSERVATIONS

Methodologies currently in use across the Dams Sector are hindered by the lack of common terminology and standards for security risk analysis. Compounding the issues are data quality and availability limitations that present further technical and logistical obstacles—often resulting in the creation of unique and incompatible solutions. As a result, these methodologies—while useful in their own right at the organization level—cannot meet the evolving requirements and expectations at the national and sector levels.

If the achievement of sector-wide interoperability of risk assessment methods and compatibility of risk assessment results is to be achieved, significant work is still necessary to synchronize the requirements of stakeholders at several multiple levels, as indicated in Figure 2. For example, asset-level risk assessment methodologies must meet the needs of owners and operators who must use them to secure their assets and develop facility-specific security programs. Sector-wide risk assessments must be able to compare, consolidate, and prioritize basic results and information from facility-specific analyses. Finally, sector-specific assessments must also provide data that is deemed acceptably comparable with assessment results from the other 18 CIKR sectors, to facilitate national-level analysis.

Numerous observations were captured during the interview process leading to the definition of benchmark methodological requirements and preferences. These are addressed below.

- Interview participants envisioned a benchmark methodology that was consistent, functional, and user-friendly. Participants unanimously stated that the consistency of a methodology would bolster the overall capability of the Dams Sector to aggregate risk values and prioritize assets and programs.


**FIGURE 1** Project elements.

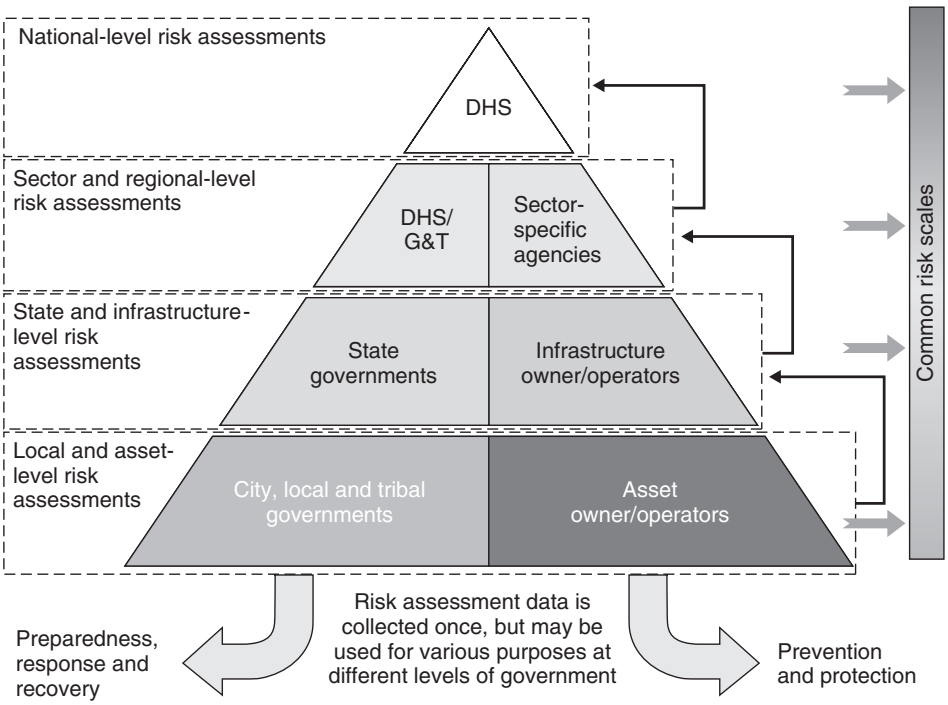



**FIGURE 2** Assessing risk at multiple levels.

- A probabilistic approach using the standard risk equation risk = f(threat, vulnerability, consequence) was considered the best practical option in the near term.
- Participants envisioned that the BMAN should principally address international terrorism, domestic terrorism, and insider threats. While this may appear somewhat limited in scope when compared to efforts to achieve an "all-hazards" methodology, it was noted that the Dams Sector has multiple programs that separately address security and safety concerns. Focusing one methodology on man-made hazards, while other programs addressed natural hazards and industrial accidents was not only stated as acceptable, but preferable. Therefore, the BMAN was envisioned as a stand-alone terrorist risk assessment methodology that did not weigh terrorism risk, natural disasters, and industrial/safety risks against one another.
- Interviewees expressed a clear preference that the BMAN should be able to assist in improving resiliency, recovery, response, and protection, even though most current methodologies focus primarily on protection alone.

- Participants agreed that it is the shared responsibility of asset owners and operators and sector-wide decision-makers to determine how best to address sector-level risks, and indicated that BMAN should measure risk at the asset level and support prioritization needs at the sector level.
- Participants envisioned a BMAN that addresses a broad array of consequences and their impacts, including loss of life, economic costs, mission disruption, interdependencies and dependencies, national security, symbolic impacts, and environmental impacts.
- Some of the participants agreed that the threat portion of the ideal methodology should be scenario-based, as is a requirement in the NIPP. Intention, capability, target attractiveness, and history of adversary were all considered critical analysis factors. Participants also articulated that the threat portion of the BMAN should be amenable to customization, particularly at the asset level, where it should facilitate development of detailed scenarios that could capture unique site characteristics.
- Participants were nearly unanimous in expecting that the BMAN should strive for a high standard of completeness and documentation. Full documentation for BMAN was defined by the participants as including detailed coverage of scope, formulas, limitations, assumptions, scales, and instructions for use.
- Interviewees identified a number of additional features necessary for the BMAN that would make it as much a risk management tool as a risk assessment tool. For example, participants preferred a methodology that included techniques for prescreening assets and enabled cost–benefit analyses.

The interview process also discovered a series of issues affecting most if not all, of the five methodologies in the initial phase of the study. It was noted that methodology developers often took divergent approaches to overcome these obstacles, influenced in large part by the needs of their original organization and their own approach to risk management. The specifics of these issues and their implications for the Dams Sector are discussed below:

### 3.1 Lexicon Problem

The ability to compare risk between assets, or to even identify which asset is at greatest risk, is undermined by the inability to compare risk results derived from one risk assessment methodology against those derived in another. At their highest level, almost all security risk assessments address consequence, vulnerability, and threat components of the problem, but more often than not they define and measure these variables in very different ways. There is little agreement on what factors are examined and how they are measured. While each methodology measures vulnerabilities, a risk analyst could not examine the results from each of these assessments side-by-side. This inconsistency is caused by design features in the methodologies themselves, as shown in Table 2, derived from information found in various parts of Ref. 1.

For example, all of the methodologies address consequences in some way (Table 2); however, by definition, consequence categories differ in significant ways. Given the same unwanted event, a methodology measuring the economic costs resulting from cascading failures associated with infrastructure dependencies and interdependencies will present a different consequence rating than the methodology that measures only direct consequences.

**TABLE 2 Risk Variables**

| | Risk Methodology No. 1 | Risk Methodology No. 2 | Risk Methodology No. 3 | Risk Methodology No. 4 | Risk Methodology No. 5 |
|---|---|---|---|---|---|
| **Consequence** | Casualties | Loss of life | Fatalities | Loss of life | Loss of life |
| | Economic impacts | Loss of dam function | Serious injuries | Economic impacts | |
| | Mission disruption | Secondary losses | Property damage | Mission disruption | |
| | Recuperation | Recovery | Equipment | | |
| | | Disruption to essential facilities | Direct economic | | |
| | | | Indirect economic | | |
| **Vulnerability** | Intrusion paths | Dam type | Adversary tactics | Security effectiveness | Likelihood of success |
| | Delivery vehicles | Feature or component vulnerabilities | Weapons | | Dam type |
| | Attack profiles | Redundancy | Delivery method | | Likelihood of failure (lack of inherent strength) |
| | Security effectiveness | Strength | Perimeter | | |
| | | Probability of loss | Facility exterior | | |
| | | | Facility interior | | |

| | | | | | |
|---|---|---|---|---|---|
| **Threat** | Profile attractiveness | Dam type | Location | Existence | Base threat (attack frequency) |
| | Scenario attractiveness | Security system effectiveness | Publicity | Capability | Criticality |
| | Relative asset attractiveness | | Asset location | Terrorist history and intentions | Suspicious activities |
| | Annual rate of attack | | Asset availability | Targeting | Security system effectiveness |
| | | | Existence | | |
| | | | Security measures | | |
| | | | Perception of success | | |
| | | | Threat level | | |
| | | | History of capability | | |
| | | | Terrorist operating environment | | |
| | | | Terrorist activities in country | | |

### 3.2 How You Measure Matters

The scales and estimation that a methodology uses to estimate risk and its components greatly influence the risk assessment process as well as the final prioritization and decision-making. Measurement methods determine how data, such as expert elicitation, modeling, or owner and operator judgments, is synthesized and aggregated into quantitative values. Four of the five methodologies use some form of ordinal scales or bins, but the criteria defining the bins are incommensurate; therefore, the various scales used by these methodologies are incompatible. Instead of using ordinal scales, the fifth methodology uses ratio scales and probabilities, which yield well-known risk metrics (e.g. *expected* loss measured in dollar amounts for a given time frame) that are mathematically defensible when the risk parameters are multiplied to yield the final result.

### 3.3 Assessing Threat is a Continuing Challenge for Quantitative Analysis

Calculating the threat posed by adversaries is one of the most pressing challenges in the broad risk-management community. This challenge is particularly acute at the facility-level analysis because local threat information is difficult to obtain, while sector-level threat data is often missing, inconsistent, or difficult to quantify. The majority of adversary threat data currently comes from intelligence reporting, which can be incomplete, conflicting, and sometimes "unfinished." Analytical products are also not written with the premise that the data will be quantified, which makes threat data difficult to incorporate into risk assessments. The weakest piece of every methodology reviewed was threat assessment. Each dealt with this problem differently, and in most cases the alternative solutions provided further undermined the credibility and compatibility of the assessments. Adopting or facilitating the development of standardized threat scenarios and corresponding quantitative threat estimates is crucial to being able to compare risk assessments at the sector and national levels.

### 3.4 The Complexity versus Practicality Problem

Many facilities in the Dams Sector do not require a complex model for assessing risk. It was considered more important to strive for a practical methodology rather than provide something that may tend to overcomplicate the process. Furthermore, employing complex methodologies often necessitates organizations looking outside of their current personnel to find the mix of skill sets necessary to conduct the most advanced assessments. As the methodology becomes more complex and rigorous, more time is not only required to perform the assessment, but also for training participants and decision-makers to understand the methodology itself. Given the number of dams within the sector, the availability of resources to produce a sector-wide assessment becomes an increasingly important constraint.

## 4 PROPOSED REQUIREMENTS FOR A SECTOR-WIDE RISK ASSESSMENT METHODOLOGY

A comprehensive, sector-wide risk assessment and management program is achievable and within the Dams Sector's reach. While each of the models reviewed has merit within a narrow field of use, none has the desirable properties of (i) satisfying the need for a

practical approach suitable for comprehensive sector-wide use, and (ii) yielding risks results that can be objectively compared to risk results across the sector as well as results from other infrastructure sectors. The model that is both ideal and achievable will allow risk analysts at the sector level to be able to leverage the data already collected by owners and operators through facility-specific assessments, with the goal of conducting a sector-wide prioritization—without having to collect or develop significant amounts of new data. This sector-wide risk assessment framework will strive for the lowest achievable complexity and logistical burden, while taking maximum advantage of existing assessments. The model that results needs to be not only simple, transparent, and easy to use, but also mathematically defensible and ratio-scalable to provide for more rigorous analyses, if needed. This joint effort between the USACE and Dams SSA has identified and consolidated a substantial set of requirements that will be critical in achieving this practical goal.

To be useful to stakeholders, a transparent and rigorous methodology would be able to evaluate risk numerically and to do this simply, so that risks ascribed to elements across critical infrastructure could be easily compared to each other. To accomplish this in a mathematically defensible way, the methodology would assign real, ratio-scalable numbers to each of the three parameters commonly accepted to compose risk: threat, vulnerability, and consequences. The simplest and most widely accepted approach for calculating risk is to multiply these three together, arriving at a value interpreted as *total risk*.

To explain the concept clearly, a system of calculations is said to be "ratio scalable" if, within the system, a number $x$ has a defined value that is half of $2x$, one-third of $3x$, and so on. As examples, a probability of 0.6 is twice the probability of 0.3; \$20 has a value of twice \$10. Such scales, probabilities, and dollars are ratio scalable. This is as opposed to ordinal scales, in which the numbers ascribed to a system do not necessarily have any well-defined ratio (such as scales that indicate relative qualities of 1 = "good" to 5 = "bad").

Threat may be considered as the *likelihood (or probability) of attack* and vulnerability as the *probability of success given an attack*. These probabilities should be treated as obeying the established laws of probability. Each will have a value between 0 and 1; when the two probabilities are multiplied together, the result will also be between 0 and 1. This product is most easily interpreted as the *probability of a successful attack* against that asset in a given time frame. When this probability is multiplied by the estimated consequences of a successful attack, the result may be logically interpreted as the *expected value of the loss in a given time frame*—or simply risk. If consequences are measured in dollars (this unit is obviously applicable to direct and indirect economic losses, and—using existing US government determinations—human casualties may be represented by an economic loss), the total risk is then estimated as the *expected loss* in dollars to an asset from a defined terrorist (or other) event.

An ideal methodology would need to include a rigorous and repeatable procedure for estimating the probability of success given an attack, assuming that an attack was attempted in the first place. More precisely, the "probability of success given an attack" is defined as the probability of success for a particular and well-defined scenario, that is, for a given attack type on a given type of asset.

A straight-forward way of determining this quantity would be to elicit from a panel of security experts the probability of success for the terrorist attack, based on the attack scenario, the generic characteristics of the asset, and the type of security measures in

place. This probability would not be calculated each time for each asset, but, once determined and systematically validated, would be made readily accessible in a lookup table or matrix that lists probabilities of success versus generic security configurations for a general type of asset. There would be a separate table for each attack type.

In the Dams Sector, much effort has already been devoted to calculating and then further refining estimates of consequences for total or partial failure of a dam or its appurtenant structures. There is a significant body of knowledge that has been developed by the dam safety community, and that could be applied to the consequence estimation problem associated with security scenarios. Therefore, the evaluation of security risks could take advantage of consequence estimates developed by different owners and operators. However, there are still significant methodological differences between the different approaches currently available, and this hinders the direct comparison of the corresponding results. Eventually, Dams Sector owners and operators should agree on recommended methodologies for dam failure consequence calculations.

Armed with a defined probability of success given an attack, and the consequences of a successful attack, these two parameters may be multiplied together to yield a *conditional risk*, that is, an expected loss given an attack attempt. A sector-wide conditional risk could offer an extremely useful insight on the attack types that could affect large segments of the sector or its subsectors, or the types of assets that could be associated with the highest risk for specific attack vectors.

Finally, the next logical step beyond the determination of conditional risk would be the estimation of *total risk*. This requires the actual determination of the *probability of attack* as the additional parameter needed to complete the risk picture. How might an ideal methodology assign a probability, over a given time period, for an attack on a given type of asset? This number would have to be derived from intelligence information, as provided through a formalized process by the corresponding analysts. The probability could be derived by first assigning a value to the probability of a significant attack on the US critical infrastructure, then multiplying this by the likelihood that, given an attack, it would be aimed at the sector being considered (i.e. Dams Sector). Finally, one would have to assign a probability that the attack on this sector would be conducted against a specific type of dam or a particular dam. Extensions of the technique would include various probabilities estimated for different types of significant attack scenarios.

The intelligence community is not usually forthcoming in producing numerical assessments of this sort. However, methods of expert elicitation have been used to dissect intelligence analysts' opinions and assessments of likelihoods, even to the point of assigning relative likelihoods to different events. Expert elicitation, using intelligence experts, is analogous to the expert elicitation described earlier for estimating the probability of success given an attack (which is accomplished using security experts rather than intelligence experts). Estimating the probability of attack, loosely termed the *threat probability*, may be done by asking the experts to engage in a series of direct pair-wise comparisons of different potential threats, given intelligence information on adversary intents and capabilities. This method can produce at least defensible probabilities of attack that can feed the risk evaluation methodology described above. As in the case of calculating a probability of success given an attack, the output from this stage of analysis would be a lookup table of probabilities of occurrence for each significant attack type on a given facility type.

Using the requirements and procedures sketched out above, different analysts would be able to apply a common methodology to facilities within a given sector and arrive

at similar, if not identical, answers that would be fully consistent. This would enable a systematic and reliable process that would directly support an effective sector-wide risk assessment framework.

## REFERENCES

1. SRA International, Inc. (2008). *Risk Methodology Evaluation Project, Draft Report Submitted to the Dams Sector Branch, Sector-Specific Executive Management Office, Office of Infrastructure Protection, U.S. Department of Homeland Security.* U.S. Department of Homeland Security, Washington, DC.
2. U.S. Department of Homeland Security. (2006). *National Infrastructure Protection Plan*. U.S. Department of Homeland Security, Washington, DC.

# CRITICAL INFRASTRUCTURES AT RISK: A EUROPEAN PERSPECTIVE

ADRIAN V. GHEORGHE

*Old Dominion University (ODU), Norfolk, Virginia*
*University Politechnica, Bucharest, Romania*

MARCELO MASERA

*European Commission Joint Research Centre, Ispra, Italy*

## 1 CRITICAL INFRASTRUCTURES: THE EUROPEAN POLICY CONTEXT

Today's infrastructures and their associated systems such as energy, pipelines, water, telecommunication, banking, Internet etc. are delivering services for addressing an adequate quality of life. They have greatly developed and advanced during the last century, growing from facilities with limited reach to continent-wide infrastructures. Most importantly, these systems were neither designed as integrated systems nor as systems-of-systems (SoS), but gradually evolved over time. Due to their relevance to the daily functioning of society, the impairment or failure of these infrastructures can have severe consequences, beyond simple business impact. As failures of critical infrastructures can affect the welfare of society at large and the stability of economic

and political systems, they are an expression of protecting our national security, that is, our homeland security [1].

Most infrastructures originate from local networks. Over time, municipal networks evolved. Interconnection of city networks and network expansion to rural areas were forged through intervention of the provincial authorities. Provincial networks thus emerged in the first half of the twentieth century. The national grid was not fully established until the second half of the century. Over time, the density of end user connections increased. Transport functions in the infrastructure were intensified (augmenting throughput and economy of scale), to serve a steadily increasing number of users and a steadily increasing demand per user. In the case of electric power, to improve the security of service, the national grid was interconnected across regions and national borders, most notably in Europe. At the moment, most national grids in Europe are interconnected and are operated as a single SoS. In the course of about one century the system's dimensions have grown by several orders of magnitude. Currently we are managing and crucially depend upon transcontinental networks for electricity transmission, oil, and gas pipelines, vastly distributed information and telecommunication infrastructures. It is fair to say that the distinguishing attribute of our society is this capacity to develop, operate, and control the risks of extensive infrastructures composed of many interconnected systems, each one run by different (mainly private) companies.

This evolution was not exempt of cross-links between politics, business, technologies and a variety of risks including financial, environmental, and political. The incorporation of new technologies, most notably the information and communications ones, enabled the expansion and networking of infrastructural systems and the improvement of their efficiency. While these infrastructures were becoming critical to society at large, policy-makers and business decision-makers realized that the assessment and management of risks was not just one more business function.

One point that still requires full recognition is the implication of the term "critical". In modern infrastructures it conveys the need to cope with new types of emerging risks. These risks are cross-organizational and international by nature: the interconnection of systems knows no borders but the risk management solutions proposed are basically a new edition of old models. This is still the case with solutions commonly offered by business continuity, civil defence, or emergency management institutions.

Some infrastructures such as energy, water supply, and telecommunications are so vital and ubiquitous that their incapacity or destruction would not only affect the security and social welfare of any nation, but would also cascade across borders. Critical infrastructures are exposed to multiple threats – such as terrorist attacks, natural disasters, or institutional changes, – and in addition their failure might induce risks to other interconnected systems. Consequently, there is an urgent need to address such problems with appropriate risk assessment and governance instruments, supported by timely policy analysis at an international level.

The main factors that have transformed the nature of infrastructures, that is, how these systems are designed, developed, deployed, and operated, are listed below:

- the liberalization of markets, mainly affecting the electric power and telecommunications fields which caused the previous monopolies to cede their position, unbundle their integrated business models, and compete with other players;

- the networking among infrastructures, that require each other for completing their functioning, generating an intertwined mesh of interdependent systems;
- the increase of cross-border interconnections, justified by the need to share capacity in case of major malfunctions, and also the mechanism for the integration of markets;
- the technological change brought about by the evolution of information and communication technologies (ICT) and their pervasive use for improving the functionality and control of technical systems, the interaction with the industrial and business sides of companies, and the relations among the actors in the supply chains;
- the advent of new systemic risks generated by complexity and nonlinear behavior of newly established SoS.

*The liberalization of markets* has diluted responsibilities with respect to potential shortcomings. Each operator of an infrastructural system licitly looks after its own business interests. The countermeasures implemented for countering the risks respond to their own judgment of costs and benefits, in the context of the rules and constraints defined by the authorities. Typically, infrastructural services are recognized as basic public services and for that reason they are subject to governmental regulation. Nevertheless, risks are still managed piecewise, without an overall consideration of the compound effectiveness of single risk management approaches.

*The interdependencies among infrastructures* makes it possible for system failures to originate from external systems. The normal way of dealing with risks is to consider systems with clearly defined interactions with their environment. But the complexity of interdependent infrastructures precludes the comprehensive knowledge of potential threats without a deeper understanding of the connected systems. The most that can be expected is the definition of service levels among the individual operators of the systems.

*The increase of cross-border interconnections* has made each nation's infrastructure dependent on the proper functioning of the ones in other countries. Some of these interconnections are part of long and complex international infrastructural corridors (e.g. energy, transport, telecommunications, etc.), that need to be consider in their entirety. Most of them will lose much of their functionality and usefulness if disconnected. In addition, this interaction means that each interconnected system is at the same time, a provider of services and a potential source of risk problems. These interconnections are not only structural and operational as they are further enmeshed in the links between markets, with operators making transactions in several of them.

The great *changes in ICT* have extended the channels connecting the systems, with most of them using open public networks. This fact augments the possibility of suffering malicious attacks. Open networks, now reachable worldwide and accessible by many users, involve many disciplines in the problem: legal and market issues, technologies, international relations, homeland, and national security.

*Systemic risks* are inevitable when implementing and operating these vast infrastructures. They originate not only from the composition of many technical installations, each one operated independently and following mainly its own autonomous rules, but also from the overlaying of several strata (technical, market, regulatory), each one split across several jurisdictional spaces.

There is no simple answer to the question of how to deal with these critical systems. The first consequence of this situation is the conjunction of subjects previously treated in a separate manner: industrial policies for the regulation and development of services and the companies offering them, civil defense and emergency management for dealing

with the negative consequences of potential accidents, law enforcement for coping with organized crime, national defense for responding to external threats and so on. In light of the nature and challenges posed by *critical infrastructures*, a convergence of these topics is required.

However, one question remains open: how should decisions about the risks in critical infrastructures be made? This goes beyond the realm of governments, as infrastructures are operated (almost exclusively) by private companies. But the accumulation of the risk management decisions by single companies will only rarely provide a proper answer to global risk situations. If the international dimension is added, the need for an apposite answer is indisputable. There is a new trend worldwide in addressing risks of complex systems, and this leads to the concept of *risk governance*.

## 2 EUROPEAN VIEW OF FUTURE CRITICAL INFRASTRUCTURE DEVELOPMENTS

At of the beginning of 2007, some policy developments in the European Union regarding Critical Infrastructure Protection (CIP) were vigorously initiated. Due to their intrinsic nature, many infrastructures show a cross-border character. Therefore, during 2005–2006 the concept of European Critical Infrastructure (ECI) has been elaborated, which materializes from an adopted directive [2] on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. It is worth noting that, although recognizing the nation-state's precedence when dealing with this subject and the privileged link between infrastructure operators and national governments, it has been accepted that certain transnational coordination is required for coping with the ECI risk. The European Union has established a European Programme for Critical Infrastructure Protection (EPCIP), under which several sector-specific programs are being implemented (e.g. information, transport, energy, etc). In addition, the CIP (Critical Infrastructure Protection) subject is also considered a priority within the European Commission's R&D 7th Framework Programme, 2007–2013.

CIP has duly been treated as a national issue within the European Union. Nevertheless, several factors have made it evident that there is a need for joint action:

- several infrastructures are composed of networks that cross borders;
- the potential widespread effects of some situations deriving from different threats (e.g. natural causes and malicious attacks);
- the potential benefits from joint investments in the development of solutions.

The European Council requested the Commission in June 2004, to prepare a comprehensive strategy aiming at the protection of critical infrastructures [3]. The Commission reacted with a communication entitled "Critical Infrastructure Protection in the Fight against Terrorism" [4] presented on October 20, 2004. There, the Commission discussed concrete proposals for improving the state of European prevention, preparedness, and response to potential terrorist attacks involving critical infrastructures [3–9].

This initial focus on terrorist attacks was then widened to all kinds of potentially malicious attacks, and ultimately to a so-called *all hazards approach*. The reason for this was the understanding that the management of risks to infrastructures should, in the end, be calibrated according to all sources of danger.

It is clear that in most, if not all sectors, there are consolidated legal frameworks for countering safety risk (caused for instance, by natural hazards, technical failures or human errors). The security dimension somewhat overlaps with these safety situations when considering the possible consequences of some events. However there are obvious dissimilarities in their causes, and therefore in the required countermeasures. The difficult task in an all-hazards approach is to provide a comprehensive stance on risk, without unnecessarily disturbing other existing industrial requirements and obligations.

In December 2004 the European Council approved the Commission's proposal for setting up a *European Programme for Critical Infrastructure Protection* (EPCIP) and a *Critical Infrastructure Warning Information Network* (CIWIN) [3]. In 2005, the Commission, led by EC Directorate General Justice, Freedom and Security (DG JLS), worked on the elaboration of EPCIP, organized two European seminars on critical infrastructure protection and a number of informal meetings together with experts from all EU member states. As a result of this process, the Commission adopted the Green Paper on a European Programme for Critical Infrastructure Protection [6] in November 2005.

This Green Paper not only put forward the definition of the principles that should guide European actions in the field, concrete proposals for the EPCIP framework, and the links between national and European critical infrastructures to the countries and society at large, but also anticipated the arrangement of funding sources for activities related to EPCIP which could include relevant studies and the development of specific methodologies.

The Green Paper was then complemented by a detailed impact assessment. A policy package on EPCIP composed of a communication and a directive was adopted by the Commission in December 2006 [8]. The communication contains nonbinding measures designed to facilitate the implementation of EPCIP, and includes an EPCIP Action Plan. It discusses the general policy framework of EPCIP (including CIWIN, the work-streams to develop the programme, sectoral interdependencies, annual work planning, and the residual work on National Critical Infrastructure), and the directive defines the approach for the designation of critical infrastructure of a European dimension (that is, ECI).

In parallel to this development, other Directorate Generals of the Commission began working on policies for the protection of the infrastructures under their remit. While EPCIP is intended to provide an overall framework for action, the specific discussions on policy measures and on how to coordinate the protection are done on a sector-by-sector basis.

DG Energy and Transport (TREN) worked with national authorities and regulators, infrastructure operators and experts, in the definition of an approach for the infrastructures in its field of reference. This resulted in the adoption of the "Communication on Protecting Europe's Critical Energy and Transport Infrastructure" in February 2007 [9]. This is the first sector-level initiative in the framework of the EPCIP programme.

The main content of the communication—which due to the sensitivity of some of the subjects discussed has been defined as restricted, meaning that it is not available to the general public—is composed of criteria for the identification of ECI in each energy and transport sector. The communication does not contain any proposals for legislative measures, but legislation remains one of the options for subsequent work.

In 2006, the EC Directorate General Information Society and Media (DG INFSO), presented a proposal of a structured process of consultation and dialogue on network and information security to be established with relevant stakeholders, including public administrations, the private sector, and individual users. The Commission adopted the

communication "Dialogue, partnership and empowerment" in 31 May 2006, creating a strategy for a Secure Information Society [7].

This strategy is partially dedicated to aspects of the Critical Information Infrastructure (CII), and recognizes that both the public and the private sector have pivotal roles to play. It aims to provide a basis for responding to the major challenge faced by Europe in that field, namely:

- *raising awareness* on the security risks;
- establishing *a culture of security* in which security is seen as a business value and an opportunity rather than as a liability and an additional cost;
- fostering an appropriate framework of conditions for *interoperable*, *open*, *and diverse solutions* provided by a competitive, innovative European industry.

The strategy recognizes that there is an increased *connectivity between information and communication networks with other critical infrastructures* (like transport and energy). The proposal is to develop a sector-specific policy for the information and communications sector for examining via a multi-stakeholder dialogue and the relevant economic, business, and societal drivers with a view to enhancing the security and resilience of the information infrastructure.

Any review of the regulatory framework for electronic communications will have to consider elements to improve network and information security. These should include both technical and organizational measures by service providers, provisions dealing with the notification of security breaches, and specific remedies and penalties regarding breaches of obligations. But although legal norms might help in fostering the creation of markets for security products and services, it is obvious that those products and services will be born out of the interaction between the operators of critical infrastructures and the suppliers of technology.

On the other hand, national governments need to put into practice best practices and be secure from the information and network point of view. A key point here is the communication and sharing of information threats, risks, and alerts but the global dimension of network and information security cannot be ignored. Europe needs to take into account the international level when coordinating and promoting cooperation on network and information security (e.g. implementing the agenda adopted at the *World Summit on the Information Society*, WSIS in November 2005).

Finally, in December 2008, an agreement on the definition of ECI was reached. It has been defined as such critical infrastructure as located in member states of the European Union, the disruption or destruction of which would have a significant impact on at least two member states [2]. The identification of the ECI is the responsibility of each country, although the European Commission on a collaborative basis "draw the attention of the relevant Member States to the existence of potential critical infrastructures which may be deemed to satisfy the requirements for designation as an ECI" [2].

The EU Directive on Critical Infrastructures defined a first period of two years in which the EU countries are obliged to identify and designate critical infrastructures in the following sectors: energy (oil, gas, and electric power), and transport (including road transport, rail transport, air transport, inland waterways transport, ocean and short-sea shipping, and ports). The oil sector includes oil production, refining, treatment, storage, and transmission by pipelines. Similarly, the gas sector includes gas production, refining, treatment, storage, and transmission by pipelines, as well as liquefied natural gas (LNG)

terminals. The electricity sector includes infrastructures and facilities for generation and transmission.

The identification of ECI will be based on an assessment of the significance of the impact of their potential loss, evaluated according to the so-called "cross-cutting" criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure, and comprises of the following: (i) potential casualties; (ii) economic effects (significance of economic loss and/or degradation of products or services, including potential environmental effects); and (iii) public effects (impact on public confidence, physical suffering, and disruption of daily life including the loss of essential services).

In the field of CII, a new European policy initiative was presented [10] in early 2009. This initiative complements EPCIP since it deals with the ICT aspects. The initiative proposes actions that supplement other existing measures (e.g. judicial cooperation for dealing with cyber crime and terrorism targeting CIIs).

This policy is based on the recognition that, with due respect for national autonomy, there is an urgent need to integrate the collaboration of all interested stakeholders as CII is essentially international in nature. Five streams of action have been identified.

- *Preparedness and prevention.* This requires the collaboration of Computer Emergency Response Teams. It is proposed that a European Public-Private Partnership for Resilience and a European Forum of Member States be created, to share information and good policy, operational practices.
- *Detection and response.* It is recognized that the need for early warning mechanisms can result in the establishment of a European Information Sharing and Alert System. This should provide services to citizens and Small and Medium Enterprises (SMEs), taking advantage of national and private sector information systems.
- *Mitigation and recovery.* The setting up of national contingency plans will be encouraged along with the organization of regular exercises for large-scale networks security incident response and disaster recovery. This is seen as the basis for the need for pan-European coordination.
- *International and EU-wide cooperation.* This is required for agreeing on EU priorities for long-term goals (e.g. regarding the resilience and stability of the Internet), establishing common guidelines where needed, and promoting principles and guidelines at the global level.
- *Criteria for the ICT sector.* In the context of EPCIP, these criteria will support the EU countries in the identification and designation of ECI regarding the ICT sector.

## 3 EUROPEAN CRITICAL INFRASTRUCTURES: CHALLENGES AND PRINCIPLES

The European Programme on CIP aims to identify and characterize ECI and also to define a common framework for managing and governing risks. For this reason, a key element is the ability to determine which systems could be of relevance to more than one country, and then to establish how it would be possible to deal with those events in terms of prevention and reaction to hazards. This relationship between national and European approaches has to be flexible enough to take into account their complementarity. The respect for national jurisdiction has to be accompanied by the examination of potentially

harmonized approaches and similar levels of protection for infrastructures crossing borders or having a potential impact on other countries. In addition, any legal framework for enhancing security should be compatible with competition rules and internal market. This indicates the many prerequisites that should be considered by Europe while setting up EPCIP viz. national and local jurisdictions, sectoral industrial policies, fair competition, law enforcement requirements concerning malicious acts, civil protection and emergency management, and last but not the least, national security.

To meet all these objectives, the EPCIP proposal identified both binding and nonbinding measures to be adopted by the Member States. The nonbinding measures are indicative of good practices that are advisable: (i) participation in CIP expert groups at EU level, (ii) use of a CIP information-sharing process, (iii) identification and analysis of interdependencies, (iv) elaboration of national CIP programmes, and (v) identification of national critical infrastructure.

The EPCIP binding measures aim at fostering a harmonious collaboration among the different countries and infrastructure actors. The proposed ones are (i) nomination of CIP contact points, (ii) identification and designation of ECI, (iii) conducting threat and risk assessments for ECI, and (iv) elaboration of Operator Security Plans and the designation of Security Liaison Officers.

In addition, the proposal of the directive presents several principles that summarized the approach that the Commission proposes for the implementation of EPCIP. They are as follows:

- *Subsidiarity.* Efforts in the CIP field should focus on ECI, and not on the ones falling under national or regional jurisdiction.
- *Complementarity.* Efforts should not be duplicated, and should be developed where they have proven to be effective, complementing and building on existing sectoral measures.
- *Confidentiality.* CIP data is sensitive and should be classified in an appropriate way, with access granted only on a need-to-know basis
- *Stakeholder cooperation.* All relevant stakeholders should be involved: owners or operators of critical infrastructures, public authorities, and other relevant bodies.
- *Proportionality.* Only relevant measures should be proposed for satisfying specific needs, proportionate to the level of risk and type of threat involved.
- *Sector-by-sector approach.* A list of CIP will be agreed upon, and then concrete actions will be developed.

## 4 CRITICAL ELECTRICITY INFRASTRUCTURE: THE EVOLUTION OF THE RISK

Europe witnessed in the last few years a number of significant power contingencies. Some of them revealed the potentiality for a vast impact on the welfare of society, and triggered off pressing questions on the nature and reliability of electric power systems. Society has incorporated electricity as an intrinsic component, indispensable for achieving the expected level of quality of life. Therefore, any impingement on the continuity and properties of the electricity service would be able to distress society as a whole, affecting individuals, social and economic activities, other infrastructures, and essential government

functions [11]. It would be possible to hypothesize that in extreme situations this could even upset national security.

The blackouts and near-misses that happened in the last few years illustrate several notable lessons that have to be carefully taken into consideration:

- *There are hints of some inadequacy*. Heavy workloads and limited reserve generation capacities make systems vulnerable to widespread disruptions. Protection systems have been found to play a key role in the majority of catastrophic failures. Power systems have not been designed to cope with the concurrent outage of two or more critical components.
- *Incidents were aggravated by other factors*. These include the lack of timely comprehension by control-room operators of potentially far-reaching failures and short-term emergency requirements.
- *The recent liberalization of the European electricity market*. This has led to increased cross-border trade for which power systems were not originally designed.
- *European TSOs*. Transmission System Operators, which only recently have developed a more system-of-systems-wide monitoring capability, have no or limited influence on international power trading and the resulting power flows, and therefore confront more and more *unanticipated congestions* on the tie-lines.

During the last decade, Europe has developed a comprehensive energy supply policy unbundling the previous monopolies and opening the generation and distribution markets [12]. This policy has deeply changed the business and regulatory landscape of the electric power infrastructure. From the consumer point of view, the effects have been positive: there are more potential suppliers, and prices follow market rules.

The immediate economic effects of the new policy have not been accompanied by changes in the underpinning physical systems whose evolution demand at least medium-term investments and planning. For the time being, the power infrastructure has shown an appropriate reliability level, but new threats can be foreseen in the horizon. Some of these threats are internal to the infrastructure mainly due to the increasing complexity of many technical and market elements; some of them are external, for instance, the menace of terrorism.

Therefore the security of the evolving European electric power infrastructure deserves a cautious and thorough consideration. A comparative analysis of policy and regulation in Western Europe has been provided earlier in Midttun [13]. Electricity is a *common good*, central to the security and welfare of almost half a billion people, and the stability and future economic development of more than 30 countries. For this reason, although local contingencies can be tolerated up to a given degree, if the power system appears unreliable at the continental level, this will become a matter of major concern. Europe cannot afford systematic failures of its power infrastructure that could eventually lead to the weakening of the citizens' trust on societal institutions.

The various national European electricity systems, after the transformation experienced in the last few years, now form part of a unique and integrated *European Critical Electricity System-of-Systems* (ECESoS). This situation results from an evolution spanning decades and is determined by two main driving forces, namely, market liberalization at the continental scale, and the high degree of interconnection among regional systems [14]. This has been made possible by the pervasive incorporation of ICT.

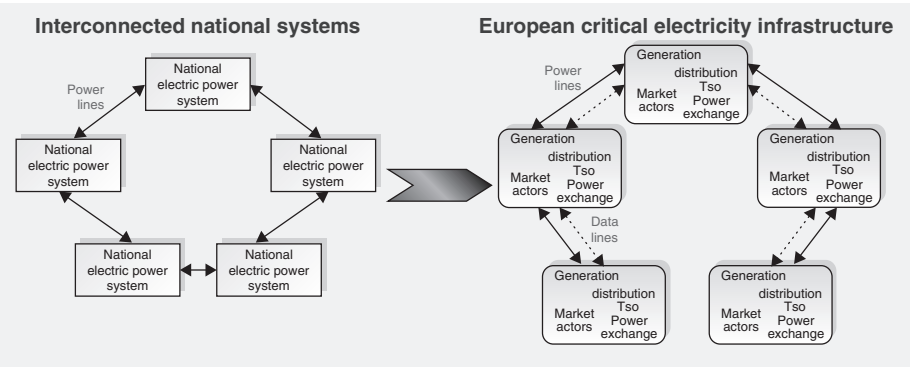



**FIGURE 1** The ECESoS concept.

This complex system is a socio-technical artifact, and tends to function as a single entity, although it includes several jurisdictions, operators, and markets. It is derived from the interconnection of national and regional systems, but at the same time it behaves as a single, *compound SoS*. It is decentralized; still, disturbances can propagate through all of it and risks have to be coped with in a coordinated way. The passage from a set of electricity systems to the ECESoS is not just a question of more elements or actors, it represents a qualitative leap. ECESoS, an infrastructural SoS, is intrinsically different from a set of weakly connected power systems where energy flows among different systems are marginal.

The materialization of ECESoS presents clear advantages, but also brings about vulnerabilities which may threaten its serviceability. The fact that these shortcomings exceed the providence of individual parties means that there is a need for new, effective instruments for managing risks.

Figure 1 outlines this evolution of national electricity power systems (EPS) being embedded into ECESoS. This paper outlines the implications of this development, and studies the positive and negative effects of the extensive interconnectedness and digitalization (i.e. the ubiquitous application of ICT).

## 5 TRENDS AND DRIVING FORCES

The *liberalization* of the European electricity sector has replaced centralized control by regional monopolies with a complex, decentralized market structure, in which many different agents control each part of a technically highly integrated ECESoS infrastructure. The distribution of the many functions in the electricity supply industry among numerous different actors and their coordination through national market mechanisms and grid codes has greatly increased the management complexity of the sector.

This *de facto* decentralized control can work appropriately in the long term only if all the different agents in the system experience the correct incentives and comply with compatible rules throughout the European infrastructure. Technical reliability, which used to be the goal for gauging the performance of electric power systems, is not enough for the ECESoS reality. Many other factors including environmental compatibility, market practicality, and national security have to be included in the decision-making process.

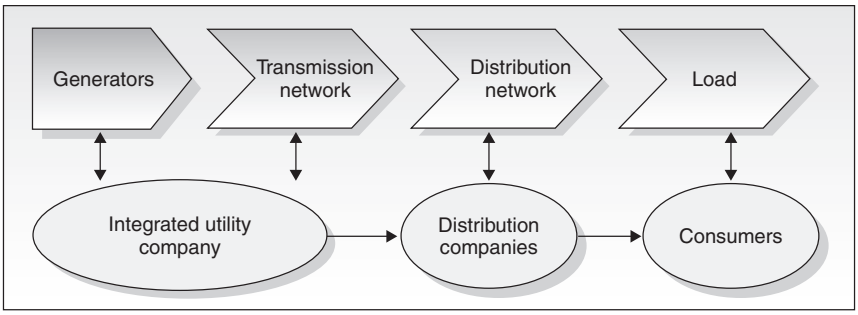



**FIGURE 2** The organizational structure of the electricity system before liberalization.

These factors can be structured in five ranked layers (where the upper one comprises the lower ones): security, sustainability, economic efficiency, reliability, and technical performance. *Security* can be used as the overarching concept that includes all the other objectives.

With respect to this notion of security, all stakeholders need to have a common understanding of the overall system goals and be willing to work toward them, both during normal operation and in case of contingencies. If not, the pursuit of their own private ends although legitimate, may be in conflict with public objectives such as availability and affordability. Whereas the regional monopolies of the past required only a relatively simple regulation of their performance and tariffs, the complex decentralized system that is the result of liberalization requires careful crafting of its institutional structure to ensure that the multiple, and sometimes conflicting, public goals are met (Fig. 2).

Figures 2 and 3 illustrate the organizational changes that liberalization has brought about. Figure 2 shows, schematically, the structure of a regional monopoly: nearly all functions are performed by the same agent, the electricity utility company. Often, distribution and end user supply were managed by separate companies but these were again regional monopolies. Figure 3 shows a simple model of a liberalized electricity system. The figure shows the different groups of actors who together control the physical system. In Europe, many of these electricity systems are interconnected with each other. The operation is coordinated in several regional blocks (e.g. UCTE or the Union for the Coordination of Transmission of Electricity, Nordel, UK), whose composition leads to ECESoS.

A second trend, which already existed prior to liberalization but was further stimulated by it, is the *internationalization* (i.e. interconnection among national grids) of the electricity system. The operation of the vast European power network is complicated by the many different jurisdictions that exist. At a technical level, the TSOs cooperate with each other. At the economic level, large differences continue to exist between the markets in different countries. In order to create an internationally level playing field, the economic conditions such as *transmission tariffs* and *network access rules* in different countries should be put into synergy. In practice, however, different countries liberalize with different speeds and implement different models, not always considering the global consequences of local measures. In addition, the changes in environmental standards, taxes, and subsidies should also be considered.

The complexity that results from the combination of the liberalization and the internationalization of the ECESoS poses a threat to the reliability of electricity services.

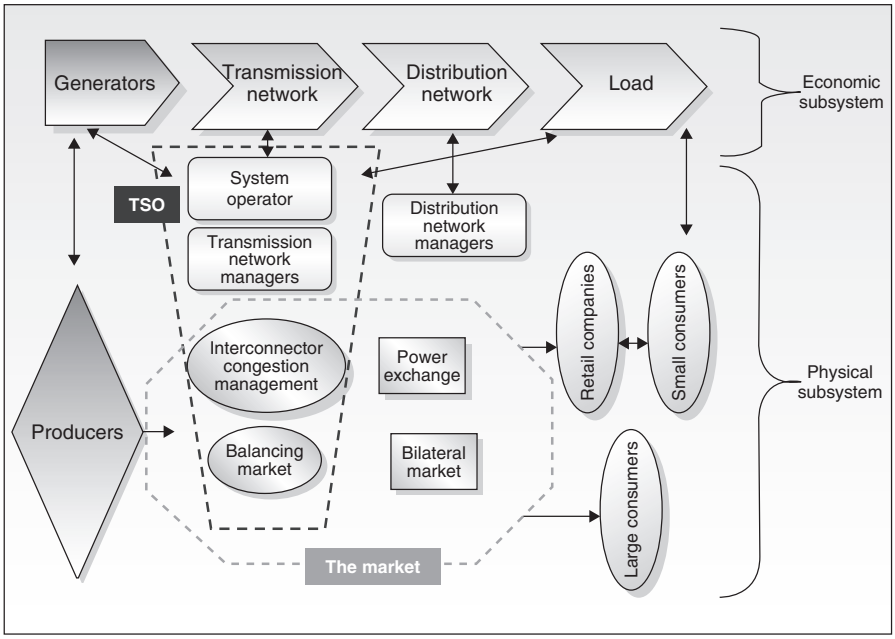



**FIGURE 3** The organizational structure of a liberalized electricity system (decentralized model).

A clear case is given by the difficulties faced in the coordination of the responses to contingencies spread over a wide area. The multitude of industrial actors and the many countries involved also complicate the achievement of a balanced development of the system in the long-term, which in turn may give rise to more contingencies.

The liberalization and the internationalization of the power systems and the facilitation of international trading, has also resulted in the adjustment of the association and cooperation among the operators of the power infrastructure. Partly as recognition of the continental reach of the power infrastructure, and partly due to the European policy initiatives toward the integration of cross-border collaboration, on 19 December 2008, 42 European TSOs from 34 European countries created a new association: the European Network of Transmission System Operators for Electricity (ENTSO-E). The declared objective is to contribute to the reliable and efficient management of pan-European and regional markets.

A third trend, which we will call *evolutionary unsuitability*, is caused by the fact that electricity transmission networks are increasingly being used in ways for which they were not initially designed. Electricity systems are not just operated under high stress conditions, but also beyond the limits of their original design. The increasing development of wind power is already leading to stability problems in certain areas. The changes in the electric output of wind parks led to fast and significant changes in the way the electricity network is used but the network was not designed for such rapid operational changes. Distributed generation, which means the generation of electricity (and often also heat) in small units close to consumers, may also change the way the networks are used. Whereas large scale wind energy mainly impacts the transmission networks, distributed generation would change the nature of distribution networks. This trend is unavoidable in an ECESoS scenario. It is impossible to foresee the many uses that the infrastructure

will be subjected to. This will require a new approach to the engineering, deployment, and operation of the infrastructure including several non-engineering aspects. It is a "Science and Art" issue that requires continuous collective learning in the production and management of complex systems.

A fourth significant trend is the wide-scale application of ICT in electricity systems from the level of individual switches up to the operational control of entire electricity networks, and from customer databases to automated spot markets. While the use of ICT provides many opportunities, the large increase in connected devices and information flows also increases the vulnerability of the ECESoS to both, failures of the information infrastructure and deliberate harm through the use of it. Therefore there is a double effect: on the one hand there is an increase in the functional capabilities due to the availability of information; but on the other there is a greater exposure of the system to cyber threats. All stakeholders have access, in one way or another, to the information components of the infrastructure therefore it is more difficult to prevent access to illegitimate intruders (Table 1).

This amalgamation of electric power systems and ICT produces a new construct, "Electricity plus Information" (or ***E+I***). The ECESoS is connatural to this E+I paradigm; it is immersed into a reality where all electricity functions (i.e. production, trading, transmission, distribution, billing, customer interaction, etc.) are dependent on information. Electricity (the physical dimension of the infrastructural services) coexists with data (the digital dimension of the same infrastructural services). The first dimension is composed of tangible assets: generators, transmission lines, transformers, control and protection equipment, etc that are the traditional objects for the valuation of the power business. The second dimension corresponds to intangibles: knowledge, transaction relationships, customer information, contracts, consumption profiles, security culture, etc. Currently, the perceived value of intangibles is overtaking that of tangibles. This happens in a continuous process that transforms the electric power infrastructure, driving the formation and establishment of the E+I paradigm (Fig. 4).

E+I is an ongoing process, with the power industry continuously incorporating ICT for the sake of improving the operations, functions, and protection of the power systems, as well as integrating engineering and business functions for linking with other technical and market operators. We can talk of the digitization of the power infrastructure. And looking into the future, we can only predict a more intense use of ICT, driven by the shift toward smart grids, distributed generation, diversity of energy sources, and further integration of the infrastructure with neighboring regions (e.g. North Africa, Russia, and Middle East).

When assessing security, this E+I reality cannot be ignored. This affects which vulnerabilities and threats have to be taken into consideration, which measures can be taken for solving the problems, and also how the governance of risk can be implemented. The wealth of information and the easy access to data sources, have to be factored in when designing the risk governance process [4].

## 6 THREATS AND VULNERABILITIES

The transformation of the electric power infrastructure driven by those trends indubitably bears favorable effects (e.g. diminishing prices for consumers, more competitive markets inducing innovative behaviors, alternative sources of electric power supply), but it might

**TABLE 1 Sequence of Events: Italian Blackout**

Importance of Risk Awareness and Crisis Management: the Italian Blackout (A Short Description)
Sequence of Events (September 28, 2003)

- 3:00 Italy imports 6.9 GW, 25% of the country's total load, 300 MW more than scheduled
- 3:01 Trip of the 380-kV line Mettlen–Lavorgo caused by tree flash-over (no adequate tree cutting); overload of the adjacent 380-kV line Sils-Soazza
- 3:11 ETRANS (CH) informs GRTN (I): Request by phone to reduce the import by 300 MW (not enough), GRTN responded within 10 min
- 3:25 Trip of the Sils–Soazza line due to tree flash-over (at 110% of its nominal capacity) Italian grid loses its synchronism with the UCTE grid; almost simultaneous tripping of all the remaining connecting lines
- 3:27 Breakdown of the Italian system, which was not able to operate separately
- 21:40 Restoration of the Italian system complete

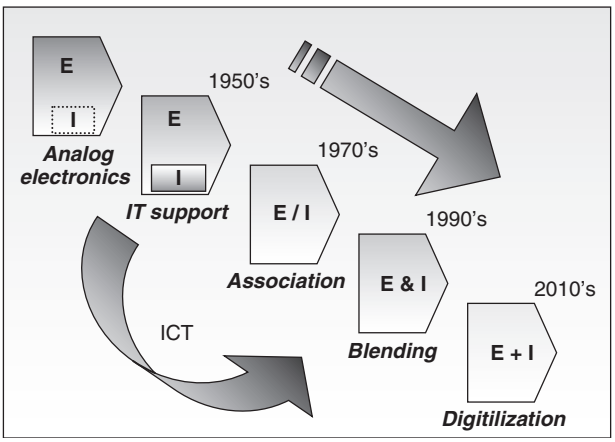



**FIGURE 4** The evolution of the E + I paradigm.

also generate negative conditions for the overall security of the infrastructure. These situations that are prone to risks are related to many facets of the infrastructure such as the organization of the power market, the regulation of the interconnections to the power grid, its topology, and the technological solutions applied. In addition, it is necessary to consider the perception and reaction of society to those risks.

The liberalization of power markets has fragmented investment decisions upon many industrial players (mainly on the generation side). The relatively long time required for developing new installations causes uncertainties about whether the combination of individual decisions will guarantee the security and adequacy of the infrastructure.

This situation can be complicated by the dependence of investments on environmental considerations, fuel prices, and fuel availability. A key fact is that the growth of transmission capacity, and in some places of generation, falls very far behind the growth in consumption. The main constraint on the creation of new power lines and generation plants is the difficulty in obtaining the necessary permits, mainly related to environmental considerations while the fuel aspects are obviously determined by geopolitical circumstances. Markets entail the danger that all new power plants will make use of the same cheapest (available) fuel and the transition to liberalized markets has brought additional uncertainties provoked by changes in the regulatory frameworks.

The central question is whether competitive markets, even in a stable phase after liberalization, provide adequate and timely investment incentives. The new regulation of power systems in Europe has a strong focus on costs. Nevertheless, it is not clear if the reduction of costs can be balanced with the need to maintain security and expand the power grid in a timely and economically efficient manner.

A key point is that different European countries have liberalized with different speeds and implemented different market models. This creates a significant risk of market distortions, which is further aggravated by the complexity of the institutional design.

Electricity generation has observed the development of power based on renewables. These are placed where the resources are available, not where the consumption exists. As a result, power transmission networks and international interconnectors are used in ways for which they were not designed, and their control and protection systems are put under stress.

These changes in power markets and in power generation and transmission are accompanied by a pervasive use of ICT. This has had a beneficial effect on the operation of power systems, and the integration of the industrial and business information systems within and between companies. But it has opened up opportunities for new types of system failures, both of accidental and malicious origins.

First of all, information security was never a point for industrial systems, and therefore there is a lack of proper security-related standards and specific security technologies. Only in the very last years, with the awareness that interconnected information systems were open to electronic attacks, standardization bodies (e.g. IEC, IEEE, NERC) have begun to work on appropriate security norms. However, technologies change rapidly and the application of standards necessitates time. This opens a window of opportunity for this kind of newly emerging risks.

The power grid is exposed to accidental failures and natural hazards similar to the ones endured in the past. The question is whether the new structure with multiple operators is as *resilient* as the more centralized one in the past. The complexity of the European power network topology creates the possibility of failures that escalate from local problems to broad disturbances, and that propagate throughout the system potentially leading to cascading blackouts across international borders. This requires well-orchestrated protection, and the coordination of restoring services in case of widespread contingencies. As a matter of fact, many of the existing control and protection strategies and contingency defence plans are outdated because they were developed at a time when international flows were smaller, generation was dispatched by the system operator, and the use of ICT was much more limited.

Much attention is currently given to the risk of terrorist attacks. The likelihood is difficult to estimate, but it would require a sophisticated, well-coordinated attack to bring a large part of the European power system down. Failure of individual power plants or

power lines is a contingency that the system is designed to withstand, but a complete assessment, considering the interdependencies with other infrastructures, has not been performed yet.

## 7 NEEDS: RISK GOVERNANCE, SCIENCE AND TECHNOLOGY

The European electric power industry has been evolving rapidly in the last decade. The Electricity Directive 96/92/EC adopted in 1996 set common rules for the EU internal electricity market. It established the basis for the opening of the national markets, for the unbundling of the vertically integrated electricity companies, and in general for the organization of the generation, transmission, and distribution business.

As a means for establishing communication between the stakeholders, electric power systems, and the policy decision-makers, a forum was organized to discuss the regulatory process and the formation of the European internal electricity market. It was set up and organized by the European Commission. The first meeting was held in 1988, and it is commonly known as the Florence Forum. Its objective is to provide a neutral and informal framework for discussions concerning the implementation of the Electricity Directives.

The normative context was complete in 2003 with the new Electricity Directive n. 54 [15], complemented by the Regulation 1228 on cross-border trade [16]. This directive aims at establishing (at the latest by July 2007), an open European market for electricity where consumers will be free to shop around across borders. At the same time, a set of regulators have been instituted in all countries for ensuring the correct operation of the market and the regularity of the public services of the electricity supply.

The fundamental issue of this policy initiative has been the institution of the European internal market for electricity, and it is possible to say that up to now it has been successful and beneficial for the European citizen. Nevertheless, risk and security (in the broad sense employed in this White Book) have not been considered main concerns. Security of supply is mentioned as one of the public service attributes to be guaranteed [17]. Specifically it is said that the goal is to achieve a "competitive, secure, and environmentally sustainable market in electricity" (Article 3) [17]. Some issues mentioned in the directive are market mechanisms for ensuring sufficient electricity generation, long-term planning, the need to monitor the balance between supply and demand, and topics left to the responsibility of each country. But no provision has been made for coping with the systemic risks that affect the European infrastructure as a whole.

Therefore it is possible to discern a mismatch between the policy goal of developing a secure market, and the lack of dedicated mechanisms for dealing with risks that might rise beyond the control of the single power company and the single country. Would current instruments be effective for dealing with systemic risks affecting the infrastructure? The only group that brings together all stakeholders (industry, regulators, policy decision-makers, consumers) is the Florence Forum. Could it be used to take care of the infrastructure risks? The answer is negative, considering its current structure and working style. It is not a decision-oriented organization, and it is oriented toward informal debates.

However, on the other hand, traditional methods of risk management (applied for instance by electric power companies) do not suffice for coping with the new challenges faced by the electricity infrastructure in its entirety. This paper analyzes these changes and proposes a new way for society to handle them: *risk governance*. On a parallel line

of work, in relation to CII (), one can consult "Policymaking for Critical Infrastructure. A Case Study on Strategic Interventions in Public Safety Telecommunications", by Gow [18].

While the regional monopolies of the past were well-equipped to handle most challenges to the system, individually or in cooperation with each other, the scale and geographical scope of the potential security risks requires decision-making at many different levels: by international bodies such as the EU and associations of TSOs, at the national level by governments and regulators, at the company level by generation companies, network companies, system operators etc., and finally, perhaps also by the end users themselves. As both the causes of the risks and the possible strategies for handling them often involve many different parties, this paper proposes an approach of risk governance to arrive at joint solutions amongst all the involved stakeholders in addition to the management of risks by individual parties.

The need for a new approach is partly due to the nature of the new risks, which range from terrorism and cyber attacks to international cascading blackouts, and partly due to the transformation of the national electricity systems into a continental infrastructure. In addition, the changing nature of the European electricity markets creates new vulnerabilities that need to be addressed. Liberalization has distributed control over the system among many more parties than used to be the case before, whereas the response to a contingency requires fast, coordinated actions. The increasing internationalization of the sector poses an additional challenge to contingency management across borders. In the near future, the European electricity infrastructure will be interconnected with North Africa, the Middle East, the whole Balkans, and substantial parts of Eastern Europe and Central Asia (from Lisbon to Vladivostok, and from the Arctic Circle to the Maghreb). Not the least, the ubiquitous application of ICT in every part of the sector creates many new opportunities but also incorporates new vulnerabilities.

Past methods of managing risk in the electricity industry are no longer adequate in the realities of the current ECESoS scenario. This is partly due to the emergence of new risks and also due to the restructuring of the electricity industry. In the past, utility companies with a regional monopoly could be held responsible for virtually every aspect of the delivery of electricity. Electric utilities managed technical risks as well as environmental and health risks, and it was common practice to apply cost-benefit analysis in order to fulfill primarily the shareholders concerns. This can have trans-European impacts.

The consequence of the current decentralized nature of liberalized electricity systems, is that individual actors cannot be held responsible for the way the system as a whole functions. This means that, more than in the past, issues such as reliability and resilience need to be addressed at the level of the whole system. This requires a new approach, which is *risk governance*, in addition to the risk management actions which were, and still need to be performed by the individual power companies. Risk governance admits the existence of multiple stakeholders, with their individual interests and viewpoints, in parallel with overall objectives (related to society as a whole). The decision-making process in general, and specifically that which is related to risks, has to take into consideration all these aspects. The diversity of objectives and actors has to be structured as a multi-criteria problem.

In a liberalized system, all these parties need to work together with each other, as well as with parties who do not directly influence the physical system such as traders, brokers, power exchanges, and retail companies. Through the risk governance process, the different affected actors (should) cooperate to handle risks that exceed the boundaries of

their own risk management processes. Risks that are (or should be) the subject of the risk governance processes are either risks that involve multiple actors or risks that originate outside the control of the involved actors.

Which issues should be dealt with through the risk governance process and which ones through the risk management process? If the solution is within the risk management loop, there is no need for governance of the issue. However, if the solution is beyond the powers of the actor who is affected, there is a need for risk governance.

## 8 CONCLUDING REMARKS: INTERDISCIPLINARY AND INTERNATIONAL DIMENSIONS

In the following we would like to summarize the main inferences drawn from the preceding discussions:

- European society is witnessing the advent of ECESoS, a new kind of human construct of great technical and organizational complexity, which—for technical and political reasons—is managed on a piecemeal basis by tens of entities. It is subject to risks that are critical for society. Those risks are of a very varied nature, and have to be counteracted with a proper approach which will inevitably be based on parallel assessments and decisions by many actors.
- The ECESoS is evolving into an "Electricity plus Information" (E+I) infrastructure. The operation of the power systems, the functioning of the markets, the links between industry, regulators, and users all are information-based. The efficiency of the system, the management of the security, the adequacy, and the market all are E+I matters. So, the electric service is now an E+I compound product.
- The new risk landscape faced by ECESoS can be deconstructed into three layers:
  - *Technical layer.* Risks are caused by technical deficiencies (including failure of components, human errors, and engineering flaws). Solutions are mainly technical in nature (e.g. strict application of information and communication security measures, proper training of operators, review of protection mechanisms). Some problems can be addressed by single actors, or by the joint effort of a limited group of them.
  - *System layer.* Risks are caused by the interaction of several technical, organizational and market factors, with effects that are not always predictable (e.g. the discrepancy between electricity flows demanded by the market, and the available capacity of transmission lines). Solutions have to unavoidably combine different aspects (e.g. technical, financial) and actors, at times crossing national boundaries.
  - *Societal layer.* Risks have a society-wide resonance, potentially affecting the proper performance of a whole community, its security and survivability. Due to the interconnectedness of ECESoS, these situations are transboundary by nature. Solutions have to address the infrastructure as a whole. This complexity calls for a European approach to risk governance.
- Most importantly, the central focus of the debate should consider the assessment and management processes related to the risk affecting the ECESoS as a whole:
  - ECESoS's emerging risks that are of relevance across Europe, have to be governed by means of a decision-making process tailored to its specific needs and

requirements. Key features to be considered are the multiplicity of stakeholders, the emergent security attributes of the infrastructure, and the dynamic nature of the system.

- In order to be successful, the *risk governance* of ECESoS needs to take into account all risk factors and all threats that cannot be dealt with adequately by individual actors' risk management processes. Risk governance should treat them in a comprehensive and systematic way: for example, bearing in mind power system dynamics, market incentives, ICT, and potential malicious attacks.
- Risk governance implies the *involvement of all stakeholders*, and clear rules for the deliberation and development of decisions. In Europe, due to the international nature of the problem, this situation will require the participation of national authorities, all businesses associated with the electric power infrastructure, international organizations, the European Union, and not least the end users.
- Risk governance is a new discipline, and more research is urgently needed to develop it. However, this should not discourage the application of current solutions to pressing problems such as those presented by ECESoS, because other alternatives are clearly less adequate.
- Risk governance needs to be *supported by proper tools*. The deployment of a risk governance process for the electric power infrastructure will require the utilization of advanced instruments (most likely based on digital platforms). These instruments should provide capabilities such as risk-related modeling, simulation, assessment, strategic gaming, metrics and visualization.

Implementing such a risk governance process for the ECESoS will require appropriate institutional settings. If nobody will be in charge of the problem, this can lead to two possible alternatives:

(a) the modification of the mission statements of current organizations of the power sector in Europe;
(b) the institution of a new organization with the specific purpose of governing the risks of ECESoS.

In the first case, the many political and industrial actors concerned with the problem will have to reflect upon the convenience of modifying the status of entities created for other purposes. In the case of similar initiatives in the USA, the certification of the North American Electric Reliability Corporation as the "Electric Reliability Organisation" with the power of U.S. Energy Policty Act [19] followed the long-term involvement of that organization with the security and adequacy of the power infrastructure. Europe does not have such an existing entity. Without trying to mimic that approach, there are some lessons worth considering: the potential effectiveness of self-regulation with a direct involvement of the operators of the power system, and the convenience in developing standards and guidance for security and reliability as a means for disseminating awareness and good practices, and promoting a common reference baseline.

The second line, that is creating a new entity for the governance of risks in the ECESoS, will require new legislative instruments. We can foresee that this road will not be straightforward–and we recognize that it is not considered a priority under the current political conditions. The focus of the attention is justifiably set on issues such

as emissions, renewable sources, and the consolidation of ownership, unbundling of the power infrastructure and the electric power markets. After the Third Energy Package issued in September 2007, no new initiatives are expected in the next few years unless a major event, as a significant blackout, proves the insufficiency of the current approaches.

With risk governance of the power infrastructure in Europe remaining an open issue, many questions still await satisfactory answers:

- Will the sum of the individual risk management measures by each operator of the ECESoS suffice to assure the reliability and security of the whole infrastructure?
- Is there a need for common standards? And in that case, is there a need for monitoring and enforcing compliance? Compliance can be guaranteed by a set of different mechanisms: peer pressure, penalties, economic incentives, etc. The verification of capabilities can be linked to certification, auditing, and other qualification procedures. Who will decide this?
- While facing systemic risks, which are the appropriate joint capabilities and how can they be developed?

A typical attribute of risk is that it is made fully apparent only with the occurrence of detrimental events which could even degenerate into disasters with catastrophic consequences. Then not only is it too late for any risk management action, but infrastructure and society might suffer serious negative consequences for years. In this respect, Europe still needs to develop a comprehensive strategy.

## REFERENCES

1. Gheorghe, A. V., Masera, M., Weijnen, M., and De Vries, L. J. (2006). *Critical Infrastructures at Risk: Securing the European Electric Power System*. Springer, Dordrecht.
2. Council (2008). *Council Directive, 2008/114/EC, European Commission, December 8, 2008*.
3. Council (2004a). *10679/2/04 Rev. 2, No. 19*.
4. European Commission (2004a). *Communication from the Commission to the Council and the European Parliament, Critical Infrastructure Protection in the Fight Against Terrorism, Brussels, October 20, 2004, COM/2004/702 final*.
5. Council (2004b). *Conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks", Adopted on December 2, 2004*.
6. European Commission (2005). *Green Paper on a European Programme for Critical Infrastructure Protection, Presented by the Commission on November 17, 2005, COM/2005/576 final*.
7. European Commission (2006a). *Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A Strategy for a Secure Information Society - "Dialogue, Partnership and Empowerment'', Presented by the Commission on June 2, 2006*.
8. European Commission (2006b). *Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection, Presented by the Commission on December 12, 2006, COM/2006/787 final*.
9. European Commission (2007). *Communication on Protecting Europe's Critical Energy and Transport Infrastructure, Adopted by the Commission on February 2, 2007 (restricted)*.

10. European Commission (2009). *Communication "Protecting Europe from Large Scale Cyber-attacks and Disruptions: Enhancing Preparedness, Security and Resilience"*, COM/2009/149.
11. Thissen, W. A. H., and Herder, P. M. (2003). *Critical Infrastructures. State of the Art in Research and Application*. Kluwer Academic, Dordrecht.
12. European Commission (2003b). *Directorate-Generale for Energy and Transport, Memo, Energy Infrastructures: Increasing Security of Supply in the Union, December 2003*.
13. Midttun, A. (1997). *European Electricity Systems in Transition*. Elsevier Science, Ltd., Amsterdam , The Netherlands.
14. European Commission (2004b). *Directorate-Generale for Energy and Transport, Memo, Towards a Competitive and Regulated European Electricity and Gas Market*.
15. European Commission (2003). *Directive of the European Parliament and the Council of June 26, 2003 Concerning Common Rules for the Internal Electricity Market; Official Journal L 176, 2003/54/EC, July 15, 2003*.
16. European Commission (2003d). *Regulation of the European Parliament and the Council of June 26, 2003 Concerning Conditions for Access to the Network for Cross-border Exchange in Electricity, Official Journal L 176, 1228/2003, July 15, 2003*.
17. European Commission (2003c). *Proposal for a Directive of the European Parliament and the Council Concerning Measures to Safeguard Security of Electricity Supply and Infrastructure Investment, COM/2003/740*.
18. Gow, G. A. (2005). *Policymaking for Critical Infrastructure. A Case Study on Strategic Interventions in Public Safety Telecommunications*. Ashgate Publishing Co, Hampshire.
19. U.S. Energy Policy Act (2005). *Public Law 109-58*. Available at http://www.gpo.gov/fdsys/pkg/PLAW-109publ58/content-detail.html.

# VULNERABILITY ASSESSMENT METHODOLOGIES FOR INTERDEPENDENT SYSTEMS

WADE R. TOWNSEND

*U.S. Department of Homeland Security, Washington, D.C.*

## 1 INTRODUCTION

The importance of infrastructure interdependencies was first highlighted at the national level by the President's Commission on Critical Infrastructure Protection (PCCIP) [1, 2].

The energy sector (both industry and government) was proactive in recognizing the need to include interdependencies into vulnerability assessments and infrastructure analyses. The National Petroleum Council report, *Securing Oil and Natural Gas Infrastructures in The New Economy*, identified the need to include interdependencies considerations in all aspects [3]. The new business model (e.g. globalization, increasing reliance on other infrastructures) is complex and requires a broad perspective to include interdependencies analyses. The level of dependency among all critical infrastructures continues to rise due to increasing reliance on one another (e.g. information technology, telecommunications, and electric power).

An example of increasing dependencies and interdependencies is the Northeast Blackout in 2003. Even though this event began in the electric sector, other infrastructures were quickly impacted. Cleveland, OH, and Detroit, MI, lost pressure in their water systems and had to issue boil water advisories. Both cities rely on electric power to operate their pumps and had inadequate backup power available to continue pump operations, and thus, could not maintain pressure in their water systems. The 2003 power outage also affected the telecommunications network. Although the telephone systems remained operational in most areas, the increased demand caused some switches to reach their capacity, resulting in some blocked calls. Cell phone users also experienced service disruptions because cellular towers generally have only battery banks with limited battery backup. Many other infrastructures, such as wastewater treatment, transportation systems, gasoline distribution including pumps, and heating, ventilation, and air-conditioning (HVAC), and fire suppression systems were also impacted.

Widespread infrastructure disruptions stress the need to look at entire systems and not just individual facilities when conducting vulnerability assessments. Many infrastructures are designed with operational redundancies so the overall system can withstand the loss of any one asset, but when multiple assets are taken offline, an entire infrastructure service can be disrupted. Hurricanes Katrina and Rita crippled several infrastructures with cascading effects to other regions throughout the country. Natural gas prices throughout the nation were impacted by these hurricanes. Even telecommunications networks hundreds of miles away from the impact areas were affected by the storms.

In 1988, in response to the PCCIP findings along with the increasing concerns about vulnerabilities from interdependencies, Department of Energy (DOE), coordinating with industry, developed the Vulnerability and Risk Analysis Program (VRAP). VRAP included the development and implementation of a vulnerability assessment methodology for the energy sector that included interdependencies. Interdependencies considerations are crucial to risk analysis in providing a holistic perspective. Teams of national laboratory experts, led by Argonne National Laboratory and working in partnership with the energy industry, successfully applied the methodology to help organizations in the energy sector to identify and understand the threats and vulnerabilities (physical, cyber, and interdependencies) of their infrastructures. Approximately 75 vulnerability assessments were conducted by DOE from 1997 to 2002. Lessons learned from these assessments, as well as best practice approaches to mitigate vulnerabilities, were documented. Several reports were developed and shared with industry to promote risk analysis. These documents include the following.

- *Vulnerability Assessment and Survey Program: Overview of Assessment Methodology* [4],

- *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities* [5],
- *Vulnerability Assessment Methodology: Electric Power Infrastructure* [6],
- *Energy Infrastructure Vulnerability Survey Checklists Template* [7], and
- *Vulnerability and Risk Analysis Program: Lessons Learned and Best Practices* [8].

Some of the lessons learned from these initial vulnerability assessments in regards to interdependencies are provided below.

- Interdependencies among infrastructures must be thoroughly investigated because they can create subtle interactions and feedback mechanisms that often lead to unintended behaviors and consequences. Problems in one infrastructure can cascade to other infrastructures.
- Interdependencies increase the complexity of infrastructures and introduce additional vulnerabilities.
- Interdependencies among infrastructures vary significantly in scale and complexity, and they also typically involve many system components. The process of identifying and analyzing these linkages requires a detailed understanding of how the components of each infrastructure and their associated functions or activities depend on, or are supported by, each of the other infrastructures.
- Contingency and response plans need to be evaluated from an infrastructure interdependencies perspective, and coordination with other infrastructure providers needs to be enhanced.

In March 2003, with the stand up of Department of Homeland Security (DHS), the DOE VRAP was absorbed by DHS/IP, and the core vulnerability assessment methodology (including interdependencies) became the foundation for DHS/IP risk analysis. DHS/IP conducted a survey of existing vulnerability assessment methodologies to identify element areas including interdependencies. This report, *Survey of Vulnerability Assessment Methodologies*, noted that the interdependencies element area was not considered in most existing government and industrial methodologies [9].

The DHS/IP Site Assistance Visit Program and Buffer Zone Protection Program's methodologies leveraged the DOE efforts and included the interdependencies element [10, 11]. Other DHS program methodologies (e.g. Risk Analysis and Management for Critical Asset Protection and Comprehensive Reviews) incorporated and refined the interdependencies element area. For example, Comprehensive Reviews include dependencies between critical facilities within a community with first responders and emergency management entities. GIS technologies bolster the DHS program methodologies and assist assessment teams in identifying infrastructure dependencies and interdependencies (e.g. single point failures and common corridors) [12].

## 2 PETROLEUM REFINERY INTERDEPENDENCIES

In early 2003, a joint industry/government working group was formed to develop a vulnerability assessment methodology for the oil infrastructure that focused on petroleum refineries and included physical and cyber security along with interdependencies. At the time, several oil industry firms were using the Center for Chemical Process Safety

(CCPS), *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites* [13]. Although no universal methodology was adopted, the CCPS was the most common since petroleum refineries share similarities with chemical facilities. Also, many oil companies own both energy and chemical facility assets. The CCPS methodology provided a sound foundation for physical security. The DOE/DHS interdependencies element area was leveraged and integrated into the CCPS methodology, resulting in a customized methodology for the oil infrastructure that was adopted by the American Petroleum Institute (API) and the National Petrochemical & Refiners Association (NPRA) [14].

The petroleum refinery methodology includes vulnerabilities from interdependencies including information technology, making the methodology more inclusive and comprehensive. While traditional assessments focused on on-site physical security (e.g. gates, guards, and guns), the API/NPRA methodology considers a facility's supporting infrastructure, supply chain, cyber infrastructure, operations security, as well as physical security. Thus, in order to examine vulnerabilities at a petroleum refinery, it is crucial to understand the inputs and outputs along with the various functions that take place. Figure 1 illustrates the systems' representation concept for interdependency analysis. It is important to map inputs and outputs (e.g. robustness and redundancy considerations) against key asset functions (e.g. criticality to operations). Within the assessment process, if an input is not critical to operations, then it is a lower priority.

Interdependency analysis also includes both upstream and downstream considerations. Figure 2 illustrates the petroleum fuel cycle. Petroleum refineries are a midstream function, or, part of the processing stage. For the entire petroleum infrastructure to operate, all stages of the fuel cycle, from production to distribution, must be functional. A disruption in any stage of the fuel cycle has the ability to ripple throughout the petroleum infrastructure and potentially cascade to other critical infrastructures. Petroleum refineries require oil production and gathering for sufficient crude oil (petroleum refinery inputs). Refineries typically maintain a limited supply of crude oil on-site, which can be quickly depleted

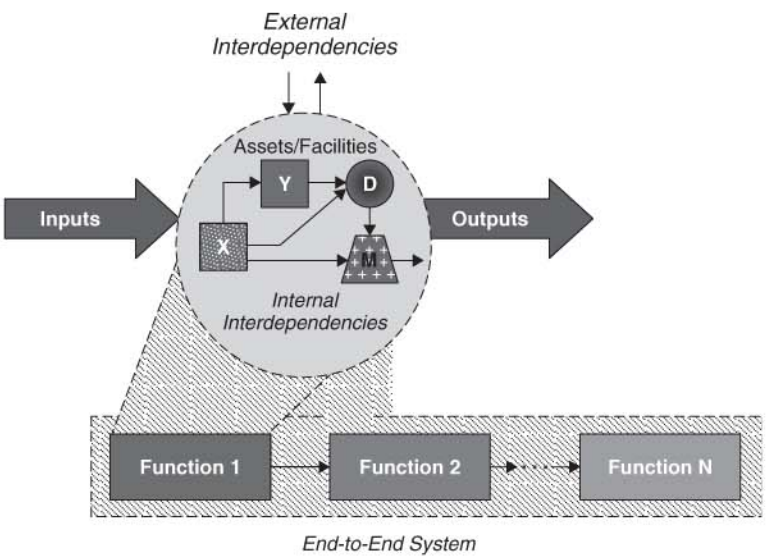



**FIGURE 1** Systems representation for interdependencies analysis.

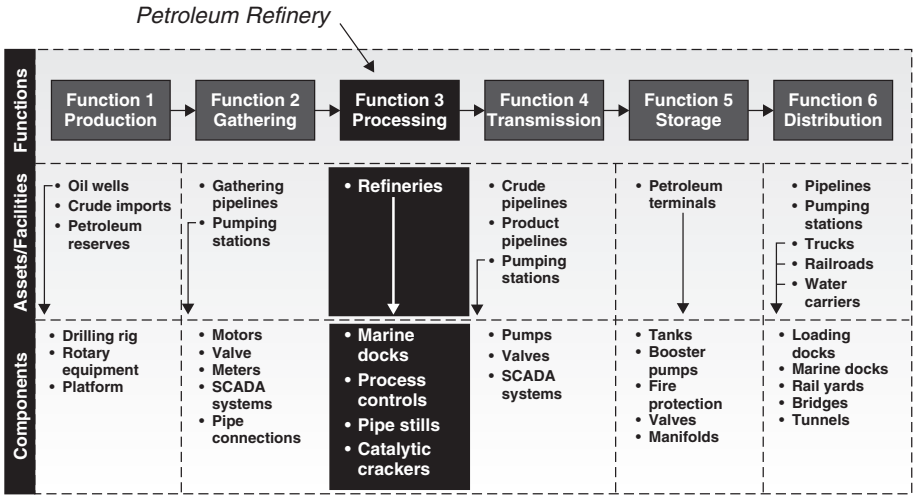



**FIGURE 2** Petroleum fuel cycle.

and result in a shutdown of the refining process if oil production and processing stages do not replenish the on-site supplies. The downstream petroleum refinery impacts are similar. If the transmission, storage, and distribution stages are nonfunctional, petroleum refineries may shut down.

Figures 1 and 2 illustrate the broader perspective that is taken through interdependencies analysis. Figure 3 provides a high-level view of petroleum refinery interdependencies to include suppliers and distributors. Petroleum refinery interdependencies include crude oil that can be deliverable by tanker, pipeline, barge, or rail; process chemicals (e.g. hydrogen, alkylation acids, and nitrogen); and other infrastructures (e.g. electric power, natural gas, water, telecommunications, and so on). All of these inputs are required to produce refined petroleum products (e.g. gasoline, heating oil, diesel, and so on) and

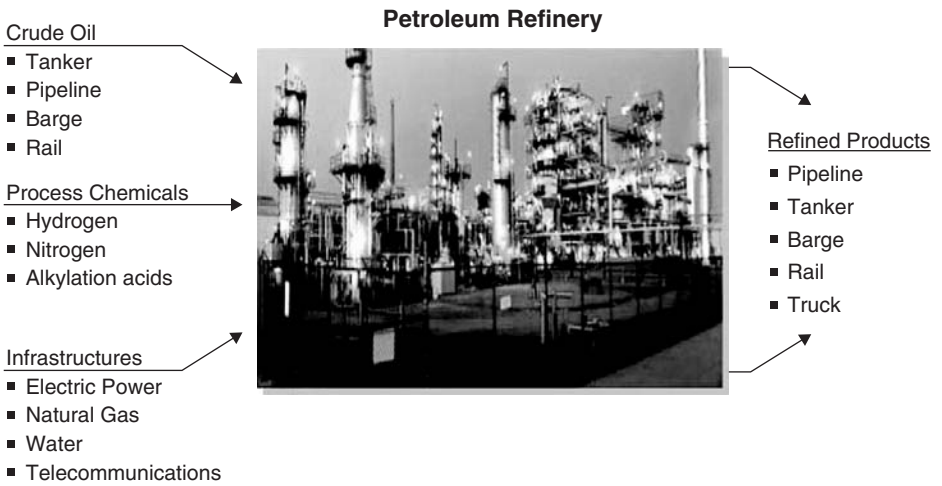



**FIGURE 3** Petroleum refinery macro illustration of interdependencies.

the resulting complex dependencies and interdependencies. Since petroleum refineries require many inputs and outputs and rely on multiple infrastructures, they provide an excellent representation of interdependency analysis.

Figures 4 and 5 further break down the petroleum refinery interdependencies model. Figure 4 identifies internal interdependencies (inside the petroleum refinery) and Figure 5

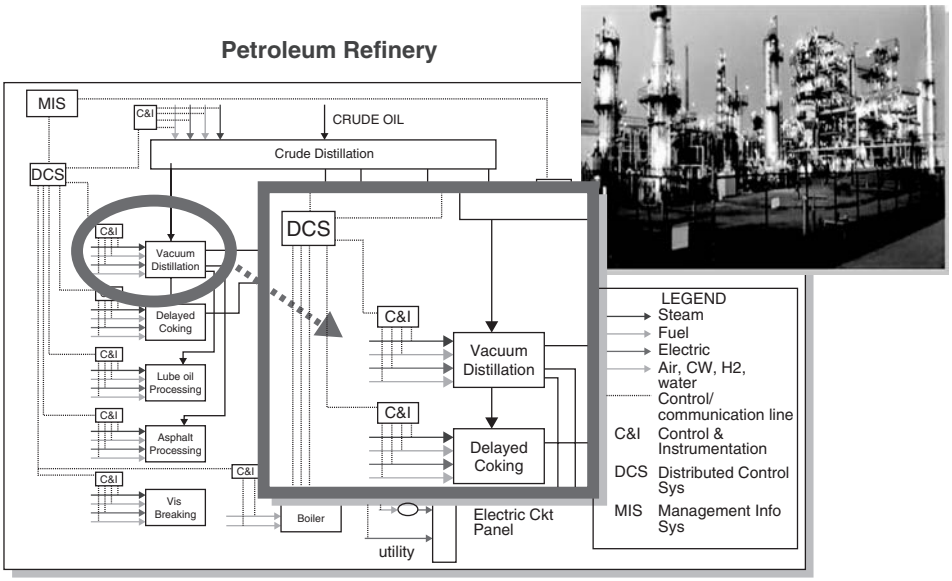



**FIGURE 4** Example of petroleum refinery internal interdependency.

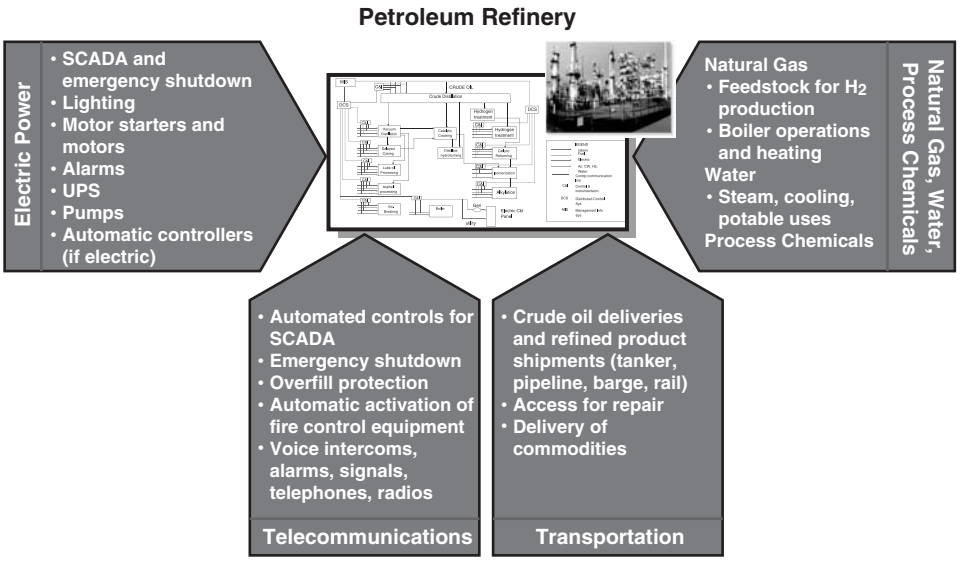



**FIGURE 5** Example of petroleum refinery external interdependency.

**TABLE 1 Interdependencies Survey Questions**

| **Checklist Considerations: Interdependencies Survey** |
|---|
| *(a) Infrastructure Oversight* |
| Does the facility have a department responsible for overseeing all or most the infrastructures? |
| *(b) Infrastructure Procedures* |
| In general, are operating procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, their availability to relevant staff, and the extent to which they are regularly followed. |
| Are contingency procedures in place for the systems that make up the internal infrastructures and for the physical connections and contracts with the external infrastructures that support them? Describe the extent of these procedures, their format, and their availability to relevant staff (Note: contingencies refer to situations brought about by a failure or disruption within an infrastructure or the infrastructures that support it.). |
| If they exist, have the contingency procedures been tested and are they exercised regularly either as a part of normal operations as through specially designed drills? Describe the drills and their results. |
| *(c) Electric Power Supply and Distribution* |
| Primary source of electric power |
| If the primary source of electric power is a commercial source, are there multiple independent feeds? If so, describe the feeds and their locations. Also specify who controls the termination points of any multiple feeds. |
| If the primary source of electric power is a system operated by the facility or asset, what type of system is it? |
| Electric distribution system |
| Are the components of the electric system that are located outside of buildings (such as generators, fuel storage facilities, transformers, and transfer switches) protected from vandalism or accidental damage by fences or barriers? If so, describe the type of protection and level of security it provides. |
| Are the various sources of electric power and the components of the internal electric distribution systems such that they may be isolated for maintenance or replacement without affecting the critical functions of the asset/facility? If not, describe the limitations. |
| Have any single points of failure been identified for the electrical power supply and distribution system? If so, list them and describe. |
| Backup electric power systems |
| Are there additional emergency sources of electric supply beyond the primary system (such as multiple independent commercial feeds, backup generators, and uninterruptible power supply [UPSs])? If there are, describe them and who controls them. |
| Commercial electric power sources |
| How many substations feed the area of the asset/facility and the asset/facility itself? That is, is the area supplied by multiple substations? If more than one, which ones have sufficient individual capacities to supply the critical needs of the asset/facility? |

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| **Checklist Considerations: Interdependencies Survey** |
|---|
| Commercial electric power pathways |
| Are the power lines into the area of the asset/facility and into the asset/facility itself above ground (on utility poles), buried, or a combination of both? If both, indicate locations of portions above ground. |
| *(d) Petroleum Fuels and Bulk Chemicals Supply and Storage* |
| Uses of petroleum fuels and bulk chemicals |
| Are petroleum fuels or bulk chemicals used in normal operations at the asset/facility? If yes, specify the types and uses. |
| Reception facilities |
| How are the various petroleum fuels and bulk chemicals normally delivered to the asset/facility? Indicate the delivery mode and normal frequency of shipments for each fuel type. |
| Supply contracts |
| Are contracts in place for the supply of petroleum fuels and bulk chemicals? Specify the name of the contractors, the types of contracts, the modes of transport (pipeline, rail car, tank truck, etc.), and the frequency of normal shipments. |
| *(e) Natural Gas Supply* |
| Sources of natural gas |
| How many city gate stations supply the natural gas distribution system in the area of the asset/facility and the asset/facility itself?<br>How may distinct independent transmission pipelines supply the city gate stations? Indicate if an individual gate station is supplied by more than one transmission pipeline and which stations are supplied by independent transmission pipelines. |
| Natural gas contracts |
| Does the asset/facility have a firm delivery contract, an interruptible contract, or a mixed contract with the natural gas distribution company or the transmission companies? Specify the companies involved and specify whether there is a direct physical link (pipeline) to each company. |
| *(f) Telecommunications* |
| Internal telephone system |
| What types of telephone systems are used within the asset/facility? Are there multiple independent telephone systems? Specify the types of systems, their uses, and specify whether they are copper-wire or fiber-optic based.<br>If there are multiple (from independent systems) or redundant (from built-in backups) switches and cables, are they physically separated and isolated to avoid common causes of failure?<br>Are the telephone switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify types of protection provided. |

**TABLE 1 (*Continued*)**

| **Checklist Considerations: Interdependencies Survey** |
|---|
| Data transfer |
| If there is a separate system for large volume and high-speed data transfer, are there redundant switches and cables. If yes, describe the situation. |
| If there are redundant switches and cables, are they physically separated and isolated to avoid common causes of failure? |
| Are the data transfer switches located in limited-access or secured areas away from potential damage due to weather or water leaks? Specify the types of protection provided. |
| Cellular/wireless/satellite systems |
| Are cellular/wireless/satellite telephones and pagers in widespread use within the asset/facility? If yes, briefly describe their uses. |
| Intranet and e-mail system |
| Is the asset's/facility's Intranet and e-mail system dependent on the asset's/facility's computers and servers or telephone system? If yes, describe the dependence. |
| Are there any critical operational items that require use of the e-mail system or internet? |
| Redundant access to intranet and e-mail system |
| Does the asset/facility have a backup or redundant Intranet and e-mail system? If yes, describe the system and the amount of backup it provides. Does an outside contractor maintain the backup? If so, what type of security oversight measures does the contractor have in place? |
| On-site fixed components of microwave/radio system |
| Are there multiple or redundant radio communications systems in place within the asset/facility? If yes, specify the types of systems and their uses. |
| Mobile and remote components of microwave/radio system |
| Are there mobile components to the radio communications system (such as on vehicles or vessels)? If yes, describe the mobile components. |
| Are the mobile components of the radio communications system protected from vandalism or accidental damage by locked boxes or lockable vehicle cabs? Specify the types of protection and level of security they provide. |
| Commercial telecommunications' carriers |
| Are there multiple telecommunications carriers used by the asset/facility (possibly commercial, contracted, or organization-owned)? List them, specify the service they provide or the type of information carried (such as analog telephone voice and FAX, digital telephone voice, Internet connections, and dedicated data transfer), and the type of media used (copper cable, fiber-optic cable, microwave, and satellite) |
| Pathways of commercial telecommunications' cables |
| Are the telecommunications' cables into the area of the asset/facility and into the asset/facility itself above ground (on utility poles), buried, or a combination of both? If both, indicate locations of portions above ground. |

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| **Checklist Considerations: Interdependencies Survey** |
|---|
| Are the paths of the telecommunications cables located in areas susceptible to natural or accidental damage (such as overhead cables near highways; cables across bridges, dams, or landslide areas)? If yes, indicate the locations and types of potential disruptions. |
| Backup communications systems |
| Are there redundant or backup telephone systems in place if the primary system is disrupted? Specify the extent to which the secondary systems can support the critical functions and activities at the asset/facility. |
| *(g) Transportation* |
| Road and rail access |
| Are there multiple roadways or rail routes into the area of the asset/facility? Describe the route or routes and indicate any load or throughput limitations with respect to the needs of the asset/facility. |
| Airports and air routes |
| Are there multiple airports in the area of the site of sufficient size and with sufficient service to support the critical functions and activities at the asset/facility? Enumerate the airports and indicate any limitations.<br>Are there any regular air routes that pass over or near the asset/facility that could present a danger to the asset/facility if there were some sort of an air disaster? Record any concerns. |
| Waterway access |
| Are there multiple water routes to the ports, harbors, or landings used by the asset/facility from the open ocean or major waterway? Describe the route or routes and indicate any load, draft, beam, or throughput limitations with respect to the needs of the organization. |
| Pipeline Access |
| What materials, feedstocks, or products (such as crude oil, intermediate petroleum products, refined petroleum products, or liquefied petroleum gas) are supplied to or shipped from the asset/facility by way of pipeline transportation?<br>Are there multiple pipelines and pipeline routes into the area of the asset/facility from major interstate transportation pipelines? If yes, indicate which pipelines or combinations of pipelines have sufficient capacity to serve the asset/facility.<br>Are the paths of the pipelines colocated with the rights-of-way of other infrastructures? If yes, indicate how often and where they follow the same rights-of-way and the infrastructures that are colocated.<br>Are the paths of the pipelines located in areas susceptible to natural or accidental damage (such as across bridges or dams, in earthquake or landslide areas)? If yes, indicate the locations and types of potential disruptions. If disruptions due to scheduled maintenance or system modifications occur, how is this communicated to your organization? |
| *(h) Water and Wastewater* |
| Primary domestic/industrial water system |
| Does the asset/facility have a domestic/industrial water system? If yes, specify the uses of the water. |

**TABLE 1 (*Continued*)**

| **Checklist Considerations: Interdependencies Survey** |
|---|
| Does the water supply for the domestic/industrial water system come from an external source (such as community, city, or regional water mains) or from an internal system (such as wells, river, or reservoir)? If internal, describe the system. |
| Backup domestic/industrial water system |
| Is there an independent backup water source to the primary domestic supply system? If yes, specify the type of backup system (such as wells, river, reservoir, and tank truck), describe the specific source of the water, indicate the adequacy of the backup supply's capacity, and indicate if it is gravity feed or requires active pumps (generally electric). |
| Primary industrial wastewater system |
| Does the asset/facility have an on-site industrial wastewater system? If yes, specify the types of wastewater that are processed and the processes used. |
| Backup wastewater system |
| Is there an independent backup system that can be used to handle the industrial wastewater? If yes, specify the type of backup system (such as a redundant system, holding ponds, and temporary discharge of unprocessed wastewater), describe the specific process, indicate the adequacy of the backup's capacity and any limitations on how long it can operate, and indicate if it is gravity feed or requires active lift pumps (generally electric). |
| Commercial/public water/wastewater supply reliability |
| Historically, has the city water/wastewater supply in the area been reliable and adequate? Quantify the reliability and specify any shortfall in the supply pressure or flow rate. |
| Typically, when disruptions in the city water/wastewater supply occur, are they of significant duration (as opposed to just a few hours)? Quantify in terms of potential effects on the critical functions and activities at the asset/facility. |
| *(i) Emergency Services (Police, Fire, And Emergency Medical)* |
| Local police, county/state police, and federal bureau of investigation (FBI) |
| How are these agencies involved in protecting the asset/facility? |
| What are typical response times and response capabilities? |
| Fire department and emergency medical services |
| How are these agencies involved in protecting or treating the asset/facility? |
| Do they provide inspection and/or certification services? |
| What are typical response times and response capabilities? |
| *(j) Computers and Servers (Mainframes, Firewalls, and Router Equipment)* |
| Electric power sources |
| Are there provisions within the asset's/facility's primary electric power supply and distribution system to supply power for the computers and servers? If yes, indicate under what conditions and for how long. |
| Do the computers and servers have their own backup electric power supply (such as local UPSs or generators)? If yes, specify the types of backup and how long they can operate. |

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| **Checklist Considerations: Interdependencies Survey** |
|---|
| Environmental control |
| Does the asset's/facility's central HVAC system provide environment control to the computer and server areas or do the computer and server areas have their own independent environmental control system? If they have their own system, specify the type. |
| Protection |
| Is there special physical security provided for the computer and server areas? If yes, specify the type of security and the level of protection provided. |
| *(k) HVAC System (Air Handlers, Heating Plants, Cooling Towers, and Chillers)* |
| Primary HVAC system |
| Can critical functions and activities dependent on environmental conditions continue without the HVAC system? If yes, specify which functions and for how long they can continue under various external weather conditions. |
| Backup HVAC systems |
| Is there a separate backup or contingency plan for the HVAC system? If yes, describe the system and the energy and water supply systems it requires. |
| *(l) Fire Suppression and Fire Fighting System* |
| Alarms |
| Does the entire asset/facility (or at least most of it) have a fire and/or smoke detection and alarm system? If yes, specify the type of system, how it is monitored, and the response procedure. |
| Fire suppression |
| Does the entire asset/facility (or at least most of it) have a fire suppression system such as an overhead sprinkler system? If yes, specify the medium (usually water) and whether it is of the flooded-pipe or prearmed type.<br>Does the water supply for the fire suppression system come from city water mains or an on-site system, such as wells, rivers, or reservoir? |
| Other systems |
| Is there special fire suppression equipment, such as Halon, Inergen, inert gases, or carbon dioxide in certain areas such as computer or telecommunications areas? If yes, indicate the types and adequacies of these special systems. |
| *(m) SCADA System* |
| Type of system |
| Does the asset/facility make use of a substantial SCADA system (i.e. one that covers a large area or a large number of components and functions)? If yes, indicate what functions are monitored and/or controlled, the type of system, and the extent of the system. |

**TABLE 1 (*Continued*)**

| **Checklist Considerations: Interdependencies Survey** |
|---|
| Control centers |
| Where is the primary control center for the SCADA system located?<br>Is there a backup control center? If yes, where is it located? Is it sufficiently remote from the primary control center to avoid common causes of failure, such as fires, explosions, or other large threats? |
| *(n) Physical Security System* |
| Electric power sources |
| Are the asset's/facility's monitoring and alarm systems normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e. is the asset's/facility's primary electric power supply and distribution system the primary electric power source?)?<br>If there a backup system that can support all the functions of the monitoring and alarm systems in terms of capacity? Specify for how long it can operate. |
| Communications pathways |
| Are the asset's/facility's monitoring and alarm systems normally dependent upon the asset's/facility's telephone system? |
| Computer support |
| Are the asset's/facility's monitoring and alarm systems normally dependent upon the facility's main computers and servers? |
| *(o) Financial System (Including Monetary Transactions)* |
| Electric power sources |
| Are the asset's/facility's financial systems and functions normally dependent on the asset's/facility's primary electric power supply and distribution system (i.e. is the facility's electric power supply and distribution system the primary electric power source?)? |
| Communications pathways |
| Are the asset's/facility's financial systems and functions normally dependent upon the asset's/facility's telephone system? |
| Computer support |
| Are the asset's/facility's financial systems and functions normally dependent upon the facility's main computers and servers? |

identifies external interdependencies (outside the petroleum refinery). Internal interdependencies include on-site energy generation, process control and monitoring, and steam. External interdependencies include commercial electricity, water sources, and feedstock. The primary focus is on critical interdependencies where loss would severely degrade or shut down operations and where no redundancy or limited redundancy exists.

By answering specific questions, assessment teams are able to determine which internal and external infrastructures are critical to operations and the redundancies of these systems. The question areas include infrastructure oversight, infrastructure procedures, and infrastructure considerations. It is important to note that although many questions are the same across all sectors, sector specific questions also have been developed. For example, the *Security Vulnerability Analysis Methodology for the Petroleum Industry* [14] provides detailed questions associated with each of these categories. A subset of infrastructure dependency questions is provided in Table 1.

## 3 NEXT STEPS

The interdependency element area is evolving and should continue to develop. DOE and DHS programs have provided a foundation for this work, and several current programs within the government and industry continue to leverage this effort. For example, the State of Ohio has adopted the interdependency questions into its statewide vulnerability assessment model in identifying state vulnerabilities and mitigation strategies. The State of Ohio had an existing vulnerability assessment template; however, the template was based on physical security. The state recognized the need for an interdependencies perspective to broaden its perspective and to help prioritize mitigation options. Thus, the state integrated a subset of the interdependency questions presented into its template.

Another example is the Pacific Northwest Economic Region (PNWER) that has conducted interdependencies seminars to bring regional stakeholders together. PNWER has developed an Infrastructure Interdependencies Identification and Assessment Tool to identify detailed interdependencies-related information relevant to operations and business continuity, and to determine appropriate ways to share data among stakeholder organizations. The questions implemented in the tool were based on the interdependency questions mentioned. The tool is helping PNWER to better understand, at a regional level, their supply chains and infrastructure dependencies and interdependencies. Taking a regional perspective allows for a more holistic approach to interdependencies and provides insights into bottlenecks within the region.

DHS continues to leverage the interdependencies work into various ongoing programs. DHS has evolved from conducting vulnerability assessments to conducting risk assessments. However, interdependencies have become increasingly important since risk comprises threats, vulnerabilities, and consequences. Each of these risk elements requires an interdependencies perspective to properly identify and quantify risk. The various assessment methodologies at DHS/IP (e.g. Site Assistance Visits, Buffer Zone Protection Plans, Comprehensive Reviews, Maritime Security Risk Assessment Model, and Risk Analysis and Management for Critical Asset Protection) continue to evolve interdependencies aspects in different ways.

## REFERENCES

1. *President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures*, October (1997).
2. Peerenboom, J., Fisher, R. (2008). *System and Sector Interdependencies: An Overview*, Wiley and Sons, New York.
3. National Petroleum Council (2001). *Securing Oil and Natural Gas Infrastructures in the New Economy*, June 2001.

4. U.S. Department of Energy (2001). *Vulnerability Assessment and Survey Program: Overview of Assessment Methodology*, September 2001.
5. U.S. Department of Energy (2002). *Energy Infrastructure Risk Management Checklists for Small and Medium Sized Energy Facilities*, August 2002.
6. U.S. Department of Energy (2002). *Vulnerability Assessment Methodology: Electric Power Infrastructure*, September 2002.
7. U.S. Department of Energy (2002). *Energy Infrastructure Vulnerability Survey Checklists Template*, February 2002.
8. U.S. Department of Energy (2001). *Vulnerability and Risk Analysis Program: Lessons Learned and Best Practices*, September 2001.
9. U.S. Department of Homeland Security (2003). *Survey of Vulnerability Assessment Methodologies*, September 2003.
10. U.S. Department of Homeland Security (2007). *Site Assistance Visit Methodology Template*.
11. U.S. Department of Homeland Security (2007). *Buffer Zone Protection Plan Template*.
12. Adduci, A., Bailey, S., Fisher, R. (2008). *Geospatial Data Support for Infrastructure Interdependencies Analysis*, Wiley and Sons, New York.
13. Center for Chemical Process Safety (2003). *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites*.
14. American Petroleum Institute and National Petrochemical & Refiners Association (2003). *Security Vulnerability Analysis Methodology for the Petroleum Industry*. May 2003.

# ROBUSTNESS, RESILIENCE, AND SECURITY OF NATIONAL CRITICAL INFRASTRUCTURE SYSTEMS

S. MASSOUD AMIN[I]

*University of Minnesota, Minneapolis, Minnesota*

## 1 NATIONAL CRITICAL INFRASTRUCTURE SYSTEMS: UNDERPINNING OUR ECONOMY, GLOBAL COMPETITIVENESS, SECURITY, AND QUALITY OF LIFE

Virtually every crucial economic and social function depends on the secure, reliable operation of energy, telecommunications, transportation, financial, and other infrastructures.

[I]Honeywell/H.W. Sweatt Chair in Technological Leadership, Director of the Technological Leadership Institute, Professor of Electrical & Computer Engineering, and University Distinguished Teaching Professor. Contact information: amin@umn.edu, or http://umn.edu/amin.

Indeed, they have provided much of the good life that the more developed countries enjoy. However, with increased benefit has come increased risk. As these infrastructures have grown more complex to handle a variety of demands, they have become more interdependent.

The Internet, computer networks, and our digital economy have increased the demand for reliable and disturbance-free electricity; banking and finance depends on the robustness of electric power, cable, and wireless telecommunications. Transportation systems, including military and commercial aircraft and land and sea vessels, depend on communication and energy networks. Links between the power grid and telecommunications and between electrical power and oil, water, and gas pipelines continue to be a lynchpin of energy supply networks. This strong interdependence means that an action in one part of one infrastructure network can rapidly create global effects by cascading throughout the same network and even infiltrating other networks.

A growing portion of the world's business and industry, art and science, entertainment and even crime are conducted through the World Wide Web and the Internet. But the use of these electronic information systems depends, as do the more mundane activities of daily life, on many other complex infrastructures, such as cable and wireless telecommunications, banking and finance, land, water, and air transportation, gas, water, and oil pipelines, and the electric power grid. All of these are, themselves, complex networks, geographically dispersed, nonlinear, and interacting both among themselves and with their human owners, operators, and users. Energy, telecommunications, transportation, and financial infrastructures are becoming increasingly interconnected, thus, posing new challenges for their secure and reliable operation.

*What is "Infrastructure"?* Infrastructure is the linked sociotechnological system of facilities and activities that provides the range of essential services generally necessary to support our economy and quality of life.

*What is a sociotechnological system?* Sociotechnological systems include the physical infrastructure, the people, and organizations who build, run, and use it, as well as the economic and legal conditions for operations.

There is reasonable concern that both national and international energy and information infrastructures have reached a level of complexity, and interconnection which makes them particularly vulnerable to cascading outages, initiated by material failure, natural calamities, intentional attack, or human error. The potential ramifications of network failures have never been greater, as the transportation, telecommunications, oil and gas, banking and finance, and other infrastructures depend on the continental power grid to energize and control their operations. Although there are some similarities, the electric power grid is quite different from gas, oil, or water networks-phase shifters rather than valves are used, and there is no way to store significant amounts of electricity. To provide the desired flow on one line often results in "loop flows" on several other lines.

Our studies in the areas of stability, robustness, resilience, and security span from marco systems (including interdependent national infrastructure and enterprises), to micro (individuals/people) within these large-scale uncertain systems, which are modeled as complex adaptive systems.

As a "micro" example, living beings must constantly adapt to changing environmental conditions and turbulence. Some seem inherently more capable of this resilient adaptation than others. As with leadership in general, there are some innate attributes that predispose

some to be more resilient than others. And as cumulative life stress increases pushing one to his/her "maximum emotional capacity" we need to learn to diffuse some of this emotion or it will push us beyond our upper control limit (i.e. exceed our maximum emotional bandwidth). The key is to learn to manage our "signal to noise ratio" in such a way that we never lose sight of our own unique inner signal. Similarly, understanding how to transform our complex infrastructure systems to be much more sensitive, discerning yet resilient, robust, and adaptive will represent a breakthrough in systems engineering.

As the world becomes increasingly VUCA (volatile, uncertain, complex, and adaptive), resulting in a wide spectrum of opportunities and challenges of complex systems abound, and concerns about the instability of these systems and their potential for large and possible catastrophic regime shifts are a dominant social concern, with "systemic risk" as a generic problem.

These concerns are at the leading edge of many environmental and engineering sciences: for example, in atmospheric science in studies of climate change; for financial risk management in the couplings and resultant systemic risks; for fisheries managers concerned with the sudden collapse of certain economically important fish stocks; for communication networks concerned with system reliability and security in the face of evolving cyber risks; in electrical and power engineering concerned with preventing disruptions to the North American power grid.

The commonality of the problem of stability and resilience to shocks in complex systems that these examples point to raises the possibility that approaches to risk management in natural and physical systems with pertinence to nearly all aspects of our lives. Some of the methods for managing risk in engineering systems, such as "multi-objective trade-off analysis" in which Pareto-optimal actions are derived by considering the subjective probabilities and payoffs associated with different shocks and their primary, secondary, and tertiary propagation pathways and consequences.

Modeling interdependent complex systems and lifeline infrastructures (e.g. the electric power, together with telecommunications, oil/gas pipelines, and energy markets) in a control theory context is especially pertinent since the current movement toward deregulation and competition will ultimately be limited only by the physics of electricity and the topology of the grid. In addition, mathematical models of complex networks are typically vague (or may not even exist); existing and classical methods of solution are either unavailable, or are not sufficiently powerful. For the most part, no present methodologies are suitable for understanding their behavior. In what follows, as examples, we briefly summarize four interdependent infrastructures, and the associated countermeasures for increased robustness, resilience, and security.

### 1.1 Example: Transportation

The backbone of the US transportation system and economy—the road infrastructure system—has continually evolved since the 1930s, but the cost to build and maintain it is rising. The US Department of Transportation estimates that the annual cost of congestion in lost productivity alone is more than $100 billion. In addition, more than 40,000 persons are killed and another five million injured each year in traffic accidents. This infrastructure, faced with the increased density in today's urban population centers, is becoming increasingly congested. Human population centers have grown dramatically in the past century, creating a "trilemma" of sustainability issues: population, poverty, and pollution. The United States along with many other nations is seeking a solution to

this worsening traffic congestion problem. Such solutions have to be viewed in terms of the economic, social, and political environments, along with the technological capability of the nation. Furthermore, the costs associated with generating and maintaining the road infrastructure are becoming increasingly higher, and the impact of inefficiencies can be measured in quantifiable terms of loss of labor-hours in the work place, loss of fuel, as well as intangibly in terms of pollution, and the general increased stress level of the work force who uses these transportation channels.

Where feasible, increasing the number of lanes or building new roads can expand present capacity, but the demand in some areas (both from population growth and travel demand) cannot be met by adding roads. A less expensive and disruptive solution is to intelligently manage the existing road infrastructure. The idea is to create and deploy technologies to improve the safety, capacity, and operational efficiency of the surface transportation system, while simultaneously reducing the burden on the environment and on our energy sources. With these objectives in mind, Congress launched the US Intelligent Transportation Systems (ITS) program in 1991. One of the program's goals is to develop Advanced Traffic Management Systems (ATMS). ATMS will rely on the consolidation of information, automotive, and highway technology. A wide range of small, complementary systems—from electronic route guidance to preemptive signal control—will essentially automate highways. Sensors and communication devices will be along the roads, as well as in the vehicle. Thus, the road will "know" its operational status, which it will then communicate to the vehicle. The vehicle operator can then make informed decisions about which routes to take to optimize individual trips and daily travel plans. Entities such as traveler information services and fleet management can use the data to plan, implement, and manage their daily operations.

Both public and private outfits can also use the road to plan, implement, and manage their daily operations, including traveler information, traffic management, public and rural transportation management, priority vehicle management, and freight and fleet management. Thus, although they pose great analytical challenges, the ATMS thrust offers significant payoff because of its broad geographical coverage and direct impact on regional economies. As complex as it is[2], the road system is only one segment of

[2]A few statistics on how we get around in America:

- Length of public roads: 46,036 miles of interstate highways (1%); over 112,450 miles of national highway System (3%); and 3.76 million miles of other (96%)
- Personal travel by mode:
  - 208 million vehicles: private vehicles 85.9%, public transport 2.8%, other means 11.3%
  - About 130 million cars, 69 million light trucks, 7 million commercial trucks, and 700,000 buses (e.g. California has 15.5 million motor vehicles, Florida has 7.3 million, ... )
  - About 1.2 million rail cars, 68 ferries, 6,000 aircraft
- Half of the total petroleum consumption in the United States is for highway vehicles and another 18% for other transportation:
  - Fuel consumption: 148 billion gallons of gasoline, 28 billion gallons of diesel, and about 4 billion gallons other
- Fatalities: 22,416 in cars (50.4%), 9,901 truck occupants (22.2%), 2,160 on motorcycles (4.9%), 1,088 on aircraft (3.1%), and 624 on trains (1.4%)
- Fatal accident types amenable to technological prevention: off-road (36%), angle collision (18%), head-on collision (17%), rear-end collision (5%), sideswipe (2%).

the transportation network. As in the other infrastructures, there are diverse sources of complexity and interdependence. Emerging issues include the following:

- Impact of Information Technology: IT and transportation systems' interrelations. Transportation is increasing links with sensors, telecommunications, and even satellites.
- Electrification of multimodal transportation systems: for example, rail networks are becoming increasingly dependent on electricity (electric and magnetic levitation trains).
- Fertile area at the intersection of CE/CS/EnvE/EE/ME/OR/Math/Control/Economics.
- Traffic modeling, prediction, and management: from operational issues to expansion planning.
- Multiresolutional simulations; real-time optimization, epsilon-optimality, and provable performance bounds.

In the area of multimodal transportation and distribution networks (air, land, and sea), emerging issues include electrification of transportation; links with sensors, telecommunications and satellites; traffic modeling, prediction, and management; multiresolutional simulations; real-time optimization with provable performance bounds with risk management; and how to develop tools in the intersection of mathematics, risk management, operations research, control theory, system science, computer science, artificial intelligence (AI), economics, and even biology to tackle these problems. Several researchers have referred to this as "*intelligent or adaptive control*"; the challenge is how to develop systems that can sense, identify, and build realistic models, and can also adapt, control, and achieve their goals.

These are challenges not only in transportation systems, but are the characteristics of any industry made up of many, geographically dispersed components that can exhibit rapid global change as a result of local actions. Prime examples are the highly interconnected and interactive industries, which make up a national or international "infrastructure," including telecommunications, transportation, gas, water and oil pipelines, the electric power grid, and even the collection of satellites in the earth orbit.

### 1.2 Example: Telecommunications

The globalization of our economy is built on telecommunication networks, including fixed networks (public switched telephone and data networks), wireless (cellular, PCS, wireless ATM), and computers (Internet and millions of computers in public and private use). These networks are growing rapidly and require secure, reliable, and high quality power supplies. This telecommunication infrastructure, like the power grid, is becoming overburdened. The satellite network, just one segment of the infrastructure, is a good example. The satellite network has three main layers:

- low earth orbit (LEO), 200–2,000 km ("little LEOs" at 750–1500 km), operating at VHF, UHF below 500 MHz; low complexity;
- medium earth orbit (MEO), 2000–20,000 km (big LEOs/MEOs at 750–11,000 km) operating at L and S microwave (1.6 and 2.5 GHz) with high to very high complexity; and

- geosynchronous orbit (GEO), at 36,000 km, operating at K microwave (19 and 29 GHz), with variable low to high complexity.

Some of the most familiar services are detailed Earth imaging, remote monitoring of dispersed locations, and highly accurate location and tracking using the continuous signals of the global positioning system (GPS). Satellite-based business and personal voice and data services are now available throughout much of the world.

The Internet is rapidly expanding the range of applications for satellite-based data communications; two of the most popular applications are accessing the Internet itself and connecting remote sites to corporate networks. Some satellite systems, including those of satellite TV providers, let users browse Web pages and download data—at 400 kbps—through a 21-in. (53 cm) roof-mounted dish receiver connected to a personal computer with an interface card. This capability could become a valuable tool for expanding an enterprise network to remote offices around the world.

Some utilities are diversifying their businesses by investing in telecommunications and creating innovative communications networks that cope with industry trends toward distributed resources, two-way customer communications, and business expansion, as well as addressing the measurement of complex and data-intensive energy systems via wide-area monitoring and control. Challenges include how to handle network disruptions and delays and manage orbits from the satellite. A big source of complexity is the interdependence of the telecommunication networks and the power grid.

The telecommunications network and the electric power grid are becoming increasingly interdependent. Issues range from the highest command and control level to the individual power stations and substations at the middle level, and then to the devices and power equipment at the lowest level.

### 1.3 Example: Financial Systems[3]

The stability of the financial system and the potential for systemic events to alter the functioning of that system have long been important topics for central banks and the related research community. Developments such as increasing industry consolidation, global networking, terrorist threats, and an increasing dependence on computer technologies underscore the importance of this area of research. Recent events, however, including the terrorist attacks of September 11th and the demise of long-term capital management, suggest that existing models of systemic shocks in the financial system may no longer adequately capture the possible channels of propagation and feedback arising from major disturbances. Nor do existing models fully account for the increasing complexity of the financial system's structure, the complete range of financial and information flows, or the endogenous behavior of different agents in the system. Fresh thinking on systemic risk is, therefore, required.

In order to promote a better understanding of systemic risk, the National Academy of Sciences and the Federal Reserve Bank of New York convened a conference in New York

[3]This section on financial systems is based on my presentation and related discussions at the "New Directions for Understanding Systemic Risk: A report on a Conference Cosponsored by the Federal Reserve Bank of New York and the National Academy of Sciences"; for the NAS book and complete FRBNY report please see: Economic Policy Review, Federal reserve Bank of New York, Vol. 13, Number 2, Nov. 2007, and New Directions for Understanding Systemic Risk, 108 pp, Nat'l Acad. Press, Washington DC, 2007. Input and material from NAS/BMSA and FRBNY is gratefully acknowledged.

in May of 2006 drawing together a broadly interdisciplinary group of scientists, engineers, and financial practitioners, ranging from electrical engineers and academic economists to risk analysts and asset managers from major investment banks. The primary purpose of the conference was to promote a cross-disciplinary dialogue in order to examine what possible leverage on the topic of systemic risk could be gained from areas of science not directly related to finance or economics. Accordingly, conference participants from the natural and mathematical sciences and from engineering disciplines drew heavily upon research on complex adaptive systems in order to build a framework both to give some substance and definition to the notion of systemic risk and to point to the possible linkages between this research and research on the financial system. Similarly, research economists presented papers that showed how some of these linkages could be leveraged, for example, in studies of international trade and, crucially for the Federal Reserve policy, in the management of the payments system. Participants from the financial industry also highlighted how thinking on systemic risk and actual systemic events affect trading activities in order to provide a context for the discussion.

For more information, please see the above-referenced report as well as the prevalence of systemic risk in very diverse areas ranging from biological and natural ecologies to financial, built and engineered complex systems in which prediction and management of systemic failures are critical.

In an engineered system, like the electric power grid or a telecommunication network, there is indeed the opportunity for control systems, and these can be quite advanced. Creating such a control capability for the electric grid required a mixture of tools from dynamical systems, statistical physics, information and communication science, along with research to reduce the computational complexity of the algorithms so they can scale up with the large size of the system being controlled. Our earlier work has led to working methods that have been applied to a variety of situations, including the electricity infrastructure coupled with telecommunications and the energy markets, cell phone networks on the Internet, and some biological systems. This is a multiscale challenge: detection of troublesome signals must be done within milliseconds, with some compensatory actions taken automatically, while some load balancing and frequency control on the grid is controlled on a timescale of seconds. At the same time, control functions such as load forecasting and management and generation scheduling take place on a timescale of hours or days. Developing a picture at the atomic level of what is going on in a system and then building up to the macroscale is a challenge that requires multiresolutional modeling in both space and time.

Just to give an idea of the complexity of modeling and controlling the electrical grid, in North America, there are more than 15,000 generators, and over 216,000 miles of high voltage lines. The overall grid is divided in several very large interconnected regions, and modeling one of them (which is necessary for understanding the systemic risks) might entail a simulation with 50,000 lines and 3000 generators. The system is typically designed to withstand the loss of any single element. To determine whether the grid can attain that design goal, we need to simulate the loss of each of 53,000 elements and calculate the effects on each of 50,000 lines, leading to over 2.6 billion cases. The analysis of these systemic risks is very challenging, but it can really make a difference in how to operate the system.

As an additional illustration of the level of detail that can successfully be modeled, we developed an example of a complex model to predict load and demand for DeKalb,

Illinois, which is a sizeable market with a mixture of commercial and residential customers. Deregulation of the electric system has reduced the correlation between power flow and demand, thus introducing uncertainty into the system, and so there has been a good deal of research to understand this phenomenon and develop the means to monitor and control it. The models and algorithms are now good enough to simulate the demand by customer type (residential, small commercial, and large commercial) on an hour-by-hour basis and attain 99.6–99.7% accuracy over the entire year. One value of these predictions is that they enable the power company to proactively dispatch small generators to meet anticipated high demands.

From a broader perspective, any critical national infrastructure typically has many layers and decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the constituent networks to remain operational and even automatically reconfigure in the event of local failures or threats of failure. In any situation subject to rapid changes, completely centralized control requires multiple, high data-rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center. But all of these are liable to disruption at the very time when they are most needed (i.e. when the system is stressed by natural disasters, purposeful attack, or unusually high demand).

When failures occur at various locations in such a network, the whole system breaks into isolated "islands," each of which must then fend for itself. With the intelligence distributed, and the components acting as independent agents, those in each island have the ability to reorganize themselves and make efficient use of whatever local resources remain to them in ways consonant with the established global goals to minimize adverse impact on the overall network. Local controllers will guide the isolated areas to operate independently while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the transition. A network of local controllers can act as a parallel, distributed computer, communicating via microwaves, optical cables, or the power lines themselves, and intelligently limiting their messages to only that information necessary to achieve global optimization and facilitate recovery after failure.

If organized in coordination with the internal structure existing in a complex infrastructure and with the physics specific to the components they control, these agents promise to provide effective local oversight and control without need of excessive communications, supervision, or initial programming. Indeed, they can be used even if human understanding of the complex system in question is incomplete. These agents exist in every local subsystem—from "horseshoe nail" up to "kingdom"—and perform preprogrammed self-healing actions that require an immediate response. Such simple agents already are embedded in many systems today, such as circuit breakers and fuses as well as diagnostic routines. The observation is that we can definitely account for loose nails and to save the kingdom.

Another key insight came out of analysis of forest fires, which researchers in one of the six funded consortia found to have similar "failure-cascade" behavior to electric power grids. In a forest fire the spread of a spark into a conflagration depends on how close together the trees are. If there is just one tree in a barren field and it is hit by lightning, it burns but no large blaze results. But if there are many trees and they are close enough together—which is the usual case with trees because Nature is prolific and efficient in using resources—the single lightning strike can result in a forest fire that burns until it reaches a natural barrier such as a rocky ridge, river, or road. If the barrier is narrow enough that a burning tree can fall across it or it includes a burnable flaw such

as a wooden bridge, the fire jumps the barrier and burns on. It is the role of first-response wild-land firefighters such as smokejumpers to contain a small fire before it spreads by reinforcing an existing barrier or scraping out a defensible fire line barrier around the original blaze.

Similar results hold for failures in electric power grids. For power grids, the "one-tree" situation is a case in which every single electric socket had a dedicated wire connecting it to a dedicated generator. A lightning strike on any wire would take out that one circuit and no more. But like trees in Nature, electrical systems are designed for efficient use of resources, which means numerous sockets served by a single circuit and multiple circuits for each generator. A failure anywhere on the system causes additional failures until a barrier—such as a surge protector or circuit breaker—is reached. If the barrier does not function properly or is insufficiently large, the failure bypasses it and continues cascading across the system.

These findings suggest approaches by which the natural barriers in power grids may be made more robust by simple design changes in the configuration of the system, and eventually how small failures might be contained by active smokejumper-like controllers before they grow into large problems. Other research into fundamental theory of complex interactive systems is exploring means of quickly identifying weak links and failures within a system.

Work during the past 11 years in this area has developed, among other things, a new vision for the integrated sensing, communications, and control-issues surrounding the power grid. Some of the pertinent issues are why/how to develop protection and control devices for centralized versus decentralized control, as well as issues involving adaptive operation and robustness to various destabilizers. However, instead of performing *in vivo* societal tests which can be disruptive, we have performed extensive "wind-tunnel" simulation testing (*in silico*) of devices and policies in the context of the whole system along with prediction of unintended consequences of designs and policies to provide a greater understanding of how policies, economic designs, and technologies might fit into the continental grid, as well as guidance for their effective deployment and operation.

This is not meant to imply that ecology and engineering have overcome all the challenges associated with representing and analyzing complex adaptive systems. Sensing the state of such systems is one ongoing challenge, as is the question of what to measure. Validation of models and verification of software remains a major challenge. There are major computational problems, including how to break models into tractable components. Self-similar systems can be reduced, but not complex systems like the electrical grid. One can use approximations to decouple complex systems, but it is difficult to analyze the errors thus introduced. One can find parts of an engineered system—and presumably in other systems—that are weakly coupled in terms of the dynamics transferred through the system and then approximate those portions with stand-alone models. This can help us reduce the complexity by dividing and conquering.

It is important to emphasize the difficulty of identifying meaningful signals from complex systems. For example, when monitoring a large fraction of the US electrical grid, how can we discern whether a perturbation in the system (be it financial, physical, communication, or cyber or a combination of them), is a natural fluctuation or the signature of a catastrophic failure. Does it reflect a naturally caused phenomenon, perhaps triggered by heat, high humidity, or a high demand in one portion of the grid, or is it actually an attack on the system or the precursor to major disturbance? How close is it to a regime shift or system flip? That can only be addressed with detection systems that can pull up

all the data, do data mining, pattern recognition, and then statistical analysis to derive the probability that we were sensing a catastrophic failure or a precursor of one.

This system monitoring problem is exacerbated if sharing of information is limited, as is the case in the banking sector. For example, I am often asked how one would monitor and control the reliability of the electrical grid under the assumption that companies did not cooperate with each other but, instead, competed and did not share the information. Such a situation would lead to a new control mechanism, and the logical question is whether this would stabilize or destabilize the system. For an Electric Power Research Institute (EPRI) project from the late 1990s, Simulator for Electric Power Industry Agents (SEPIA), we began exploring this case. The analysis was done for four large regions of the United States, and explored whether one could increase efficiency without diminishing reliability. This concept would need to be scaled up in order to reach a definitive conclusion.[4]

There is also a work on highly optimized tolerance that Professors John Doyle and Jean Carlson have been developing in California, in which they basically use a genetic algorithm, a neural network approach to evolve the properties of systems. They consider a variety of systems with particular structures and feedback properties, expose them to perturbations, observe their recovery, and just as one would train a chess playing program, these systems are modified until they become more tolerant to the disturbances to which they are exposed. So that is a way how even when one can not solve mathematics, but one can improve the structure of systems. The difficulty with these approaches, as Doyle and Carlson point out, is that systems become robust yet fragile in their terminology, meaning, systems that are engineered or have evolved to be tolerant to a particular set of disturbances often do so at the expense of their response to other classes of disturbances, something that we have to be careful about in the design of systems.[5]

Complex systems abound, and many different disciplines are concerned with understanding catastrophic change in such systems. We focus on three principal areas: risk assessment, modeling and prediction, and mitigation.

## 1.4 Example: North American Power Grid

***1.4.1 Electrification of transportation and enabling a smart self-healing grid.*** Our economy places increased demand for reliable, and disturbance-free electricity. The electric power grid is quite different from other infrastructure systems, such as gas, oil or water networks. A distinguishing characteristic of electricity, for example, is that there is no way to store significant amounts of energy; thus the system is fundamentally operating in real time. For this and related reasons, energy infrastructure systems have a unique combination of characteristics that makes control and reliable operation challenging like:

- Attacks and disturbances can lead to widespread failure almost instantaneously.
- Billions of distributed heterogeneous infrastructure components are tightly interconnected.

[4]See Amin, Massoud, Restructuring the Electric Enterprise: Simulating the Evolution of the Electric Power Industry with Adaptive Agents, Chapter 3 in *Market Based Pricing of Electricity*, A. Faruqui and M. Crew, eds., Kluwer Academic Publishers, Dec. 2002.

[5]See, for example, T. Zhou, J. M. Carlson and J. Doyle, Mutation, specialization, and hypersensitivity in highly optimized tolerance, *Proceedings of the National Academy of Sciences* 99:2049–2054. 2002. and J. M. Carlson and J. Doyle, Complexity and robustness, *Proceedings of the National Academy of Sciences* 99 suppl. 1:2538–2545. 2002.

- A variety of participants—owners, operators, sellers, buyers, customers, data and information providers, data and information users—interact at many points.
- The number of possible interactions increases dramatically as participants are added. No single centralized entity can evaluate, monitor, and manage them in real time.
- The relationships and interdependencies are too complex for conventional mathematical theories and control methods.

These characteristics create unique challenges in modeling, prediction, simulation, cause and effect relationships, analysis, optimization, and control, which have important implications for the use of IT for electric power. This article addresses these challenges by first presenting the technologies involved in the electricity infrastructure and then considers management and policy challenges to the effective performance both in the short and long term.

The North American power network may realistically be considered to be the largest and most complex machine in the world—its transmission lines connect all the electric generation and distribution on the continent. In that respect, it exemplifies many of the complexities of electric power infrastructure and how IT can address them. This network represents an enormous investment, including over 15,000 generators in 10,000 power plants, and hundreds of thousands of miles of transmission lines and distribution networks, whose estimated worth is over US$800 billion. In 2000, transmission and distribution was valued at US$358 billion (EIA 2003; EPRI 1999–2003).

At its most fundamental level, the network's transmission lines form a vertically integrated hierarchical network consisting of the generation layer (noted above) and three other network levels. The first is the *transmission* network, which is meshed networks combining extrahigh voltage (above 300 kV) and high voltage (100–300 kV), connected to large generation units and very large customers and, via tie-lines, to neighboring transmission networks and to the subtransmission level. The second level is *subtransmission*, which consists of a radial or weakly coupled network including some high voltage (100–300 kV) but typically 5–15 kV, connected to large customers and medium size generators. Finally, the third network level is *distribution*, which is typically a tree network including low voltage (110–115 or 220–240 V) and medium voltage (1–100 kV) connected to small generators, medium size customers, and local low voltage networks for small customers.

In its adaptation to disturbances, a power system can be characterized as having multiple states, or "modes," during which specific operational and control actions and reactions take place: normal, disturbance, and restorative. In the normal mode, the priority is on economic dispatch, load frequency control, maintenance, and forecasting. In the disturbance mode, attention shifts to faults, instability, and load shedding. And in the restorative mode, priorities include rescheduling, resynchronization, and load restoration. Some authors include an Alert Mode before a disturbance actually affects the system. Others add a System Failure Mode before restoration is attempted.

Beyond the risk management note above, the electric power grid's emerging issues include (i) integration and management of renewable resources and "microgrids"; (ii) use and management of the integrated infrastructure integrated with an overlaid sensor networks, secure communications and intelligent software agents (including dollars/economic factors and watts); (iii) active-control high voltage devices; (iv) developing new business strategies for a deregulated energy market; and (v) ensuring

system stability, reliability, robustness, and efficiency in a competitive marketplace and carbon-constrained world.

In addition, the electricity grid faces (at least) three looming challenges: its organization, its technical ability to meet 25-year and 50-year electricity needs, and its ability to increase its efficiency without diminishing its reliability and security.

***1.4.2 Smart self-healing grid.*** The term smart grid refers to the use of computer, communication, sensing and control technology which operates in parallel with an electric power grid for the purpose of enhancing the reliability of electric power delivery, minimizing the cost of electric energy to consumers, and facilitating the interconnection of new generating sources to the grid.

The concept for smart grid research and development was originally conceived by this author when I was at the EPRI during 1998–2003. The genesis of the smart grid was in the EPRI/DOD Complex Interactive Networks/Systems Initiative (CIN/SI) that I created and led during 1998–2001.

Beginning in 1998, the original concept and tools developed within CIN/SI were referred to as *The Self-Healing Grid*. This name has undergone several changes and finally emerged as "The Smart grid."

More recently, after joining the University of Minnesota in 2003, my research team and I have been engaged in research and also in telling our colleagues about this concept through publications, lectures, and seminars to diverse stakeholders, which include a wide spectrum from local to international utilities, companies, state and federal organizations, universities and think tanks, to congressional staffers, R&D caucus and committees who have invited our assessments and presentations.

The smart grid is a term also built into the Energy Independence and Security Act (EISA) of 2007, and more recently the American Recovery and Reinvestment Act of 2009 (the stimulus bill). The US Congress allocated $11 billion to research and demonstration projects in the smart grid area. This technology is currently an active topic on TV news and is discussed widely in the media.

Title XIII of EISA 2007 mandates a "Smart Grid" that modernizes and improves the information infrastructure. The Smart Grid represents the information and control functionality that will monitor, control, manage, coordinate, integrate, facilitate, and enable achievement of many of the benefits of innovations envisioned in national energy policy. Examples of Smart Grid functionality include the following:

- Connecting end user loads to grid information and control to facilitate energy efficiency improvements.
- Integrating alternative energy sources and providing the means for mitigating their intermittency.
- Providing the necessary information and control to integrate pluggable hybrids into the grid.
- Allowing problems to be detected and addressed before they become grid disturbances.

Information on these is widely available through EPRI assessments and reports, the US Department of Energy (The Smart Grid—An Introduction, 2008), and the IEEE National Energy Policy Recommendations related to the Smart Grid is a great resource.

In summary, an electric power system has two infrastructures:

- an electric infrastructure—that carries the electric energy in the power system, and,
- an information infrastructure that monitors, controls, and performs other functions related to the electric infrastructure.

The existing electric power grid is not dumb. It has long been designed to continue operating even in the face of problems. Equipment breaks, thunderstorms happen, curious animals get into substations, and drivers crash cars into distribution poles. The power grid is designed and operated so that any single situation does not interrupt the flow of power (the so-called "$n - 1$ criterion"). That requires intelligence, which comes from electromechanical automation, intelligent electronic devices (IEDs), control centers, computers, and communications systems. Such functions have been part of the electric grid for many years. However, because of a combination of cost and operational continuity issues, many of these systems lag, sometimes by decades, advances and capabilities in computer and communications technology.

The institutional and economic framework envisioned for the twenty-first century power system ultimately depends upon building new types and levels of functionality into today's power system. These needed capabilities will be "enabled" by several breakthrough innovations, including, but not limited to the following:

- *Digitally controlling the power delivery network* by replacing today's electromechanical switching with real-time and power-electronic controls. This will become the foundation of a new "smart, self-healing power delivery system" that will enable innovative productivity advances throughout the economy. Digital control, coupled with communications and computational ability is the essential step needed to most cost-effectively address the combined reliability, capacity, security, and market-service vulnerabilities of today's power delivery system.
- *Integrating communications* to create a dynamic, interactive power system for real-time information and power exchange. This capability is needed to enable retail energy markets; power interactive, microprocessor-based service networks; and fundamentally raise the value proposition for electricity. Through advanced information technology coupled with sensors, the system would be "self-healing" in the sense that it is constantly self-monitoring and self-correcting to keep high quality, reliable power flowing. It can sense disturbances and instantaneously counteract them, or reconfigure the flow of power to cordon off any damage before it can propagate.
- *Automating the distribution* system to meet evolving consumer needs. The value of a fully automated distribution system integrated with communication—derives from four basic functionality advantages:
  1. Reduced number and duration of consumer interruptions, fault anticipation, and rapid restoration.
  2. Increased ability to deliver varying levels of reliable, digital-grade power.
  3. Increased functional value for all consumers in terms of metering, billing, energy management, demand control, and security monitoring, among others.
  4. Access to selective consumer services including energy-smart appliances, electricity-market participation, security monitoring, and distributed generation.

  The value of these advantages to consumers, suppliers, and society alike more than justify the needed public/private investment commitment. This transformation

will enable additional innovations in electricity service that are bounded only by our imagination.

- *Transforming the meter* into an EnergyPort (EnergyPort is a service mark of EPRI). EnergyPort is a consumer gateway that allows price signals, decisions, communications, and network intelligence to flow back and forth through the two-way energy/information portal. This will be the linchpin technology that leads to a fully functioning marketplace with consumers responding (through microprocessor agents) to service offerings and price signals. This offers a tool for moving beyond the commodity paradigm of twentieth century electricity service, and quite possibly ushering in a set of new energy/information services as diverse as those in today's telecommunications.
- *Integrating distributed energy resources including intermittent and renewable generation and storage systems*. The smart power delivery system would also be able to seamlessly integrate an array of locally installed, distributed power generation as power system assets. Distributed power sources could be deployed on both the supply and consumer side of the energy/information portal as essential assets dispatching reliability, capacity, and efficiency.
- *Accelerating end-use efficiency*. The growing trend toward digital control can enable sustained improvements in efficiency and productivity for nearly all industrial and commercial operations. Similarly, the growth in end-use energy consuming devices and appliances, networked with system controls, will afford continuous improvements in productivity and efficiency.

Other benefits of the Smart Grid go beyond energy efficiency:

- The Smart Grid will facilitate use of alternative generation that supports energy independence. This is a matter of national security.
- Both cyber-security protection and defense against EMP: Components of the Smart Grid will need to be hardened by design.
- There are likely to be numerous benefits of the Smart Grid that defy quantification. Examples include the flexibility to accommodate new requirements, the ability to accommodate innovative grid technology, and the ability to support innovative regulatory concepts, all without major replacement of existing equipment.
- The flexibility may help avoid future rate increases as new technology or requirements arise, but the exact benefit might not be quantifiable.

Revolutionary developments in both information technology and material science and engineering promise significant improvement in the security, reliability, efficiency, and cost-effectiveness of all critical infrastructures. Steps taken now can ensure that critical infrastructures continue to support population growth and economic growth without environmental harm.

## 2 DIGITAL NETWORK CONTROL: OPERATIONAL SYSTEMS

IT has and will play a critical role in ensuring the reliable transmission and distribution of electricity. Electricity's share of total energy in the world is expected to continue

to grow, as more efficient and intelligent processes are introduced, such as controllers based on power electronics combined with wide-area sensing and management systems for improved performance. In the next two decades, it is envisioned that the electric power grid will move from an electro-mechanically controlled system to one that is electronically controlled.

In this sense, the electrical infrastructure is becoming increasingly intertwined with the IT infrastructure that supports it. Current and future power systems applications for telecommunications include the following:

- surveying overhead transmission circuits and rights-of-way;
- transmitting supervisory control and data acquisition (SCADA) system data (usually via telephone circuits);
- measuring overhead conductor sag;
- measuring phasors (using a precise timing signal derived from the GPS to time-lag measurements of AC signals);
- fitting sine waves to AC signals, and determining magnitude and phase of v(t), i(t) in remote locations;
- enhancing situational awareness by generating real-time pictures of system states and real-time power flow as well as real-time estimation of the systems' state and topology;
- using data from LEO satellites for faster-response control (more than 100 times less delay than High Earth Orbit (HEO) satellites) and connecting to existing parallel data stream facilities (effectively a high speed global RS-232 channel).

The technologies support the operational control of electrical networks, ranging from energy management systems (EMS) to remote field devices. Critical systems include those described below.

*EMS.* The objective of the EMS is to manage production, purchase, transmission, distribution, and sale of electrical energy in the power system at a minimal cost with respect to safety and reliability. Management of the real-time operation of an electric power system is a complex task requiring interaction of human operators, computer systems, communications networks, and real-time data-gathering devices in power plants and substations. An EMS consists of computers, display devices, software, communication channels and remote terminal units that are connected to Remote Terminal Units (RTUs), control actuators, and transducers in power plants and substations. The main tasks it performs is dependent upon generator control and scheduling, network analysis and operator training. Control of generation requires that the EMS maintain system frequency and tie line flows while economically dispatching each generating unit. Management of the transmission network requires that the EMS monitor up to thousands of telemetered values, estimate the electrical state of the network, and inform the operator of the best strategy to handle potential outages that could result in an overload or voltage limits violation. EMSs can have real-time two-way communication links between substations, power plants, independent system operators, and other utility EMSs.

*SCADA system.* A SCADA system supports the operator control of remote (or local) equipment, such as opening or closing a breaker. A SCADA system provides three

critical functions in the operation of an electric power system: data acquisition, supervisory control, and alarm display and control. It consists of one or more computers with appropriate applications software connected by a communications system to a number of RTUs placed at various locations to collect data, perform intelligent control of electrical system devices and report results back to an EMS. SCADAs can also be used for similar applications in natural gas pipeline transmission and distribution applications. A SCADA can have real-time communication links with one or more EMSs and hundreds of substations.

*RTU.* RTUs are special purpose microprocessor-based computers that contain analog to digital converters (ADCs) and digital to analog converters (DACs), digital inputs for status and digital output for control. There are transmission substation RTUs and distribution automation (DA) RTUs. Transmission substation RTUs are deployed at substation and generation facilities where a large number of status and control points are required. DA RTUs are used to control air switches and various compensation capacitor banks (that support voltage) on utility poles, control pad-mounted switches, monitor and automate feeders, monitor and control underground networks, and for various uses in smaller distribution substations. RTUs can be configured and interrogated using telecommunication technologies. They can have hundreds of real-time communication links with other substations, EMS, and power plants.

*Programmable logic controller(PLC).* PLCs have been used extensively in manufacturing and process industries for many years and are now being used to implement relay and control systems in substations. PLCs have extended input/output (I/O) systems similar to transmission substation RTUs. The control outputs can be controlled by software residing in the PLC and via remote commands from a SCADA system. The PLC user can make changes in the software without making any major hardware or software changes. In some applications, PLCs with RTU reporting capability may have advantages over conventional RTUs. PLCs are also used in many power plant and refinery applications. They were originally designed for use in discrete applications like coal handling. They are now being used in continuous control applications such as feedwater control. PLCs can have many real-time communication links inside and outside substations or plants.

*Protective relays.* Protective relays are designed to respond to system faults such as short circuits. When faults occur, the relays must signal the appropriate circuit breakers to trip and isolate the faulted equipment. Distribution system relaying must coordinate with fuses and reclosures for faults while ignoring cold-load pickup, capacitor bank switching, and transformer energization. Transmission line relaying must locate and isolate a fault with sufficient speed to preserve stability, reduce fault damage, and minimize the impact on the power system. Certain types of "smart" protective relays can be configured and interrogated using telecommunication technologies.

*Automated metering.* Automated metering is designed to upload residential and/or commercial gas and/or electric meter data. This data can then be automatically downloaded to a PC or other device and transmitted to a central collection point. With this technology, real-time communication links exist outside the utility infrastructure.

*Plant distributed control systems ( DCSs).* Plant DCSs are plantwide control systems that can be used for control and/or data acquisition. The I/O count can be as high as 20,000 data points or higher. Often, the DCS is used as the plant data highway for communication to/from intelligent field devices, other control systems such as PLCs, RTUs, and even the corporate data network for enterprise resource planning (ERP) applications. The DCS traditionally has used a proprietary operating system. Newer versions are moving toward open systems such as Windows NT and Sun Solaris. DCS technology has been developed with operating efficiency and user configurability as drivers, rather than system security. Additionally, technologies have been developed that allow remote access, usually via PC, to view and potentially reconfigure the operating parameters.

*Field devices.* Examples of field devices are process instrumentation such as pressure and temperature sensor and chemical analyzers. Other standard types of field devices include electric actuators. Intelligent field devices include electronics to enable field configuration, upload of calibration data, and so on. These devices can be configured off-line. They also can have real-time communication links between plant control systems, maintenance management systems, stand-alone PCs, and other devices inside and outside the facility.

## 3 DIGITAL INTERDEPENDENCIES AND SECURITY RISKS

Recognizing the increased interdependence between IT and electricity infrastructures, along with technical and business opportunities, electric power utilities typically own and operate at least parts of their own telecommunications systems which often consist of backbone fiber optic or microwave connecting major substations, with spurs to smaller sites. The energy industry has historically operated closed, tightly controlled networks. Deregulation and the resulting commercial influences have placed new information sharing demands on the energy industry. Traditional external entities like suppliers, consumers, regulators, and even competitors now must have access to segments of the network. The definition of the network must be expanded to include the external wide-area network connections for these external entities. This greatly increases the security risk to other functional segments of the internal network that must be protected from external connections. This is true whether a private network or the Internet is used to support the external wide-area network.

The external entities already have connections to the Internet and as such the Internet can provide the backbone for the External Wide-Area Network. Duplicating this backbone to create a private network requires not only large up front start up costs, but also ongoing maintenance costs and potentially higher individual transaction costs than using the Internet.

Information systems and on-line data processing tools include: the Open-Access Same-time Information System (OASIS), which is now in operation over the Internet; and Transfer Capability Evaluation (TRACE) software, which determines the total transfer capability for each transmission path posted on the OASIS network, while taking into account thermal, voltage, and interface limits.

Increased use of electronic automation raises issues regarding adequacy of operational security: (i) reduced personnel at remote sites makes them more vulnerable to hostile threats; (ii) interconnection of automation and control systems with public data networks

makes them accessible to individuals and organizations, from any worldwide location using an inexpensive computer and a modem; (iii) use of networked electronic systems for metering, scheduling, trading or e-commerce imposes numerous financial risks.

Utility telecommunications often include several media and diversified communications networks which in part provide redundancy; these range from dedicated fiber-optic cables, digital and analog microwave, and VSAT satellite to power line carrier technology as well as the use of multiple address radio, spread spectrum radio, trunked mobile radio, and cellular digital packet data. Security of the cyber and communication networks now used by businesses is fundamental to the reliable operation of the grid; as power systems start to rely more heavily on computerized communications and control, system security has become increasingly dependent on protecting the integrity of the associated information systems. Part of the problem is that existing control systems, which were originally designed for use with proprietary, stand-alone communications networks, were later connected to the Internet (because of its productivity advantages and lower costs), but without adding the technology needed to make them secure. Communication of critical business information and controlled sharing of that information are essential parts of all business operations and processes.

If the deregulation of the energy industry resumes, information security will become more important. Energy-related industries will have to balance what appear to be mutually exclusive goals of operating system flexibility with the need for security. Key electric energy operational systems depend on real-time communication links both internal and external to the enterprise. The functional diversity of these organizations has resulted in a need for these key systems to be designed with a focus on open systems that are user configurable to enable integration with other systems both internal and external to the enterprise. In many cases, these systems can be reconfigured for security using telecommunication technologies and in nearly all cases the systems dynamically exchange data in real time. Power plant DCS systems produce information necessary for dispatch and control. This requires real-time information flow between the power plant and the utility's control center, system dispatch center, regulatory authorities, and so on. A power plant operating as part of a large wholesale power network may have links to an independent system operator, a power pool, and so on. As the generation business moves more and more into market-driven competitive operation, both data integrity and confidentiality will become major concerns for the operating organizations.

Any telecommunication link which is even partially outside the control of the organization owning and operating power plants, SCADA systems or EMSs represents a potentially insecure pathway into business operations and to the grid itself. The interdependency analysis done by most companies during Y2K preparations have both identified these links and the systems' vulnerability to their failures. Thus, they provide an excellent reference point for a cyber-vulnerability analysis.

In particular, monitoring and control of the overall grid system is a major challenge. Existing communication and information system architectures lack coordination among various operational components, which usually is the cause for the unchecked development of problems and delayed system restoration. Like any complex dynamic infrastructure system, the electricity grid has many layers and is vulnerable to many different types of disturbances. While strong centralized control is essential to reliable operations, this requires multiple, high data-rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center, all of which are especially vulnerable when they are needed most—during serious system stresses or

power disruptions. For deeper protection, intelligent distributed control is also required; this would enable parts of the network to remain operational and even automatically reconfigure in the event of local failures or threats of failures.

Distributed control capability is becoming available in next-generation integrated sensors that are equipped with two-way communication capability and support "intelligent agent" functions—not just sensing, but data assessment, adaptive learning, decision-making, and actuation. The development of IEDs that combine sensors, telecommunication units, computers, and actuators will allow highly automated adjustments to be made at many points on the system and protect substantially against cascading failures. The use of distributed intelligent agents also opens the door to the development of a self-healing power grid that responds adaptively to counteract disturbances at the site of their occurrence.

Intelligent sensors will be capable of gathering a wide range of operating data, including time-stamped measurements of voltage, current, frequency, phase angle, and harmonics. This information, that provides input for distributed control, can also be integrated into a real-time system-wide database and coupled with analysis tools that perform dynamic monitoring, state estimation, disturbance analysis, and contingency assessment for the grid as a whole. Unfortunately, simulation-based techniques and mathematical models are presently unable to accurately portray the behavior of interactive networks, whose dynamics can be highly nonlinear. Fine-tuning existing models with real-world input from distributed sensors may offer improvements, but substantial progress will require the formulation of new models.

SCADA and EMS system operations are critically dependent on the telecommunication links that gather data from geographically dispersed sources and transmit operational and control instructions to geographically dispersed facilities. In the North American grid, these telecommunications links run the gamut from hardwired private networks to multinetwork systems using a combination of private and public networks for both data acquisition and control. Not all of the networks are hardwired. Microwave and satellite communications links are common alternatives in areas where topography and/or distance makes wireless more cost effective. At first glance it would seem that a private, hardwired network that is totally within the control of the owner organization is a secure system. However, even hardwired private networks will be linked to networks outside the control of the company. Typical outside data sources are bulk power customers, major retail customers, bulk power providers, power pools, independent system operating entities, and so on. These connections can offer a multitude of paths into the SCADA and EMS systems. Without proper security design and management, each link is a potential security risk.

Challenges include how to handle network disruptions and delays and manage orbits from the satellite. A major source of complexity is the interdependence of the telecommunication networks and the power grid. Issues range from the highest command and control level to the individual power stations and substations at the middle level, and then to the devices and power equipment at the lowest level.

As the readers of this Handbook know, technology is a two-edged sword. In the case of electricity, the aforementioned discussion reveals one edge (i.e. the risk) to be the extent to which IT introduces a new set of security concerns. The other edge (i.e. the promise) remains because of the substantial increases in capacity and efficiency that are made possible through continuing IT advancements. The following is a sample of the emerging technologies that promise continuing gains in the electricity sector:

- Flexible Alternating Current Transmission System (FACTS) devices, which are high voltage thyristor-based electronic controllers that increase the power capacity of transmission lines and have already been deployed in several high value applications (At peak demand, up to 50% more power can be controlled through existing lines.);
- Unified Power Flow Controller (UPFC), a third-generation FACTS device that uses solid-state electronics to direct power flow from one line to another to reduce overloads and improve reliability;
- Fault Current Limiters (FCLs), which absorb the shock of short circuits for a few cycles to provide adequate time for a breaker to trip (Preliminary results of post–August 14th outage show that FCLs could have served as "shock absorbers" to limit the size of blackouts.);
- Innovations in materials science and processing, including high temperature superconducting (HTS) cables, oxide-power-in-tube technology for HTS wire, and advanced silicon devices and wide-bandgap semiconductors for power electronics;
- Information systems and on-line data processing tools such as the OASIS and TRACE software, which determine total transfer capability for each transmission path posted on the OASIS network, while taking into account thermal, voltage, and interface limits;
- Wide-Area Measurement Systems (WAMS), which integrate advanced sensors with satellite communication and time stamping using GPSs to detect and report angle swings and other transmission system changes;
- Enhanced IT systems for Wide-Area Measurement/Management Systems (WAMS), OASIS, SCADA systems, and EMS;
- Advanced software systems for dynamic security assessment of large/wide-area networks augmented with market/risk assessment; and
- IEDs with security provisions built in by combining sensors, computers, telecommunication units, and actuators; related "intelligent agent" functions such as assessment, decision, and learning.

However, even if most of the above technologies are developed and deployed, there is still a major management challenge in making such a complex network perform reliably with security. These issues are taken up next.

## 4 MANAGEMENT

*Human performance.* Infrastructures are systems with "humans in the loop". This is indeed the case for electricity networks. Several key human resources issues arise in bringing IT to improve the performance of electric power. The first is operator experience. The second is retaining professionals in the field of electric power engineering. The third is how users and consumers can interface with IT-enabled electric power systems.

*Operator training.* Several root causes of the August 14th outage point to lack of operators' situational awareness and coordination. IT has a key role to play in the optimization of operator interfaces and other human factor issues. Basically, the problem is finding the most effective way for machines and humans to work together, and the data glut and maintaining operator attention is largely at the center

of the problem. Good operator interfaces provide adequate visualization of the state of the system, and they should be designed so that the user can remain tuned in to many different factors while giving active attention to only a few.

Much of the answer is simply a matter of how information is packaged for viewing. IT innovations are expected to have applications in personnel training and optimization of human performance, for example, through the use of virtual reality for training, for maintenance or rapid repair work, especially, those involving hazardous situations. Voice recognition is another technology expected to come into broad use over the next decade; replacement of keyboarding with voice-based input capability could greatly streamline and simplify human interaction with computers and other electronic control equipment.

Since humans interact with these infrastructures as managers, operators, and users, human performance plays an important role in their efficiency and security. In many complex networks, human participants themselves are both the most susceptible to failure and the most adaptable in the management of recovery. Modeling and simulating these networks, especially, their economic and financial aspects, will require modeling the bounded rationality of actual human thinking, unlike that of a hypothetical "expert" human as in most applications of AI. Even more directly, most of these networks require some human intervention for their routine control and especially, when they are exhibiting anomalous behavior that may suggest actual or incipient failure.

*Retaining a trained workforce.* A growing concern related to the human network is the erosion of technical knowledge within the power industry. To a large extent this is a matter of the retirement of seasoned power engineers, exacerbated by recent downsizing and reductions of in-house workforce. These key employees take their knowledge with them when they go. It will take a long time to recruit replacements. A second related issue is that new engineers are not entering the field rapidly enough to replace retirees. The average power engineer's age has increased significantly over the last two decades. A serious shortage of power engineers is developing, and is expected to continue for several decades.

*Users.* Operators and maintenance personnel are obviously "inside" these networks and can have direct, real-time effects on them. But users of a telecommunication, transportation, electric power or pipeline system also affect the behavior of those systems, often without conscious intent. The amounts, and often nature, of demands put on the network can be the immediate cause of conflict, diminished performance, and even collapse. Reflected harmonics from one user's machinery degrade power quality for all. Long transmissions from a few users create Internet congestion. Simultaneous, lawn watering drops everyone's water pressure. No one is "outside" the infrastructure.

Given that there is some automatic way to detect actual or immanent local failures, the obvious next step is to warn the operators. Unfortunately, the operators are usually busy with other tasks, sometimes even responding to previous warnings. In the worst case, detected failure sets off a multitude of almost simultaneous alarms as it begins to cascade through the system, and, before the operators can determine the real source of the problem, the whole network has shut itself down automatically.

Unfortunately, humans have cognitive limitations that can cause them to make serious mistakes when they are interrupted. In recent years, a number of systems have

been designed that allow users to delegate tasks to intelligent software assistants ("softbots") that operate in the background, handling routine tasks and informing the operators in accordance with some protocol that establishes the level of their delegated authority to act independently. In this arrangement, the operator becomes a supervisor, who must either cede almost all authority to subordinates or be subject to interruption by them. At present, we have very limited understanding of how to design user interfaces to accommodate interruption.

*Information security.* The electric power industry traditionally has been a vertically integrated industry that in some cases operated in pseudo-monopolistic fashion. However, the industry is currently undergoing restructuring, which frequently results in a break-up of the vertical structure. Additionally, there has been a significant move on the part of the control system suppliers to electric and petrochemical industries toward open, user-configurable systems utilizing real-time communications. With a vertical structure, local and wide-area networks were sufficient to maintain a reasonably secure data network. However, deregulation and new networking technologies are making secure communications more important, and more difficult to develop and maintain.

Information security is concerned with the relationships between people and information. In these relationships, people are owners, custodians, creators, readers, modifiers, certifiers, or even subjects of the information. It follows then that the information itself is the object of various actions by people—creation, destruction, reading, modification, and certification. Information security is concerned with first defining appropriate relationships between people as actors and information resources as objects; these relationships are usually defined as a set of rules defining permitted actions. Not all threats come from outside the organization nor are all threats malicious.

Information security is also concerned with controlling the relationships between people and information so that information is managed according to well-defined rules. Some human agent or institutional agency of authority is usually charged with creating, communicating, applying, monitoring, and enforcing these information security rules. Examples of contemporary information security rules are: rules for handling government classified documents; rules for ensuring client-attorney privilege or privacy of shared information; rules followed by corporate accountants and checked by financial auditors; and rules for ensuring accuracy and completeness of patients' health records. Generally, these rules define information security controls based on properties of special classes of information; these properties fall into three broad categories: confidentiality of sensitive information; integrity and authenticity of critical information; and availability of necessary information. These principles need to be applied to the management of electricity systems, including the operators and managers of these systems.

*Complex system failure.* Beyond the human dimension, there is a strategic need to understand the societal consequences of infrastructure failure risks along with benefits of various tiers of increased reliability. From an infrastructure interdependency perspective, power, telecommunications, banking and finance, transportation and distribution, infrastructures are becoming more and more congested, and are increasingly vulnerable to failures cascading through and between them. A key concern is the avoidance of widespread network failure because of cascading and

interactive effects. Moreover, interdependence is only one of the several characteristics that challenge the control and reliable operation of these networks. Other factors that place increased stress on the power grid include dependencies on adjacent power grids (increasing because of deregulation), telecommunications, markets, and computer networks. Furthermore, reliable electric service is critically dependent on the whole grid's ability to respond to changed conditions instantaneously.

Prior to the tragic events of September 11th, the US President's Commission on Critical Infrastructure Protection in 1997 highlighted growing concern (CIAO 1997). It noted the damaging and dangerous ways cascading failures could unpredictably affect the economy, security, and health of citizens. Secure and reliable operation of these systems is fundamental to our economy, security and quality of life, as noted by the President's Commission on Critical Infrastructure Protection Report published in October 1997 and the subsequent Presidential Directive 63 on Critical Infrastructure protection, issued on May 22, 1998.

Secure and reliable operation of critical infrastructures poses significant theoretical and practical challenges in analysis, modeling, simulation, prediction, control, and optimization. To address these challenges, a research initiative—the EPRI/DOD CIN/SI—was undertaken during 1998–2001 to enable critical infrastructures to adapt to a broad array of potential disturbances, including terrorist attacks, natural disasters, and equipment failures.

The CIN/SI overcame the long-standing problems of complexity, analysis, and management for large interconnected systems—and systems of systems—by opening up new concepts and techniques for the strategic management of this infrastructure system. Dynamical systems, statistical physics, information and communication science, and computational complexity were extended to provide practical tools to measure and model the power grid, cell phone networks, Internet, and other complex systems. For the first time, global dynamics for such systems can be understood fundamentally.

## 5 NEXT STEPS

Funding and sustaining innovations, such as the smart self-healing grid, remain a challenge as utilities must meet many competing demands on precious resources while trying to be responsive to their stakeholders, who tend to limit R&D investments to immediate applications and short-term return on investment. In addition, utilities have little incentive to invest in the longer term. For regulated investor-owned utilities there is added pressure caused by Wall Street to increase dividends.

Several reports and studies have estimated that for existing technologies to evolve and for the innovative technologies to be realized, a sustained annual research and development investment of $10 billion is required. However, the current level of R&D funding in the electric industry is at an all-time low. The investment rates for the electricity sector are the lowest rates of any major industrial sector with the exception of the pulp and paper industry. The electricity sector invests at most only a few tenths of a percent of sales in research—this in contrast to fields such as electronics and pharmaceuticals in which R&D investment rates have been running between 8% and 12% of net sales—and all of these industry sectors fundamentally depend on reliable electricity.

A balanced, cost-effective approach to investments and use of technology can make a sizable difference in mitigating the risk.

## ACKNOWLEDGMENTS

I developed most of the context and many of the findings presented here while I was at the EPRI in Palo Alto (during 1998–2003), and for the Galvin Electricity Initiative (during 2005–2006). I gratefully acknowledge the feedback from Mr John Voeller (the editor of this series). The support and feedback from numerous colleagues at EPRI, universities, industry, national laboratories, and government agencies with funding from EPRI, NSF, and the ORNL is gratefully acknowledged.

## FURTHER READING

Amin, S. M., and Schewe, P. (2007). *Preventing Blackouts*. Scientific American, pp. 60–67, www.Sciam.com.

Amin, S. M., and Gellings, C. W. (2006). The North American power delivery system: balancing market restructuring and environmental economics with infrastructure security. *Energy* **31**(6–7), 967–999.

Amin, S. M., and Wollenberg, B. F. (2005). Toward a smart grid. *IEEE Power Energy Mag.* **3**(5), 34–38.

Amin, S. M. (2005). Energy infrastructure defense systems. *Proc. IEEE* **93**(5), 861–875.

Amin, S. M. (2002). Restructuring the electric enterprise: simulating the evolution of the electric power industry with adaptive agents. In *Electricity Pricing in Transition*, A. Faruqui, and K. Eakin, Eds. Kluwer Academic Publishers, Chapter 3, pp. 27–50.

Amin, S. M. (2000). National infrastructures as complex interactive networks. In *Automation, Control, and Complexity: An Integrated Approach*, T. Samad, and J. Weyrauch, Eds. John Wiley and Sons, New York, Chapter 14, pp. 263–286.

Amin, S. M. (2000). Toward self-healing infrastructure systems. *IEEE Comput. Mag.* **33**(8), 44–53.

Amin, S. M. (2001). Toward self-healing energy infrastructure systems. *IEEE Comput. Appl. Power* **14**(1), 20–28.

Amin, S. M. (2000). "Modeling and Control of Electric Power Systems and Markets. *IEEE Control Systems Magazine* **20**(4), 20–25.

Amin, S. M., and Ballard, D. (2000). Defining new markets for intelligent agents. *IEEE IT Prof.* **2**(4), 29–35.

*Special Issue of Proceedings of the IEEE on Energy Infrastructure Defense Systems*. (2005). (Guest editor: Amin, S. M.) **93**(5), 855–1059.

*Special issues of IEEE Control Systems Magazine on Control of Complex Networks*. (2001). (Guest editor: Amin, S. M.) **21**(6); (2002) **22**(1).

*Special issue of IEEE Control Systems Magazine on Power Systems and Markets*. (2000). (Guest editor: Amin, S. M.). **20**(4), 20–90.

(1995). Network, control, communications and computing technologies in intelligent transportation systems. In *Mathematical and Computer Modeling*, Vol. 22(4–7), (Guest co-editors: S. M. Amin, A. Garcia-Ortiz, and J. R. Wootton). Elsevier Science Ltd, pp. 454.

Amin, S. M. (2004). Electricity. In *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*, R. Zimmerman, and T. Horan, Eds, Chapter 7, pp. 116–140.

Amin, S. M. (2004). Balancing market priorities with security issues: interconnected system operations and control under the restructured electricity enterprise. *IEEE Power Energy Mag.* **2**(4), 30–38.

Starr, C., and Amin, S. M. (2003). *Global transition dynamics: unfolding the full social implications of national decision pathways*,11, submitted to the President of the US National Academy of Engineering.

# INHERENTLY SECURE NEXT-GENERATION COMPUTING AND COMMUNICATION NETWORKS FOR REDUCING CASCADING IMPACTS

ROBERT P. EVANS
*Idaho National Laboratory, Idaho Falls, Idaho*
VIRGIL B. HAMMOND AND SHABBIR A. SHAMSUDDIN
*Argonne National Laboratory, Argonne, Illinois*

## 1 INTRODUCTION

Security is of vital interest to all participants in the control system sphere of interest. This includes governmental agencies, vendors, users, and consultants, as well as industry advisory groups. The article explores some of the efforts being used by these participants to identify and mitigate security exposures using risk management methodologies, technology tools, and standards.

## 2 STANDARDS, GUIDELINES, AND BEST PRACTICES

Standardization has a major impact on each of us, yet most of us do not understand what it means or how it affects our lives. Standardization is the process of establishing a technical benchmark that may be defined by written documents that lay out the criteria for the standardized measure. This technical benchmark document may take one of several forms, depending on its level of acceptance, and can be described as a set of criteria some of which may be mandatory, voluntary guidelines, and/or best practices.

## 3 STANDARDS

Standards are an important part of the total effort to achieve control system cyber security. As rules or requirements that define accepted operational criteria, they provide a measure of consistency and a means for quantifying quality and reliability. Standards provide a performance framework for hardware and software vendors who build the components for a control system. Standards provide a similar service for the personnel who operate and maintain the control system, once it becomes operational. Standards are most effective when the engineers and operators using the standards understand the capabilities and limitations of each standard and its history.

A standard, as defined by the National Standards Policy Advisory Committee is:

> "A prescribed set of rules, conditions, or requirements concerning definitions of terms; classification of components; specification of materials, performance, or operations; delineation of procedures; or measurement of quantity and quality in describing materials, products, systems, services, or practices" [1].

Standards are sets of rules or requirements, which define the accepted criteria for a component, procedure, system, and so on. Standards are developed by a consensus of the judgment of volunteers, which pool their knowledge base and experience.

### 3.1 Guidelines

Guidelines are tools that attempt to streamline a process or procedure. They may consist of rules or suggestions that, when applied, may simplify the process or procedure, and provide a level of quality and consistency. Guidelines may be issued by any organization to make the processes more uniform and expectantly, of high quality. By definition, guidelines are not mandatory but attempt to provide a set of knowledge that can be applied [2, 3].

## 4 BEST PRACTICE

*Best practices*, sometimes referred to as *recommended practices*, are a management tool that asserts that there is a technique, method, process, and so on, which is more effective at delivering a particular result than any other. As with standards and guidelines, best practices may consist of a set of good and practical industry practices or suggestions, which, when followed, will produce superior performance. As with guidelines, best practices are not mandatory, unless they become a standard and are imposed by a particular organization as a requirement [4, 5].

### 4.1 Cyber and Control Systems Security Standards in Common Use

The use of cyber security standards (including standards, guidelines, and best practices) can greatly assist in the protection of critical infrastructure by providing requirements, guidelines, and requisite imperatives in the implementation and maintenance of computer-controlled systems. Standards are most effective when the decision-makers, engineers, and operators using the standards understand what each addresses and does not address.

There is a link between cyber vulnerabilities and the standards that are intended to provide mitigation opportunities. For example, standards for equipment design and operation offer direction for vendors to use in bringing usable and compatible products to market, while providing companies the specifications required to select and implement the appropriate equipment and procedures. Most of all, these standards ensure that equipment is operated and maintained efficiently [6].

Standards' organizations are, for the most part, public organizations that have little or no enforcement ability. They rely on educating the users as to the importance of security, and of the potential benefits that standards can add to their operations. Where cyber security standards are implemented, they provide reliable direction toward achieving an acceptable level of cyber security by providing a framework

on which to construct a viable and rational security policy. They also provide an important frame of reference when performing risk analysis of an operating control system.

The cyber security standards issued by these organizations are frequently referred to as either *sector-specific* or *cross-sector* in their focus. Sector-specific standards include standards and associated documents, which address cyber security considerations that are specific to operators within the issuing industry.

Cross-sector standards are developed and issued by organizations whose focus extends across several discrete and dissimilar operating arenas, whose only common interest may be the prevention and mitigation of cyber attack upon their facilities. These standards address security issues that are of universal concern to infrastructure operators, without regard to the particular industry that may be implementing the standard.

Certain of these standards, such as those issued by the Federal Energy Regulatory Commission (FERC) and the Health Insurance Portability and Accountability Act (HIPAA), come from the Federal government and have the driving force of public law. Most others are issued by private and/or public industry organizations, and are dependent upon voluntary compliance.

## 5 MEASURE AND ASSESS SECURITY POSTURE

### 5.1 Risk Assessment Factors

Managing the security risks associated with the industry's growing reliance on control system and information technology (IT) is a continuing challenge. In particular, many private organizations have struggled to find efficient ways to ensure that they fully understand the cyber security risks affecting their operations, and can implement appropriate controls to mitigate these risks. A principal challenge that many companies face is identifying and ranking the cyber and control systems' security risks to their operations, which is the first step in developing and managing an effective security program. Taking this step helps ensure that organizations identify the most significant risks, and determines what actions are appropriate to mitigate them [7].

The General Accounting Office, in its white paper titled, "Information Security Risk Assessment: Practices of Leading Organizations" [8], has identified a set of common critical success factors that are important to the efficient and effective implementation of the organizations' information security risk assessment programs. These factors help ensure that the organizations benefit fully from the expertise and experience of their senior managers and staff, that risk assessments are conducted efficiently, and that the assessment results lead to appropriate remedial actions. The critical risk assessment success factors include the following:

1. Obtain senior management commitment, support, approval, and involvement to ensure that the resources are available to implement the program, and that assessment findings result in implementation of appropriate changes to policies and controls.
2. Designate individuals or groups as focal points to oversee and guide the overall risk assessment processes.

3. Define documented procedures for conducting risk assessments, and develop tools to facilitate and standardize the process.
4. Involve business and technical experts including a variety of individuals from the business unit having expertise in business operations, business processes, security, information resource management, IT, and system operations.
5. Hold business units responsible for initiating and conducting risk assessments, as well as evaluating and implementing the resulting recommendations.
6. Limit the scope of individual assessments by conducting a series of narrower assessments on various individual segments of the business and operations.
7. Document and maintain results so that managers could be held accountable for the decisions made, and a permanent record is established that can be used by auditors for compliance to the security policy [8].

### 5.2 Risk Measurement

The challenge in measuring risk is determining what to measure and how it should be measured. To measure the security posture of a control system, the organization needs to follow a set of rules that focuses the company security goals by applying the risk assessment factors described earlier. When assessing vulnerability, it is worthwhile to be aware of certain qualitative terms. Exposure is about possibility. Risk is about probability. And impact is about consequence. The following equation is sometimes used to express these mathematically: [9]

$$\text{Expected loss} \times \text{threat} \times \text{vulnerability} = \text{exposure} = \text{risk}$$

Exposure measurements can be used as a relative comparison within an environment or across companies. If one can assume that risk is constant for like-sized companies (even if we do not know the number itself), this exposure measure can act as a "risk proxy" to measure the relative difference in risk levels.

The Department of Homeland Security (DHS) under the FY2007 Homeland Security Grant Guidance describes the DHS approach to risk assessment as follows: risk will be evaluated at the federal level using a risk analysis model developed by DHS in conjunction with other federal entities. Risk is defined as the product of three principal variables:

- Threat (T)—the likelihood of an attack occurring.
- Vulnerability and consequence (V&C)—the relative exposure and expected impact of an attack [10].

$$\text{Risk } (R) = T \times V \times C$$

### 5.3 Security Metrics

Metrics and measurement are two vastly different concepts. Measurements are generated by counting, and provide specific views of discrete factors. Metrics, on the other hand, are generated through analysis. They are derived from measurements, to which contextual

information has been added for comparison, to a predetermined baseline, or comparing two or more measurements taken over time [11]. The measure of security policies, processes and products is the much-sought-after solution to this conundrum. Security managers in industry look for a magic formula that calculates risk and effectiveness in reducing risk, but the reality is that security metrics are not that simple. Measuring security is about using common sense. An organization needs to determine what to measure, and to organize the variables in a way that makes them manageable and meaningful. It needs to build repeatable formulas that show the snapshot status of security and how it changes over time.

Truly useful metrics indicate the degree to which goals are being met, and then drive actions taken to improve organizational processes. When applied to control system security performance, the metric is the expression of the state and/or quality of a critical aspect of the control system infrastructure. It is the basis for directing investments to areas of high risk, as well as a forum for communication to stakeholders both inside and outside the organization. Applying regular, repeatable metrics to a security performance initiative can benefit organizations in a number of ways. They:

1. provide a measurement of the effectiveness of controls;
2. identify and target areas for improvement;
3. communicate the effectiveness of risk management programs;
4. drive proper actions in focused areas and extend accountability;
5. provide hard evidence of compliance for internal and external use; and,
6. provide actionable views across the enterprise, lines of business, or specific areas of IT and control systems infrastructures [11].

## 6 CYBER SECURITY THREATS AND VULNERABILITIES

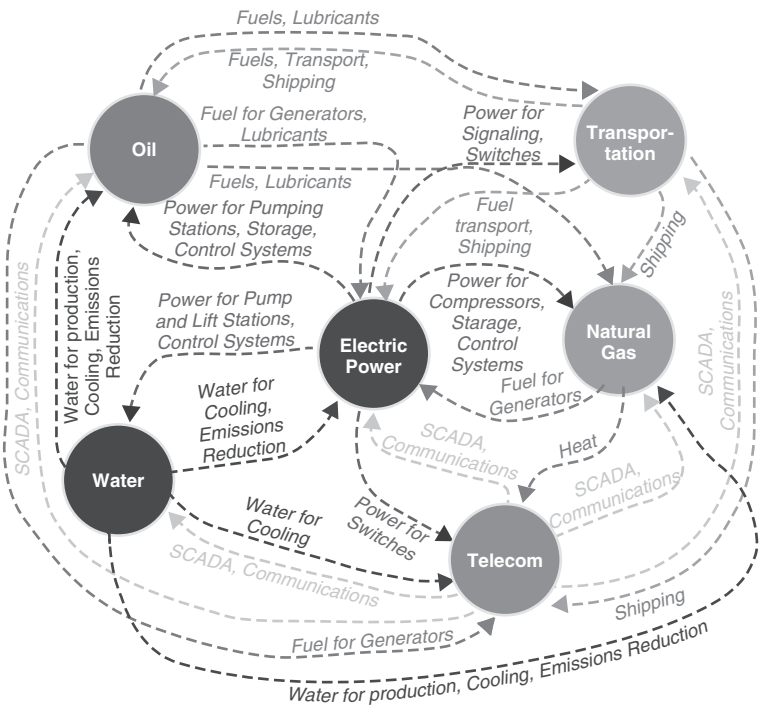
Many companies today have and are conducting security vulnerability analyses to evaluate the risks of physical attacks on their facilities, and many of these facilities have been hardened since 9/11. However, the importance of cyber security for manufacturing and control systems has only recently been recognized, and therefore has not yet been fully addressed by most industrial companies. Appropriate security measures must be taken to avoid events, which could have cascading impacts on other critical infrastructures (Figure 1) [12].

Lesser cyber attacks have and are occurring everyday. Actions are needed now to deal with this threat. Companies must conduct cyber security vulnerability analyses to identify threats to their control and support systems, to determine if vulnerabilities are present, and to evaluate existing countermeasures to determine if they need to be strengthened or new ones implemented. Control systems, and their support systems, are subject to threats from adversaries who may wish to disable or manipulate them by cyber or physical means, or who may want to obtain, corrupt, damage, destroy, or prohibit access to valuable information. The organization should evaluate the risk of these threats in order to decide what protective measures should be taken to protect systems from disruption. The vulnerabilities typically observed in the course of conducting vulnerability assessments are grouped in the following five categories: data, security administration, architecture, network, and platforms. Any given control system will usually exhibit a subset of these vulnerabilities, but may also have some unique additional problems [13]. The

Federal government has played an irreplaceable role in providing support for fundamental, long-term IT research and development (R&D), generating technologies that gave rise to the multibillion-dollar IT industry. The President's Information Technology Advisory Committee (PITAC) review of current federally supported R&D in cyber security finds an imbalance, however, in the current cyber security R&D portfolio. Most support is for short-term, defense-oriented research; there is relatively little support for fundamental research to address the larger security vulnerabilities of the civilian IT infrastructure, which supports defense systems as well.

In the report to the President in 2005, PITAC urged changes in the Federal government's cyber security R&D portfolio to increase federal support for fundamental research in civilian cyber security, intensify federal efforts to promote recruitment and retention of cyber security researchers and students at research universities, provide increased support for the rapid transfer of federally developed cutting-edge cyber security technologies to the private sector, and strengthen the coordination of the Interagency Working Group on Critical Information Infrastructure Protection and integrate it under the Networking and Information Technology Research and Development Program [14]. The Homeland Security Department has teamed with 13 organizations on a 12-month project to secure the process control systems of the nation's oil and gas industries against cyber security threats.

A cyber attack on the control and data systems that operate electric power plants, oil refineries, and gas pipelines, which are pieces of the nation's 18 critical infrastructure




Peerenboom, Fisher, and Whitfield, 2001

**FIGURE 1** Illustrative infrastructure interdependencies.

sectors, could potentially bring the country to a halt. The problem is compounded because private companies control more than 85% of the country's critical infrastructure, leaving the government few avenues to ensure that IT and control systems are secure. The potential costs of an infrastructure attack are significant. The Northeast Blackout on August 14, 2003, left 50 million customers and parts of eight states and Canada without power. According to a report by an electricity consumers research council, the outage cost an estimated $7–10 billion in financial losses; shut down parts of a 2 million barrel-per-day pipeline; and airports in 13 cities, To combat the cyber threats, the government, industry, research labs, security vendors, and process control technology vendors embarked on the project, "Linking the Oil and Gas Industry to Improve Cyber security", to come up with technology that could reduce vulnerabilities in infrastructure and could fix system vulnerabilities. The potential solution to such cyber threats is a strong cyber security posture by the entities that may be vulnerable to such attacks. A major challenge to preserve system protection is that system architectures change, technology changes, and threats change, all of which means that defenses must change.

## 7 CASCADING FAILURE

A cascading failure occurs when a disruption in one infrastructure causes a disruption in a second infrastructure (e.g. the August, 2003, blackout led to communications and water-supply outages, air traffic disruptions, chemical plant shutdowns, and other interdependency-related impacts) [12]. The complexity of multiple infrastructure linkages and the implications of multiple contingency events that may affect the infrastructures are apparent even in the highly simplified representation shown in Figure 1. The security, economic prosperity, and social well being of the nation depend on the reliable functioning of our increasingly complex and interdependent infrastructures. These include energy systems (electric power, oil, and natural gas), telecommunications, water-supply systems, transportation (road, rail, air, and water), banking and finance, and emergency and government services. In the new economy, these interconnected infrastructures have become increasingly fragile and subject to disruptions that can have broad regional, national, and global consequences. A disruption in an infrastructure would be magnified by the codependencies in supervisory control and data acquisition (SCADA) systems. An example might be a power loss that affects telecommunication systems upon which banking transactions rely. Vulnerability to these cascading effects was seen during Hurricanes Katrina and Rita in 2005, where a major American city came to a virtual standstill. As we are now seeing, it will take years to rebuild. Failure nodes are repeatedly created at the intersections of our tightly coupled, highly sophisticated transportation, electric power, and telecommunications systems. These failure potentials are compounded by the infrastructures' reliance on information and control systems' hardware and software. Understanding, analyzing, and sustaining the robustness and resilience of these infrastructures require multiple viewpoints and a broad set of interdisciplinary skills. For example, engineers (civil, electrical, industrial, mechanical, systems, etc.) are needed to understand the technological underpinnings of the infrastructures, as well as the complex physical architectures and dynamic feedback mechanisms that govern their operation and response (e.g. response to stresses and disruptions). Computer scientists, IT specialists, and network/telecommunication experts are needed to understand the electronic and informational (cyber) linkages among the

infrastructures. IT security, information assurance professionals, and control engineers are needed to ensure information and control system security [15].

## 8 LEGACY SYSTEMS

The term *legacy control system* is used variously to refer to old mainframe, dumb-terminal applications from the 1970s and 1980s; client/server systems of the 1990s; and even to first generation web-based business applications developed in the late 1990s [16]. In this section we will refer to legacy systems in the context of the first two examples. Legacy control systems were originally designed to be free standing networks without Internet access. These control systems monitored and controlled critical infrastructure processes. They were operated in an isolated or stand-alone environment where computer systems and devices communicated with each other exclusively, and typically did not communicate or share information with systems not directly connected to the control system network. These control systems typically comprised proprietary hardware, software, and protocols designed specifically for control system operations. Knowledge of these proprietary applications and protocols was limited to a small population. Proprietary control system protocols and data were not readily available to the general population and significant effort and resources would have been required to acquire the proprietary information, understand the control system, discover vulnerabilities in the control system, develop the tools to exploit the identified vulnerabilities, and gain sufficient access to the control system so that vulnerabilities could be exploited to carry out unauthorized or malicious activities. For the reasons presented, in particular because access to control systems was greatly limited, critical infrastructure control system security efforts were primarily focused on protecting control systems from physical attacks. More recently, with the vast IT expansion and the drive toward having information readily available from any location, many previously stand-alone control systems are being transitioned to the "always connected" world, where real-time control system information can be readily and easily accessed remotely by vendors, engineers, maintenance personnel, business managers, and others via corporate networks, the Internet, telephone lines, and various wireless devices.

Legacy systems that have been retrofitted to incorporate Internet accessibility may be especially vulnerable to attack due to the ad hoc manner of their integration with the network. This imperfect fit between the different software applications could generate more vulnerable code aspects than would be found in a single piece of software. It may be possible, for example, through a poorly defined variable, to force a software program to behave in a way not expected by the author. When two programs are brought together, the potential program weaknesses are multiplied. Thus, legacy systems with network access added may be more prone to security flaws and weaknesses than systems that use a single piece of software for both functions [17]. To reduce operational costs and improve performance, control system vendors and critical infrastructure owners and operators have been transitioning from proprietary systems to less expensive standardized technologies, operating systems, and protocols currently prevalent on the Internet. These widely accepted technologies, protocols, and operating systems, such as Ethernet, Internet Protocol, Microsoft Windows, and web technologies, have a large number of known cyber vulnerabilities, and new vulnerabilities are reported on a daily basis. Exploitation tools, malware, and how-to papers are often readily available shortly after the announcement of a new vulnerability. Significant information on control systems is

now publicly available, including design and maintenance documents, technical standards for the component interconnections, and standards for communicating between devices. In addition, control system security concerns are elevated because control systems are typically not up-to-date with the latest security patches, fixes, and best practices due to concerns with taking real-time systems off-line and concerns over making system modifications, which might affect the time sensitive operations of the control system or potentially affect existing agreements with control system vendors or others [18]. Legacy system operators must be aware of the vulnerabilities inherent with upgrading to meet today's networking capabilities, and implement appropriate protection options. Some examples of "best practice" options (that are applicable to all systems, from legacy to state-of-the-art) include: disabling unused ports; encryption; dual authentication; and working with both private sector and government agencies to identify and put into use more robust security measures.

## 9 INTRUSION DETECTION AND RESPONSE TECHNOLOGY

The increasing speed of attacks against IT and control systems highlights a requirement for comparably timely responses. Threats such as malware and scripted exploits often allow a time frame of only a few minutes or even seconds to respond, which effectively eliminates the feasibility of manual intervention and highlights a requirement for automated approaches to provide a solution. However, it can be seen that existing security technologies are often insufficient. For example, although intrusion detection systems (IDS) can be used to identify potential incidents, they have a tendency to produce high volumes of false alarms and consequently cannot be trusted to issue automated responses for fear of disrupting legitimate activity. Intrusion detection has been at the center of intense research in the last decade, owing to the rapid increase of sophisticated attacks on computer systems. Typically, intrusion detection refers to a variety of techniques for detecting attacks in the form of malicious and unauthorized activity. In the event that intrusive behavior is detected, it is desirable to take evasive and/or corrective actions to thwart attacks and ensure safety of the computing environment. Such countermeasures are referred to as *intrusion response*. Although the intrusion response component is often integrated with the IDS, it receives considerably less attention than IDS research, owing to the inherent complexity in developing and deploying responses in an automated fashion. Development of an effective response mechanism for potential intrusions is inherently complex due to the requirement to analyze a number of "unknown" factors in various dimensions: intrusion cause/effect, identification of optimal response, state of the system, maintainability, and so on. As such, it is necessary to have a complete understanding of the problems that need to be addressed for developing a smart and effective response system.

Considerable research has focused on intrusion response specification that addresses the countermeasure steps to sophisticated attacks on the control and computer support systems. For example, the following specifications are being considered as requirements in the development of an ideal intrusion response system:

1. *Automatic.* The volume and the intensity of intrusions today require rapid and automated response. The system must be reliable to run without human intervention. Human supervision often brings a significant delay into intrusion handling; the response system alone should have means to contain incurred damage and

prevent harmful activity. Although complete automation may not be achievable in practice due to presence of novel intractable intrusions, significant reduction of human effort and expert knowledge is desirable.

2. *Proactive.* Modern software systems are built on multiple heterogeneously developed components that have complex interactions with each other. Because of these interactions, intrusions are likely to spread rapidly, causing more damage. A proactive approach to response is the most practical in intrusion containment.
3. *Adaptable.* The presence of multiple components that constitute a software system also results in a dynamic environment owing to the complex interactions between components. As such, intrusive behavior can affect systems in a way that is unpredictable. The intrusion response system should be equipped with means to recognize and react to changes in the dynamic environment.
4. *Cost-sensitive.* Response to intrusions in dynamic and complex systems requires a careful consideration of the trade-offs among cost and benefits factors. A simple basic response action, triggered every time certain symptoms are observed, might be a wasteful effort and may cause more damage [19].

## 10 RESEARCH DIRECTION

Because of the constantly changing threats to control systems, as well as the vulnerabilities of these systems to cyber attack, multiple approaches to security should be undertaken. For one, continued research is needed to develop security policies, guidelines, and standards for control system security. This could include things such as authentication methods and the use of networks. The results of this research should then be incorporated into standards, in order that all stakeholders may benefit from the research. Continued development of strong standards is a key in securing control systems from cyber intrusions.

Another approach to be considered is the use of vulnerability assessments. An organization must be able to conduct a comprehensive vulnerability assessment if it intends to successfully measure the security posture of its control systems. A key step in this process is to learn and apply the seven critical risk assessment success factors listed earlier in the article. These factors are important to the efficient and effective implementation of the organizations' information security risk assessment programs. The Federal government must continue to be in the forefront of programs providing support for fundamental research in civilian cyber security.

Organizations should implement effective security management programs that include consideration of control system security. To measure security posture of the control systems, the organization needs to employ a set of rules, or metrics that quantify its achievement in terms of the company security goals. Vulnerability should be determined in terms of exposure to attack, probability of attack, and consequences of an attack. The goal should always be to identify vulnerabilities and then to implement mitigation strategies. Possible strategies include developing or improving the organization security policy. Adherence to one or more recognized security standard should always be part of organization policy.

Cascading failures can have broad regional, national, and global consequences. Control systems need to be carefully designed to reduce the interdependence of multiple infrastructures, and to mitigate the effects when a failure occurs.

Legacy control systems no longer profit from "security through obscurity" [20]. In fact, those that have been retrofitted to incorporate Internet accessibility may be especially vulnerable to attack, due to imperfect matchups between software applications. Legacy system operators must be aware of the vulnerabilities inherent with upgrading to meet today's networking capabilities, and implement all appropriate protection options.

In order to cope with the speed and frequency of today's cyber attacks, effective intrusion detection and response systems must react in similar rapid fashion. Current research and development efforts focused on new technology and tools to counter such attacks indicate a need for automated, proactive responses, which are adaptable to changing situations and technology, and are cost-effective.

## REFERENCES


1. National Standards Policy Advisory Committee (1978). *National Policy on Standards for the United States and a Recommended Implementation Plan*, National Standards Policy Advisory Committee, Washington, DC, p. 6.
2. CPM Resource Center (2007). *How to Write Practice Guidelines*, CPM Resource Center, http://www.cpmrc.com/events/workshop_17.shtml, accessed 01/22/2007.
3. *Guideline, Wikipedia, the Free Encyclopedia*, (2007). http://en.wikipedia.org/wiki/Guideline, accessed 01/22/2007.
4. *Definition of Best Practices*, (2007). Walden 3-D, Inc., http://www.walden3d.com/og1/bp.html, accessed 01/22/2007.
5. *Best Practice, Wikipedia, the Free Encyclopedia*, (2007). http://en.wikipedia.org/wiki/Best_practice, accessed 01/21/2007.
6. Joseph Weiss, P. E., Ed. (2003) *IEEE Task Force Revising Equipment Standards to Protect Against Cyber Attacks*, Electric Energy T & D Magazine http://realtimeacs.com/?page_id=13.
7. U.S. General Accounting Office (1999). *Information Security Risk Assessment; Practices of Leading Organizations Exposure Draft*, U.S. General Accounting Office (GAO/AIMD-99-139)] 08/1999, http://www.gao.gov/special.pubs/ai00033.pdf.
8. U.S. General Accounting Office (1999). *Information Security Risk Assessment: Practices of Leading Organizations Exposure Draft*, U.S. General Accounting Office (GAO/AIMD-99-139) 08/1999, http://www.gao.gov/special.pubs/ai00033.pdf.
9. Lindstrom, P. *"RISK MANAGEMENT STRATEGIES" Security: Measuring Up*, CISSP 02/18/2005.
10. *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, CRS Report for Congress, February 2, 2007.
11. *Seven Steps to Security Metrics Success*, white paper by ClearPoint Metrics http://www.dreamingcode.com/dc_ecomm/DocumentManage/DocumentManagement/56_82doc.pdf, 2008.
12. Peerenboom, J. P., and Fisher, R. E. (2007). *Analyzing Cross-Sector Interdependencies*, Infrastructure Assurance Center, Argonne National Laboratory, http://ieeexplore.ieee.org/iel5/4076361/4076362/04076595.pdf.
13. Stamp, J., Dillinger, J., and Young, W. (2003). *Common Vulnerabilities in Critical Infrastructure Control Systems*, Sandia National Laboratories, May 22, http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf.
14. President's Information Technology Advisory Committee (PITAC) (2005). *Report to the President - Cyber Security: A Crisis of Prioritization, February*.
15. Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Complex Networks: Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *Infrastructure*

*Interdependencies—Overview of Concepts and Terminology*, Infrastructure Assurance Center, Argonne National Laboratory, http://www.ce.cmu.edu/∼hsm/im2004/readings/CII-Rinaldi.pdf.

16. Weber C. (2006). *Assessing Security Risk in Legacy Systems*, Cigital, Inc., Copyright © 2006, Cigital, Inc., https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/legacy/624-BSI.pdf.
17. Shea, D. A. (2003). *Critical Infrastructure: Control Systems and the Terrorist Threat* Report for Congress (Updated February 21, 2003) Consultant Resources, Science, and Industry Division.
18. Dacey, R. F. (2003). *Critical Infrastructure Protection: Challenges in Securing Control Systems*, Information Security Issues, US General Accounting Office, October 10.
19. Stakhanova, N., Basu, S., and Wong, J. (2006). *A Taxonomy of Intrusion Response Systems*, Department of Computer Science Iowa State University, Iowa, USA, February.
20. Furnell, S., and Papadaki, M. (2005). *Automated Intrusion Response*, Network Research Group, School of Computing, Communications & Electronics, University of Plymouth, for Business Briefing Data Management, Storage, & Security Review, http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VJC-4HDWHP7-4&_user=1722207&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_version=1&_urlVersion=0&_userid=1722207&md5=b8a685ed03dfeadde206a5e355f4f2dd.

## FURTHER READING

Carlson, R. E., Dagle, J. E., Shamsuddin, S. A., and Idaho, P. E. (2005). *A Summary of Control System Security Standards Activities in the Energy Sector prepared for Department of Energy Office of Electricity Delivery and Energy Reliability under National SCADA Testbed*, October 2005.

Balepin, I., Maltsev, S., Rowe, J., and Levitt, K. (2003). Using specification-based intrusion detection for automated response". *Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection*, Pittsburgh, PA.

Chiles, J. R. (2001). *Inviting Disaster: Lessons From The Edge of Technology*, HarperCollins Publishers, New York.

Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, October 1997.

Instrumentation, Systems, and Automation Society. (2004). ISA-TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control Systems Environment*, ISBN: 1-55617-889-1, Research Triangle Park, NC.

Instrumentation, Systems, and Automation Society. (2004). ISA-TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems*, ISBN: 1-55617-886-7, Research Triangle Park, NC.

Kabiri, P., and Ghorbani, A. A. (2005). Research on intrusion detection and response. A survey. *Int. J. Netw. Secur.* **1**.

Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*, Princeton University Press, Princeton, NJ.

Petroski, H. (1992). *To Engineer Is Human: The Role of Failure in Successful Design*, Vintage Books, New York.

Petroski, H. (1994). *Design Paradigms: Case Histories of Error and Judgment in Engineering*, Cambridge University Press, Cambridge.

Rinaldi, S., Peerenboom, J., and Kelly, T. (2001). For a more complete description of infrastructure interdependencies, see *Complexities in Identifying, Understanding, and Analyzing Critical*

*Infrastructure Interdependencies* invited paper for special issue of IEEE Control Systems Magazine on "Complex Interactive Networks," December.

United States Computer Emergency Readiness Team (2005). *Control Systems Cyber Security Awareness* US-CERT Informational Focus Paper, Produced by, July 7.

# IMPLICATIONS OF REGULATION ON THE PROTECTION OF CRITICAL INFRASTRUCTURES

REBECCA HAFFENDEN

*Los Alamos National Laboratory, Los Alamos, New Mexico*

## 1 INTRODUCTION

In analyzing the security of a nation's infrastructure facilities, the impact of the regulatory environment on an infrastructure or a facility must also be considered. Laws and regulations that control both the day-to-day operations and emergency response activities for any facility can originate from a variety of sources. Such regulations are promulgated on the basis of very specific legislation enacted in response to public needs, political forces, or particular events. These regulations, although well written and well thought out for their particular purpose, can have unintended impacts on the security of infrastructure facilities and on the interaction between infrastructures (i.e., interdependencies). Consequently, there should be a mandatory review process for proposed legislation and the corresponding regulations to determine if the legislation or regulation could impact security or emergency response requirements and policies at both the federal and state levels, if the regulation could unintentionally result in increasing the vulnerability of the affected facilities/industries or even if other interdependent facilities/industries will be impacted.

## 2 THE REGULATORY PROCESS

In the United States, the general regulatory process starts with the enactment of legislation granting authority to one or more federal agencies to create, implement, and enforce a regulatory program based on the intent and scope of the legislation (the legislative mandate). The federal agency then drafts its proposed regulations pursuant to that authority.

Under the Administrative Procedures Act, the agency must publish the proposed regulation in the Federal Register to allow the public to comment. The federal agency then reviews the proposed regulation in light of the comments received and issues a final rule. The final rule is also published in the Federal Register and after the indicated effective date, it can be implemented and enforced.

In general, regulations are limited to the intent and scope established in the enabling legislation and to the express statutory authority granted to a federal agency.[1] This legislative mandate or statutory authority generally addresses either the specific industry or a specific topic within the jurisdiction of the implementing regulatory agency. For example, the Nuclear Regulatory Commission (NRC) issues regulations pertinent to a specific type of facility, namely, nuclear power plants; it does not issue regulations on the operation of airports. The Environmental Protection Agency (EPA) issues regulations on activities that impact the environment; even though the regulatory program may impact a number of different types of infrastructures or industries, they address only the environmental impact, not the stock issuance requirements of those industries. Therefore, it is likely that proposed industry, facility, or activity specific regulations may only be reviewed for their impact on the industry/topical activities they specifically address and not on their unintentional impact on the security of the affected facilities/industries, the emergency planning that may involve the affected facilities/industries, or the impact on other critical interdependent infrastructures.

A classic example of this conflict is found in the regulatory implementation of Section 112(r) of the Clean Air Act (CAA) [2]. The accidental and sudden release of methyl isocyanate in an industrial accident at the Union Carbide plant in December 1984 in Bhopal, India spurred the study of the risk of accidental chemical releases in the United States. In 1990, Congress enacted Section 112(r) of the CAA to address the threat of catastrophic releases of chemicals that might cause immediate deaths or injuries in surrounding communities. Pursuant to this legislation, EPA promulgated regulations for the prevention and mitigation of accidental releases of extremely hazardous substances. Covered facilities are required to submit to EPA a risk management plan (RMP) describing the source's risk management program. Covered facilities are required to conduct potential off-site consequences analysis (OCA) of hypothetical worst case and alternative accidental release scenarios. Under the original rule, facilities were required to include a brief description of this analysis in the executive summary of their RMPs. The RMPs were required to be made available to the public and the executive summaries were to be posted to the EPA Internet site.

The Federal Bureau of Investigation and other representatives of the law enforcement and intelligence communities raised concerns that releasing the OCA portions of RMPs via Internet would enable individuals anywhere in the world anonymously to search electronically for industrial facilities in the United States to target for purposes of causing an intentional industrial chemical release. In response to those concerns, EPA posted RMPs on the Internet without the OCA results.

However, those OCA sections, and any EPA electronic database created from those sections, were still subject to public release in electronic format pursuant to the Freedom

[1]The interpretation put on the statute by the agency charged with administering it is entitled to deference, [1], but the courts are the final authorities on issues of statutory construction. They must reject administrative constructions of the statute, whether reached by adjudication or by rulemaking, that are inconsistent with the statutory mandate or that frustrate the policy that Congress sought to implement.

of Information Act (FOIA).[2] On August 5, 1999, the Chemical Safety Information, Site Security and Fuels Regulatory Relief Act (CSISSFRRA) was enacted[3] to provide at least a one-year exemption from FOIA for the OCA portions of RMPs and any EPA database created from those portions. As required by the CSISSFRRA, assessments were conducted of both the increased risk of terrorist and other criminal activity that would result from posting OCA information on the Internet and the chemical safety benefits of allowing public access to the information.

Based on the assessments, the EPA and the Department of Justice (DOJ) issued regulations governing access to, and dissemination of, restricted forms of information about the potential off-site consequences of accidental chemical releases from industrial facilities. That regulation, found at 40 Code of Federal Regulations (CFR) 1400, allows the public with access to paper copies of OCA information through at least 50 federal reading rooms distributed across the United States and its territories. It also provides Internet access to the OCA data elements that pose the least serious criminal risk. In addition, the rule authorizes any member of the public will be able to read at federal reading rooms, although not remove or mechanically reproduce, a paper copy of OCA information for up to ten facilities per calendar month located anywhere in the country, without geographical restriction. In addition, any person will be able to view OCA information for facilities located in the jurisdiction of the Local Environmental Protection Committee (LEPC) where the person lives or works and for any additional facilities with a vulnerable zone extending into that LEPC's jurisdiction. This rule was effective from August 4, 2000.

The regulations promulgated by the EPA under Section 112(r), were intended to carry out the legislative mandate to inform communities from the release of hazardous chemicals in their area; however, only after promulgation and implementation was the impact on chemical facility security recognized.

In addition, in the United States, some rule making is accomplished through regulatory negotiation (RegNeg) where the implementing agency works with industry partners, industry associations, or other related entities to formulate regulations in a cooperative atmosphere. These regulations are thus negotiated with a small, narrow group of like partners that may not consider the impact of their decisions on other infrastructures or activities.

Another form of rule making is that conducted pursuant to Office of Management and Budget (OMB) Circular A119 and the National Technology Transfer and Advancement Act [3]. OMB Circular A119 directs federal agencies to use voluntary consensus standards in lieu of government-unique standards except where inconsistent with law or otherwise impractical. Voluntary consensus standards bodies are usually made up of interested parties and have the following attributes: openness, balance of interest, due process, an appeals process, and consensus (or general agreement). Therefore, standards developed or adopted by voluntary consensus standards bodies again would be, if adopted by a federal agency, a regulation made up by a small, narrow group of like partners that may not consider the impacts of the regulation on other aspects of the affected infrastructure or other interdependent infrastructures.

[2]5 U.S.C. 552.
[3]Public Law No. 106–40.

## 3 FEDERAL VERSUS STATE/LOCAL LAW

Many laws and regulations that impact critical infrastructure industries and facilities originate at the federal level. Some regulatory schemes specifically create a process for states to be authorized to implement and enforce the federal regulatory programs within their individual states, for example, the EPA hazardous waste regulations[4] or the Department of Transportation Office of Pipeline Safety pipeline inspection and safety regulations.[5] Under most of the state-delegated authority regulatory schemes, the state may adopt more stringent, but not less stringent, requirements than those in the federal regulations.

However, states may adopt state-specific requirements for critical infrastructure industries and facilities, such as state permitting or siting requirements for federally licensed energy facilities.[6,7] In general, under Article VI of the United States Constitution, the "Supremacy Clause", federal law is the law of the land "anything in the constitutions or laws of any State to the contrary notwithstanding." Therefore, states can legislate/regulate only those areas where federal law does not apply or those areas where the federal law specifically delegates authority to the states. Federal preemption of state law can be (i) expressed or directly stated in the federal legislation or regulation, (ii) implied, where it is inferred from the Congressional intent, as revealed by legislative history or statutory language, (iii) where the federal regulatory program is found to be pervasive and there is nothing left for the states to regulate, often called "occupation of the field", (iv) where the state law frustrates the perceived Congressional policy or program, and/or (v) where there is a direct conflict between the state and the federal regulatory programs. States can also adopt state-specific laws and regulations regarding areas where the federal government has not implemented a regulatory scheme, or where the safety and health of the state citizens is a major factor in regulation [5].

Although the terminology discussed above represents the regulatory process in the United States, most nations have a similar process. For instance, similar to the United States Congress, the Australian Commonwealth Parliament is able to make laws only in relation to a range of specific subjects listed in the Constitution, including defense, external affairs, trade, and immigration, and taxation. The Commonwealth has also legislated by agreement with the states, in areas with Australia-wide application, such as broadcasting, navigation, and food standards. Again, similar to the United States, the Australian Constitution does not limit the subjects on which the states may make laws; however, a state law is invalid to the extent it is inconsistent with a valid Commonwealth law on the same subject [6].

For the European Union (EU), legislation is proposed by the European Commission. Such proposed legislation, depending on the legal basis of the proposal, is either adopted or rejected by the European Council or by the Council and the European Parliament jointly. The legal basis of the proposed legislation also determines whether there should be consultation with other EU institutions or agencies. Once adopted, legislation is applicable

[4]40 Code of Federal Regulations (CFR) 260, et seq.

[5]49 CFR. Parts 190, 191, and 192.

[6]For example, Oregon Revised Statutes, Chapter 469: Energy Conservation Chapter 345-021-0000 et seq., Oregon Administrative Rules; In 2001, the Colorado Legislature approved House Bill 01-1195. The bill provided a legal means for public utilities to appeal local land use decisions on utility siting issues to the Public Utilities Commission.

[7]The regulation of health and safety matters is primarily and historically a matter of local concern [4].

to all EU members and each nation must adopt its own laws and regulations to implement the legislation.

In addition, and often forgotten, local agencies can have local ordinances (e.g. city or county zoning, building, and fire codes) that apply to critical infrastructure assets.[8] Local ordinances (i.e., county or municipal), can also impact infrastructure facilities. As with the federal—state regulatory scheme, local ordinances are either based on delegated powers from the state government or are limited to those areas where local jurisdiction is either statutorily established or historically left to local governments. Examples include property zoning regulations; fire, building, and electrical codes; noise limits; and highway requirements (e.g. traffic patterns, speed limits, and road weight restrictions).

This regulatory scheme results in multiple layers of regulation for each infrastructure and each facility/asset. Each layer (federal, state, or local) has a different jurisdiction and each agency within each layer has its own statutory mandate.

## 4 THE REGULATORY ENVIRONMENT FOR CRITICAL INFRASTRUCTURES

Regulations may provide for agency oversight (e.g. agency inspections, recordkeeping, and reporting requirements), may be economic based (e.g. rate setting or investment incentives) or may involve very specific, detailed prescriptive or performance-based requirements for operational activities or even physical configuration of a facility. Some regulations are specific to a particular industry (e.g. air emissions from publication rotogravure printing facilities[9]), whereas others affect a number of industries and asset types (e.g. Occupational Safety and Health Administration (OSHA) worker safety[10] or American with Disabilities Act (ADA) regulations [7]).

In general, most private industry owners resist any governmental regulation of their activities, including security and vulnerability reduction. There are arguments on both sides of the issue with some, including the Congressional Budget Office, stating businesses would be "inclined to spend less on security than might be appropriate for the nation as a whole if they faced losses from an attack that would be less than the overall losses for society;" [8] whereas others would argue companies are motivated to invest in security in order to protect their own continuity of operations, without which the company has no income/profit, which is in their best interest[11]. Many critical infrastructure facilities and activities were already heavily regulated before the events of September 11, 2001. However, at this time, only a few critical infrastructures have had in-depth governmental security regulations imposed upon them, generally in the transportation, maritime, and nuclear power industries.

However, all 17 critical infrastructures and key resources[12], both governmental and privately owned, are regulated by a variety of overarching health, safety, environmental,

[8]40 CFR 63.824.
[9]29 CFR 1900, et seq.
[10]28 CFR Part 36.
[11]Agriculture & Food, Public Health, Water, Energy, Banking, National Monuments, Defense Industrial Base, Commercial Chemical, Telecommunications, Postal & Shipping, Government Facilities, Transportation, Dams and Nuclear Power.
[12]The Guidelines are not however, enforceable requirements, but instead FERC inspectors review the effectiveness of each installation's protective measures on a case-by-case basis.

employee, and privacy regulations (i.e., nonsecurity-related regulations) that impact their day-to-day operations as well as their response to emergency situations. Some infrastructures have deregulated such that economic regulatory control and oversight may have lessened, including telecommunications, electric power, natural gas, and oil production, however, these general overarching regulations would still apply to the activities and facilities of these "deregulated" industries. Table 1 shows the major regulatory agencies for each infrastructure, as well as a list of the general areas of jurisdiction.

The commercial sector, which is usually made up of privately owned industrial facilities, commercial buildings, shopping malls, arenas, or stadiums, has few industry-specific security regulations, though they will be subject to worker safety, general zoning, fire protection, and other building safety regulations.

In addition, many infrastructures also must meet independent industry association requirements. For instance, since rate deregulation, energy infrastructures must also meet the requirements of the Independent System Operator (ISO) for marketing energy in interstate and intrastate commerce. In addition, the North American Electric Reliability Council requires its members to meet its regulations for safety and security of the electric power transmission grid. The chemical and hazardous materials infrastructure has numerous independent industry associations that impose member requirements for safety and security, including the American Chemical Council's Responsible Care initiative. These industry self-regulations add another layer of requirements that could impact nonsecurity regulatory requirements and security policy requirements.

As discussed above, most federal, state, and local regulations are established on the basis of implementing each agency's specific statutory scope of authority. Therefore, a critical infrastructure facility may be regulated by various federal, state, and local agencies, each for a separate purpose. In addition, many infrastructures are systems, made up of many assets. For example, the electric power infrastructure has generation facilities (which can be nuclear, fossil fuel, or hydropowered), transmission and distribution facilities, substations, communication networks, marketing activities, personnel, equipment/trucks, and other transportation facilities (e.g. railroads for coal). Regulation by these various local, state, and federal agencies can be additive, duplicative or even conflicting. Figure 1 shows an example of the numerous regulatory interfaces for the electric power infrastructure.

## 5 THE INTERRELATIONSHIP BETWEEN SECURITY AND NONSECURITY-RELATED REGULATIONS

Nonsecurity-related regulations might have an unintentional positive or negative impact on the security of critical infrastructure facilities and assets. Conversely, new security-related regulations may unintentionally impact and even conflict with nonsecurity regulations, rights, or policies.

The security of critical infrastructures/key assets is dependent on many factors. Each type of critical asset has a need for a different type of security depending on the type of threat. Some critical assets are susceptible to physical attack; others to cyber infiltration.

Nonsecurity regulations may impact both the physical security/vulnerability of the regulated facility, the cyber security/vulnerability of information, the facility/industry operational security/vulnerability (e.g. availability of sensitive information about the regulated facility/industry), or the ability of the facility to recover from a catastrophic incident. On the other hand, security-related regulations may impact health and safety requirements,

**TABLE 1 Key Regulatory Authorities by Infrastructure**

| Infrastructure | Regulating Agencies | General Areas of Jurisdiction |
|---|---|---|
| Agriculture and food | • Department of Agriculture | • Crops |
| | | • Packaging |
| | • US Food and Drug Administration | • Additives |
| | | • Animal husbandry |
| | • Department of Commerce, National Marine Fisheries Service | • Meat processing |
| | | • Fish processing |
| | | • Pesticide Application/residuals |
| | • Environmental Protection Agency | |
| | • State Agriculture and Pesticide Regulators | |
| Banking and finance | • Department of the Treasury | • Banks |
| | | • Federal Reserve System |
| | • Federal Reserve | • Mints |
| | • Federal Deposit Insurance Corporation | • Stock trading |
| | | • Commodities future trading |
| | • Securities and Exchange Commission | |
| | • Commodities Futures Trading Commission | |
| | • State Banking Regulators | |
| Chemical and hazardous materials | • Department of Transportation | • Air emissions |
| | | • Storing and handling of chemicals/hazardous materials |
| | • Environmental Protection Agency | |
| | • Department of Labor | • Hazardous wastes |
| | –Occupational Safety & Health Administration | • Pesticides |
| | • Local Zoning Boards | |
| Commercial | • Department of Education | • Schools |
| | • Local Building and Fire Codes | • Office buildings |
| | | • Public assembly facilities |
| | | • Residential buildings |
| | | • Stadiums/arenas/raceways |
| Dams | • Federal Emergency Management Agency | • Dams |
| | | • Levees |
| | • United States Army Corps of Engineers | |
| | • FERC | |
| | • Department of the Interior | |
| | –Bureau of Reclamation | |
| | –Bureau of Land Management | |
| | –National Park Service | |
| | –Fish and Wildlife Service | |
| | • Department of Agriculture | |
| | • Tennessee Valley Authority | |

**TABLE 1 (*Continued*)**

| Infrastructure | Regulating Agencies | General Areas of Jurisdiction |
|---|---|---|
| | • Department of Energy<br>• Nuclear Regulatory Commission<br>• International Boundary and Water Commission<br>• State Dam Safety Agencies | |
| Defense industrial base | • Department of Defense | • Defense contractor facilities |
| Emergency services | • Federal Emergency Management Agency | • Police |
| | | • Fire |
| | • State Emergency Management Agencies | • Emergency medical technicians |
| | | • Ambulance |
| Energy | | |
| Electric | • Department of Energy<br>–Federal Energy Regulatory Commission | • Generation facilities<br>–Fossil fuel |
| | | –Hydro |
| | • State Public Utility Commissions | –Wind |
| | | –Solar |
| | | • Transmission lines |
| | | • Distribution lines |
| | | • Substations |
| | | • Switching stations |
| Natural gas | • Department of Energy<br>–Federal Energy Regulatory Commission | • Wells<br>• Gathering pipelines |
| | | • Transmission pipelines |
| | • Department of Transportation | • Distribution pipelines |
| | | • Compression facilities |
| | • State Public Utility Commissions | • Storage |
| | | • Liquefied natural gas plants |
| | • State Environmental or Mineral/Mining/Drilling Agencies | |
| Petroleum | • Department of Energy<br>–Federal Energy Regulatory Commission | • Wells<br>• Outer continental shelf drilling |
| | • Department of the Interior | • Gathering pipelines |
| | | • Transportation pipelines |
| | –Minerals Management Service | • Storage terminals |
| | | • Refineries |
| | • Environmental Protection Agency (oil spills) | • Port facilities |
| | • State Environmental or Mineral/Mining/Drilling Agencies | |
| Government facilities | • General Services Administration | • Personnel-related buildings (e.g. Headquarters) |
| | • Federal Protective Service | • Research-related buildings |

**TABLE 1 (*Continued*)**

| Infrastructure | Regulating Agencies | General Areas of Jurisdiction |
|---|---|---|
| Information technology | • Department of Homeland Security | • Internet |
| | • Office of Cyber Security and Telecommunications | |
| National monuments and icons | • Department of the Interior | • National monuments |
| | | • National parks |
| | –National Park Service | • National forests |
| | –Bureau of Land Management | • Iconic government buildings |
| | –Bureau of Reclamation | |
| | • Department of Agriculture | |
| | –Park Service | |
| | • General Services Administration | |
| Nuclear plants | • Nuclear Regulatory Agency | • Nuclear power plants |
| | | • Radioactive materials |
| | | • Radioactive wastes |
| Postal and shipping | • United States Postal Service | • Post offices |
| | | • Commercial shipping |
| | • Department of Transportation | |
| Public health | • Department of Human Health and Services | • Public health system |
| | | • Laboratories |
| | –Public Health Service | • Possession, use, and transfer of select agents and toxins |
| | –Centers for Disease Control and Prevention | |
| | • State Health Departments | • Hospitals and clinics |
| Tele-communications | • Federal Communication Commission | • Telephone switching facilities |
| | • Department of Commerce, National Telecommunications and Information Administration | • Telephone lines |
| | | • Cellular telephone towers |
| | | • Satellite services |
| | | • Radio communications |
| | | • Underwater cable landings |
| | • Office of Science and Technology Policy and National Security Council | |
| | • State Public Utility Commissions | |
| Transportation | • Department of Homeland Security | • Highways |
| | | • Tunnels |
| | –Transportation Security Administration | • Bridges |
| | | • Railroads |
| | –United States Coast Guard | • Maritime ports |
| | | • Locks and dams |
| | • United States Army Corps of Engineers | • Pipelines |
| | | • Trucks and drivers |
| | • Department of Transportation | |

**TABLE 1 (*Continued*)**

| Infrastructure | Regulating Agencies | General Areas of Jurisdiction |
|---|---|---|
| | – Federal Railroad Administration<br>– Pipeline and Hazardous Materials Safety Administration<br>– Federal Transit Administration<br>– Federal Highway Administration<br>– Federal Motor Carrier Safety Administration<br>– Federal Aviation Administration<br>– Maritime Administration<br>– Surface Transportation Board<br>• State Transportation and Transit Agencies | |
| Water and Wastewater | • Environmental Protection Agency<br>• State Environmental Agencies | • Potable water treatment<br>• Portable water distribution<br>• Wastewater treatment<br>• Wastewater collection<br>• Aqueducts |

individual or corporate privacy, or interstate commerce. The following section discusses some examples of where regulations may impact the security/vulnerability of critical infrastructure facilities and assets.

### 5.1 Health and Safety Versus Security

An example of safety regulations assisting in protecting critical infrastructure/assets is found in Federal Energy Regulatory Commission (FERC) regulations applied to FERC-regulated dams. Pursuant to FERC regulations, an owner of a project may be required to install and properly maintain any signs, lights, sirens, barriers, or other safety devices necessary to adequately warn and/or protect the public in its use of project lands and waters. Under FERC Guidelines[13] for Public Safety at Hydropower Projects certain physical protections are suggested for dam owners, such as restraining devices, fences, or guards.

Restraining devices include boat restraining barriers, fences, guardrails, natural barriers, trashracks, debris deflector booms, and other similar devices. Under the Guidelines, boat- restraining barriers, as well as warning devices, should be provided at those projects, where boaters and canoeists are exposed to hazardous spillways, tailrace areas, or intake areas. However, boat restraining barriers are not required at those projects where bridges or other structures constitute an adequate physical barrier, or if it can be assured that hazardous flows and conditions do not occur at the projects during time of the year when boaters or canoeists use the reservoirs. Any type of barrier, such as trash booms, debris deflector booms, log booms, and specially designed barriers that have been placed

[13]For Example, City of Chicago Municipal Code, Section 13-196-084, which requires access to the interior of the building and to the second vertical exit from a stairwell.

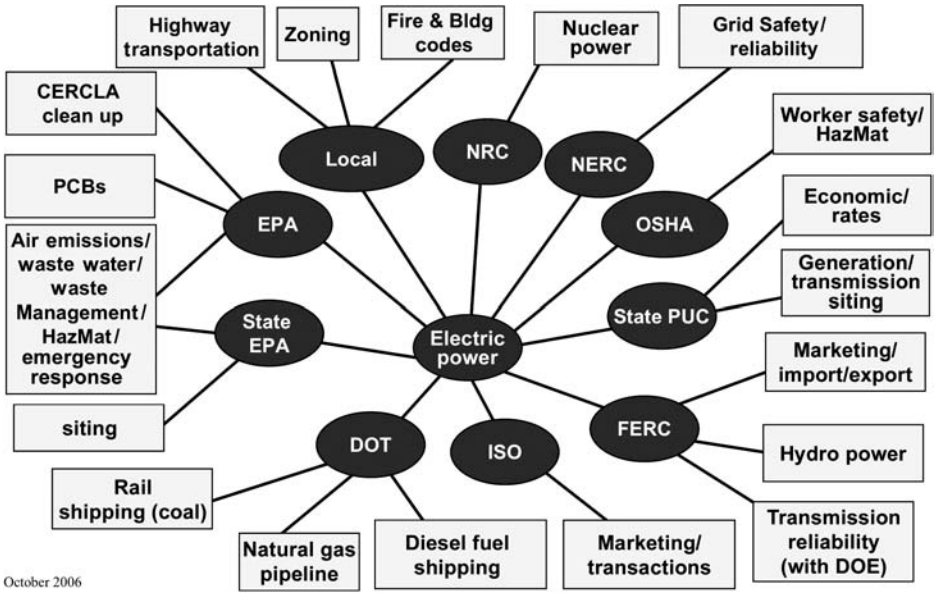



**FIGURE 1** Electric power infrastructure regulatory environment.

upstream of dams may be considered as satisfactory boat restraining barriers. In addition, no-boating zones are often established regardless of physical barriers. These requirements are implemented to protect the public from the hazardous areas and components of hydropower projects, though they also serve to restrict maritime avenues of approach to critical assets at the dam.

However, other nonsecurity-related regulations might adversely impact the security at critical infrastructure facilities/assets. Local health and safety codes frequently require emergency exit stairwell doors remain unlocked, if not all of the time, at least during a fire emergency (e.g. when the fire alarm is activated), allowing access to all floors of the building during evacuation.[14] This, however, also impacts the security of a facility in that, once someone has access to the bottom stairwell door, they have access to the entire facility. Therefore, building security must be adjusted to accommodate the factor that the stairwell doors may not be locked or must be equipped with an electronic mechanism that unlocks all stairwell doors only when the fire alarm is activated.

In another example, Title III of the ADA[10] prohibits discrimination on the basis of disability by public accommodations and requires places of public accommodation and commercial facilities to be designed, constructed, and altered in compliance with the accessibility standards established by this part. The DOJ has promulgated regulations to implement Title III.[15] These regulations require handicapped accessible parking spaces serving a particular building be located on the shortest accessible route of travel from adjacent parking to an accessible entrance and that accessible route cannot have curbs or stairs or other barriers.[16] In addition, passenger loading zones shall provide an access

[14]42 U.S.C. 12181.
[10]28 CFR Part 36.
[15]28 CFR Part 36, Appendix A, Section 4.3 and 4.6.
[16]49 CFR Part 171 and 172.

aisle at least 60 in. (1525 mm) wide and 20 ft (6100 mm) long adjacent and parallel to the vehicle pull-up space and if there are curbs between the access aisle and the vehicle pull-up space, then a curb ramp must be provided. Generally, at public entrances to facilities where there are large gatherings of people (e.g. stadiums, arenas, shopping malls, or convention centers), security policy would require barriers to protect populated main entrances from speeding vehicle-borne improvised explosive devices (VBIEDs). Similarly, security policy would limit parking near public buildings within designated blast effect distances. However, such requirements could impact the accessibility of the facility to those protected under the ADA.

### 5.2 Public Availability of Information Versus Security

Federal DOT regulations require placards to be placed on all shipments of hazardous materials, based on the type and quantity of material in the vehicle/container [9]. There are two placarding hazard classes. One requires placards be displayed to identify any quantity of material in the vehicle/container and the other to identify only when the quantity of material is over 1001 pounds. The first class includes high explosives, poison gas, dangerous when wet material, some organic peroxides, poison inhalation material and certain radioactive materials. The second includes explosives, flammable and non-flammable gases, flammable and combustible liquids, flammable solids, spontaneously combustible materials, oxidizers, some organic peroxides, poisons that do not pose an inhalation hazard, and corrosive materials.

The placards are diamond-shaped signs placed on both ends and both sides of trucks, railcars, and intermodal containers that carry hazardous materials. They are coded by color and contain symbols and numbers that designate the hazard class of the hazardous material that is contained in the vehicle/container. In addition, the placarding requirements are based on the United Nations' (UN) Model Regulation on the Transport of Dangerous Goods, which are widely adopted into national and international regulations.

In addition, these regulations may require other markings such as proper shipping names and material identification numbers, including for shipments of certain bulk commodities and for other shipments of materials that are poisonous by inhalation, marine pollutants, and elevated temperature materials. Under the North American Free Trade Agreement, the United States, Canada, and Mexico have harmonized the hazardous materials placarding requirements of the three countries and jointly published the Emergency Response Guidebook (ERG2004). The Emergency Response Guidebook (ERG2004) is available from the DOT website. It allows anyone to search for a chemical by the material identification number or shipping name with reference to a specific hazard guide. It provides fire or explosive and health hazards, public safety information (e.g. personal protective equipment and evacuation), as well as emergency response for fire, spill/leak, or first aid.

The DOT has recognized that placards, which are important for communicating the presence of hazardous materials, also might aid a terrorist in identifying hazardous materials in transportation. In this case, DOT has studied this interrelationship between the existing federal hazardous materials regulations and transportation security concerns [10]. At this time, DOT has concluded that placards are a critical source of hazard information to emergency response personnel, transport workers, and to regulatory enforcement personnel and play a critical role in the event of a hazardous materials incident. DOT

concluded that there are more appropriate means of enhancing security related to the transportation of hazardous materials rather than entirely replace the placard system.

Having discussed situations where nonsecurity-related regulations may impact security policies or requirements, the following section now discusses some examples where security regulations may unintentionally impact the nonsecurity-related regulations of and requirements at critical infrastructure facilities and assets.

### 5.3 Security Versus Personnel, Health, or Safety

A General Accounting Office (GAO) report found that security directives issued by the Department of Homeland Security Transportation Security Administration (TSA) conflicted with certain safety regulations.[17] After the bombing of passenger rail facilities in Spain, the TSA, on May 20, 2004, issued emergency security directives applicable to the passenger rail industry (effective May 23, 2004). The directives required rail operators to implement a number of security measures, such as conducting frequent inspections of stations, terminals, and other assets, or utilizing canine explosive detection teams, if available. According to TSA officials, because of the need to act quickly, the rule-making process for these security directives did not include a public comment period.

Examples of conflicting provisions include a requirement that the doors of the rail engineer's compartment be locked. However, according to the Federal Railroad Administration (FRA), the provision conflicts with an existing FRA safety regulation calling for these doors to remain unlocked for escape purposes.[18] What follows is as stated by the GAO Report:

> According to FRA, a locked door pursuant to the directive would not allow the locomotive engineer to quickly exit the cab when faced with an impending highway rail grade crossing collision or other accident. In some cases, the door providing access to the locomotive's cab also serves as one of only two primary paths for emergency exit by passengers and is marked as an emergency exit. According to FRA, if these doors are locked pursuant to the directives, they may not be usable in an emergency, and passenger evacuation time could be substantially increased.

Another example raised in the report is the requirement to remove trash receptacles at stations determined by a vulnerability assessment to be at significant risk and only to the extent practical, *except for clear plastic or bomb-resistant containers*. However, the American Public Transportation Association, Association of American Railroads, and some rail operators raised concerns about the feasibility of installing bomb-resistant trash cans in certain rail stations because they could direct the force of a bomb blast upward, possibly causing structural damage in underground or enclosed stations.

### 5.4 Security Versus Privacy

Closed-circuit television (CCTV) systems typically involve a camera or cameras linked to monitors and recording devices. A CCTV system allows the remote cameras to be viewed and operated from a centralized control room. CCTV systems have been installed

[17] 49 CFR 238.235.

[18] Alabama, Arkansas, California, Delaware, Georgia, Hawaii, Kansas, Maine, Michigan, Minnesota, New Hampshire, South Dakota, and Utah.

at many types of infrastructure facilities, including commercial establishments, schools, and places of employment. In addition, more Police departments in the United States now use CCTV to deter and detect crime. Since September 11, 2001, law enforcement has also begun to use CCTV to combat terrorism.

There are currently no specific federal regulations concerning the use of CCTV cameras in public places, such as public streets, parks, and subways, or semipublic, such as schools and workplaces. However, the laws of 13 states [11] expressly prohibit the unauthorized installation or use of cameras in private places without permission of the people photographed or observed.

A private place is defined by the courts as one where a person may reasonably expect to be safe from unauthorized surveillance. The Fourth Amendment protects people from unreasonable searches and seizures. According to the Supreme Court, if the person under surveillance has a reasonable expectation of privacy, the Fourth Amendment applies, and a warrant is generally required to conduct a lawful search. Conversely, if the person under surveillance does not have a reasonable expectation of privacy, the Fourth Amendment does not apply, and no warrant is required for police surveillance [12]. A recent GAO report found that civil liberties advocates have raised issues concerning CCTV's potential impact on individual privacy as well as the potential for inappropriate use of CCTV systems and the mishandling of CCTV images [13]. The Security Industry Association (SIA) and International Association of Chiefs of Police (IACP) and other organizations have developed guidelines for CCTV users that address some of the issues raised by civil liberties advocates through the use of management controls [14]. These include developing written operating protocols, establishing supervision and training requirements, providing for public notification, and requiring periodic audits. These legal issues will continue to be raised as more schools, workplaces, subways, shopping malls, and other areas install and use CCTV to monitor employees and visitors. Fear of criminal prosecution may deter some institutions from installing CCTV for security purposes.

## 6 INTERDEPENDENCY BETWEEN INFRASTRUCTURE REGULATORY SCHEMES

In addition, interdependency of infrastructures adds another layer of overlapping and possibly conflicting regulatory schemes. Interdependency refers to the failure in one asset or infrastructure which can cascade to cause disruption or failure in others, and the combined effect could prompt far-reaching consequences affecting government, the economy, public health and safety, national security, and public confidence [15]. This interdependency impact can affect the performance of other infrastructures under normal and stressed operations, due to disruptions (including coincident events), or during repair and restoration. Interdependencies also change as a function of outage duration, frequency, and other factors. Backup systems or other mitigation mechanisms can reduce interdependency problems. There are also linkages between critical infrastructures and community assets (for response and recovery) (Figure 2).

Interdependency can be

- physical (e.g. material output of one infrastructure used by another),
- cyber (e.g. electronic, informational linkages),
- geographic (e.g. common corridor), and
- logical (e.g. dependency through financial markets).

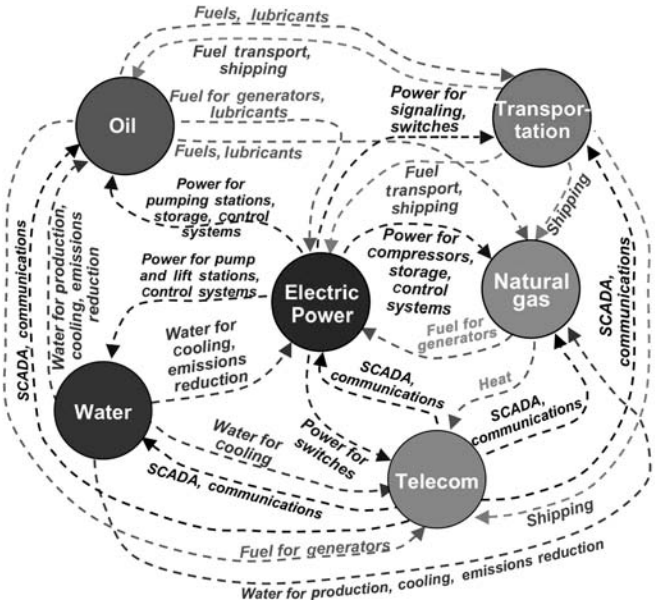



**FIGURE 2** Electric power infrastructure interdependencies.

Interdependency impacts can be caused by the following:

- *Common cause failure.* A disruption of two or more infrastructures at the same time because of a common cause.
- *Cascading failure.* A disruption in one infrastructure causes a disruption in a second infrastructure.
- *Escalating failure.* A disruption in one infrastructure exacerbates a disruption of a second infrastructure.

An example of the impact of regulations on geographic interdependency can be seen in the application of environmental and zoning regulations for siting infrastructure assets. As stated in the Congressional Research Service Report to Congress on Vulnerability of Concentrated Critical Infrastructure the Background and Policy Options are as follows:[19]

> When infrastructure is physically concentrated in a limited geographic area it may be particularly vulnerable to geographic hazards such as natural disasters, epidemics, and certain kinds of terrorist attacks. Whereas a typical geographic disruption is often expected to affect infrastructure in proportion to the size of an affected region, a disruption of concentrated infrastructure could have greatly disproportionate—and national—effects.

Geographic concentrations of national critical infrastructure have developed for multiple reasons—typically some combination of resource proximity, agglomeration economies, scale economies, capital efficiency and federal, state, and local regulations. For instance, state environmental and local zoning or health regulations can limit the siting of industries that use hazardous materials near sensitive areas (e.g. schools)

[19]For example, Massachusetts regulations on Wellhead Protection Zoning and Non-zoning Controls, found at 310 CMR 22.21 (2).

and environmental regulations regulate the operation of facilities handling hazardous materials in groundwater (wellhead) protection zones.[20,21]

Regulatory limitations on the siting of critical infrastructure tend to group infrastructure assets together along roadways and other established corridors or public utility rights-of-way or in specific zoning districts. For example, in many communities, zoning regulations/ordinances allow transmission lines utilizing multiple-legged structures, generating or treatment plants, substations, pumping, or regulator stations to be built only in certain zoning districts. In other cases, utility siting is encouraged only in existing corridors, which forces utilities to share existing corridors.[22] This clustering of infrastructure assets into close proximity can result in escalating failures of these geographically interdependent infrastructures.

An example of cascading failure is the disruption in rail service for coal deliveries to power plants. This would result in determining alternative transportation infrastructure options. However, local road restrictions on load weights could prevent the transportation of coal by truck, particularly given the amount of coal required to replace one coal unit train delivery.[23] Another such example, may be the need to haul heavy replacement transformers by truck rather than the usual specialized rail cars could require a permit or a waiver.

## 7 CONCLUSION

Since September 11, 2001 (9/11), there has been an impetus to evaluate the vulnerabilities of the nation's critical infrastructures and to implement programs to reduce or mitigate those vulnerabilities. Over the last five years, a flurry of legislation, regulatory rule making, policy directives, and federal agency guidance documents have created security-related requirements applicable to some critical infrastructure facilities. Therefore, at this time, vulnerability mitigation activities can take the form of strict governmental security regulation, governmental information-gathering-and-assistance programs aimed at the private sector, governmental policies, and programs for implementation at governmental facilities, industry association developed and implemented security programs (both voluntary and mandatory) for their members (e.g. North American Electric Reliability Council and American Chemical Council), and, finally, security planning, policies, and technology installations by private businesses using in-house personnel and outside security consultants. However, there are also many nonsecurity-related regulations that are promulgated every month that could also impact the security of critical infrastructure assets or impede mitigation or emergency response. These proposed regulations are not reviewed in light of the security laws, regulations, and policies being enacted at the federal level.

[20]For example, Wellesley, Massachusetts Zoning Bylaws Section XIVE, Water Supply Protection Districts.

[21]See, Aberdeen, Maryland Zoning Regulations, Appendix A—Table of Use Regulations or Alameda, California, Chapter XXX—Development Regulations, Article I—Zoning and District Regulations, Section 30-4—District Uses and Regulations. Both regulations limit the construction of transmission lines, generating plants, substations and other infrastructure facilities without approval in some districts.

[22]For example, City of Redmond, Washington, Comprehensive Plan, Utilities Chapter.

[23]The usual unit train has about 100 cars, each holding about 100 tons of coal. The maximum weight for interstate highway trucks is 80,000 pounds gross weight (tractor/tare weight/cargo weight) (29 CFR 658.17). It may be lower on non-interstate (state or country) roads. However, in general, for 40' equipment this would equal a cargo weight of 45,000 depending on tractor weight. Thus, it would take approximately 450 legal interstate truck shipments to make up for one unit train delivery.

Section 603(b) of the Regulatory Flexibility Act of 1980 (5 U.S.C. 601 et seq.) specifies that the contents of the Regulatory Flexibility Analysis (RFA) include the following five requirements:

- description of the reasons why action by the agency is being considered;
- statement of the objectives of, and legal basis for, the final rule;
- description of and, where feasible, an estimate of the number of small entities to which the final rule will apply;
- description of the projected reporting, recordkeeping and other (Page 39, 362) compliance requirements of the rule, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record; and
- identification, to the extent practicable, of all relevant Federal rules that may duplicate, overlap, or conflict with the final rule.

Therefore, under the Regulatory Flexibility Act, all proposed federal regulations should be reviewed for conflict with or impact to the security of critical infrastructure facilities and assets. It should be recognized by those conducting the RFA that any regulation could impact not only the security, including physical, cyber, and sensitive information, of critical infrastructures and assets. In fact, it may have an impact on an infrastructure other than the one for which the proposed regulations was intended to regulate.

In addition, proposed state and local regulations, as well as federal policy and guidance documents from a wide variety of federal regulatory agencies, could also impact the security of critical infrastructure facilities and assets. However, there is no requirement for these to be analyzed against existing security regulations or existing knowledge of vulnerability reduction and mitigation programs.

This chapter only presents a few examples of regulations that could impact the security of critical infrastructure assets. A review of existing regulations could also be prudent to determine if there are regulations that could be unintentionally increasing critical infrastructure vulnerabilities or impeding mitigation or emergency planning.

In addition, nonsecurity-related regulations should be reviewed and their impact should be determined before developing infrastructure security/vulnerability assessment methodologies, recommending protective measures, and/or undertaking research and development activities.

## REFERENCES

1. (a) *FEC vs. Democratic Senatorial Campaign Comm.*, 454 U.S. 27 (1981); (b) *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 275 (1974); (c) Udall v. Tallman, 380 U.S. 1, 16 (1965); (c) *SEC v. Sloan*, 436 U.S. 103, 118 (1978); (d) *FMC v. Seatrain Lines, Inc.*, 411 U.S. 726, 745–746 (1973); (e) *Volkswagenwerk v. FMC*, 390 U.S. 261, 272 (1968); (f) *NLRB v. Brown*, 380 U.S. 278, 291 (1965).
2. 42 United States Code (U.S.C.) Section 7401 et seq. (1990).
3. National Technology Transfer and Advancement Act of 1995, Pub. L. No. 104-113, 110 Stat. 775 (codified as amended in scattered sections of 15 U.S.C.).
4. *Hillsborough County, Florida v. Automated Med. Lab., Inc.*, 471 U.S. 707, 719 (1985).
5. Australian Constitution, Chapter I, Part V, http://www.aph.gov.au/senate/general/constitution.
6. For example, Chicago Zoning Ordinance, Chapter 17 available at http://webapps.cityofchicago.org/zoning/default.jsp, 2007.

7. Congressional Budget Office (2004). *Homeland Security and the Private Sector*, December 2004, Section 3 of 7, available at www.cbo.gov.
8. Lewis, T. G., Darken, R. (2005). *Homeland Security Affairs*, Volume I, Issue 2, Article 1.
9. U.S. Department of Transportation Research and Special Programs Administration Office of Hazardous Materials Safety (2003). *The Role of Hazardous Material Placards In Transportation Safety and Security*, John A. Volpe National Transportation Systems Center, January 15, 2003. Available at: http://hazmat.dot.gov/riskmgmt/hmt/0803RedactedPlacardingReportSSI.pdf
10. General Accounting Office (2005). *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*. Report number GAO-05-851, October 7, 2005.
11. *Katz v. United States*, 389 U.S. 347, 360–61 (1967). (Harlan, J., concurring).
12. General Accounting Office (2003). *Information on Law Enforcement's Use of Closed-Circuit Television to Monitor Selected Federal Property in Washington, D.C.*. Report number GAO-03-748, June 2003.
13. Closed Circuit Television (CCTV) (2000). *GUIDELINE: Closed Circuit Television (CCTV) for Public Safety and Community Policing, issued by Security Industry Association (SIA) and International Association of Chiefs of Police (IACP)*, Final Revision Number 9, January 1, 2000.
14. *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, February 2003.
15. Parfomak, P. W., Congressional Research Service (CRS) Report for Congress (2005). *Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options*, Order Code RL33206, December 21, 2005.

# CHARACTERIZING INFRASTRUCTURE FAILURE INTERDEPENDENCIES TO INFORM SYSTEMIC RISK

TIMOTHY MCDANIELS AND STEPHANIE CHANG
*University of British Columbia, Vancouver, BC, Canada*
DOROTHY A. REED
*University of Washington, Seattle, Washington*

## 1 SCIENTIFIC OVERVIEW

Critical infrastructure systems, sometimes referred to as lifelines, provide vital services for societal functions. Until recently, planning and management for provision of these

services has focused on individual infrastructure systems. Yet, analysts, planners, and decision makers increasingly recognize that these systems are highly interconnected and mutually interdependent in a number of ways [1, 2]. For example, the US government established the National Infrastructure Simulation and Analysis Center to examine infrastructure interdependencies through modeling and simulation [3].

Infrastructure systems have become more congested and thus increasingly vulnerable to failures due to interactions within and between systems. The electrical power delivery system is a prime example. It has increased risk of large-scale failures, due to increasing demands on the system that have not been met by a corresponding increase in capacity [4]. Major power outages, affecting 1 million or more people, occur about every 4 months on an average in the United States [3]. This research examines infrastructure interdependencies by focusing on major outages in the electrical system and the effects these outages have on other infrastructures. Extreme events, as defined by the National Science Foundation, are typified by nonlinear responses, low probabilities, high consequences, and the potential for systems interaction that leads to catastrophic losses [5].

Models of outage impacts in which the power delivery system is treated as an individual civil infrastructure system are common. Recently, new conceptual models and simulation approaches have been developed as a means of representing complex, interconnected systems. Examples include the infrastructure risk analysis model [6], hierarchical holographic modeling [7], and agent-based simulation [8]. Additionally, models that integrate civil engineering, electrical engineering, and social science dimensions of infrastructure failures are becoming more common [4, 9, 10].

We employ an empirical approach to understand infrastructure interdependencies, which we refer to as *infrastructure failure interdependencies* (IFI). We define IFIs as failures in interdependent infrastructure systems, which are due to an initial infrastructure failure stemming from an extreme event. When major power outages affect other infrastructures, the interdependencies among the systems prolong and greatly exacerbate the consequences of the initial outage. Planning to address extreme events should take into account these interdependencies because they are the pathways through which indirect impacts of a major outage ripple through societal interactions and economic activity. As framed at present, ours is not a predictive model but rather an *ex post* risk analysis approach derived from observation of actual events. This model can be used to help clarify IFI patterns. Such information is important for setting priorities about potential ways to mitigate the likelihood and the consequences of these infrastructure interactions.

The next section outlines relevant concepts and presents a framework for characterizing the nature, extent, and severity of IFIs. This framework is applied in Section 3 to IFIs occurring in two extreme outage events, the August 2003 blackout and the 1998 ice storm, both of which affected northeastern North America. Section 4 discusses the implications of this analysis and a conclusion is reached in Section 5.

## 2 CONCEPTS AND FRAMEWORK

### 2.1 Partitioning Patterns and Consequences

Haimes and his colleagues have addressed fundamental aspects of the analysis of extreme events and interdependent systems. Their approach recognizes the pitfalls of simple

expected value calculations as a means of characterizing the implications of extreme events within an overall distribution for a given random variable [11]. Their work on the *conditional* expected value (e.g. conditional on exceeding some threshold value) (e.g. [12, 13]) helps focus the attention of decision makers and analysts on the tails of a probability distribution.

This work is similar in spirit to the approach of Haimes and his colleagues, by partitioning both patterns of occurrence and consequences, but with a different emphasis. Here we deal with a *vector* of events, which are all the potential IFIs (defined above) that could arise, given an extreme event occurrence within a given system of infrastructure systems. This approach partitions a vector defining all specific kinds of IFIs, by considering their patterns of occurrence, given that an extreme event to trigger IFIs has occurred. It also partitions consequences, by considering the consequences of a vector containing each specific kind of IFI, separate from the direct consequences of the initial extreme event. In this respect, the approach here also partitions the patterns and consequences in time. It is an approach that is effectively *ex post*, conditional on the occurrence of an extreme event.

### 2.2 A Matrix of Infrastructure Failure Relationships

Haimes and Jiang [14] developed a Leontief-based model of risk in interconnected infrastructure systems. Their risk measure is cast as the *risk of inoperability* of a given infrastructure system, which is the product of the probability and degree (percentage) of inoperability for that system. They provide a model definition, drawing on what is termed the $\boldsymbol{A}$ matrix in input–output analysis, cast in terms of inoperability or failure relationships among infrastructure systems, rather than economic interdependencies as the Leontief work. In this article, we proceed in the spirit of the Haimes and Jiang framework, with somewhat different terminology, notation, and emphasis.

We adopt the following definitions: $\mathbf{X}$ is defined as an overall system of interdependent, nonredundant infrastructure systems $X_i$, where $i = 1, 2, 3 \ldots, n$. $\mathbf{X}$ could be defined for spatial or physical units ranging from a building to a neighborhood, city, region, nation, or even a continent, depending on the scale of interest. Systems $X_i$ and $X_j$ within $\mathbf{X}$ have an interdependent relationship defined as $\mathrm{A}_{ij}$, which characterizes the extent to which a failure of operability in $X_i$ could lead to operability failures in $X_j$. An operability failure $C$ could render the system $X_i$ completely or partially inoperable, as in Haimes and Jiang [14]. An $\mathrm{IFI}_{ij}$ is a specific failure event $C\ (X_i)$ within a specific infrastructure system $X_i$, given a specific failure of a different infrastructure system $C(X_j)$ where both $X_i$ and $X_j$ are within $\mathbf{X}$. The matrix $\mathbf{C}$ contains all the specific IFI events $C(X_i)$ that could arise within a defined system of infrastructure systems $\mathbf{X}$, given that the initial extreme event triggers opportunities for the $\mathrm{IFI}_{ij}$ events in $\mathbf{C}$. The dimensions of $\mathbf{C}$ include the specific system that fails and the degree of impairment of the functions of the system.

### 2.3 Event Patterns as Ex Post Risk Analysis

Risk is sometimes defined as a triplet of conditions: what could go wrong, how likely it is to go wrong, and the consequences if it does go wrong [15, 16]. Here we add an additional initiating event $C(X_j)$, which has already gone wrong, as the conditional basis for examining this triplet approach to define risk of IFI. We use patterns of events to explore the nature of $C(X_j)|C(X_j)$. Characterizing probabilities in terms

of $P(C(X_i)|C(X_j))$ would require data from (i) databases to characterize the relative frequency of $P(C(X_i)|C(X_j)$; (ii) expert judgments informed by these databases; or (iii) simulation efforts again informed by such databases. Yet, to our knowledge, the efforts discussed here are among the first to empirically examine such interactions. Hence, we provide an early step toward characterizing such probabilities in future studies by exploring the patterns of these $\mathrm{IFI}_{ij}$ events in specific contexts and their broad social consequences. In effect, we use these patterns as a basis for characterizing event patterns to help inform planning. This approach characterizes IFIs in terms of an *ex post* version of systematic risk analysis.

### 2.4 A Framework for Characterizing IFIs

We discuss this framework in terms of infrastructure systems $X_i$ that could be affected due to interrelationships $\mathrm{A}_{ij}$, given that a large scale failure $C(X_e)$ in the electrical system $X_{(e)}$ has occurred. This electrical system failure could be the result of an extreme event involving equipment failure within the electrical system, as in the case of the August 2003 blackout that affected northeastern North America. It could also be the effect of an extreme event outside the electrical system such as the ice storm in Quebec in 1998. The framework will be applied to these outages in the next section.

The basis for this framework is the observation that an IFI arising from an outage leads to certain societal consequences. The framework is thus divided into three sections characterizing the outage itself, the IFIs resulting from the outage, and the consequences of those IFIs as shown in Table 1. The outage is characterized by date, a description of the event, whether the initiating event was internal or external (to the electrical system), the spatial extent and duration of the event, and the weather conditions and temperature at the time of the event. This information remains constant for any one event. For example, the Northeast blackout is characterized as beginning on August 14, 2003, initiated by an event internal to the power system. Because it affected both the United States and Canada, the spatial extent is considered to be international. The blackout lasted for days in some areas and the weather conditions were moderate, though the temperature was hot. In contrast, the 1998 ice storm occurred in winter with extreme weather conditions causing the blackout. The initiating event in this case is deemed to be external to the power system; in some locales, the system was out for weeks (Also, a storm is a "continuous" event that lasts a minimum of hours, possibly days, or weeks.).

The second part of our framework characterizes the infrastructure failure interactions. The values associated with this part of the framework, many of which are drawn from key concepts in the work of Peerenboom et al. [17], Nojima and Kameda [18], and Yao et al. [19], are shown in Table 2. The four interdependency characteristics—physical, cyber, geographic, and logical—are discussed by Peerenboom et al. [17]. Human actions play a particular role in interdependencies categorized as logical. The IFI types *cascading* and *escalating* also come from their work, as well as the characteristics' *complexity*, *operational state*, and *adaptive potential*. The research of Nojima and Kameda in lifeline interactions in the Kobe earthquake yields the IFI types, *compound damage propagation* and *restoration*. Yao et al. [19] use multiple earthquakes to develop their classification of lifeline interactions, containing all of the categories used by the other two groups, but with different names. In addition, they include a category called *substitute interaction* or *substitutive* in our framework.

Rinaldi et al. [9] distinguish between dependency and interdependency, where dependency is a unidirectional relationship and interdependency is a bidirectional relationship

**TABLE 1 Infrastructure Failure Interdependencies**

| Characteristic | Values | Explanation |
|---|---|---|
| Impacted system | Building support, business, education, emergency services, finance, food supply, government, healthcare, telecommunications, transportation, utilities | The infrastructure systems |
| Specific system | *Various* | A subdivision of the impacted system |
| Description | *Various* | A brief summary of the impact on the system |
| Types of interdependency | Physical | The system requires electricity to operate |
| | Geographic | The system is colocated with electrical infrastructure |
| | Cyber | The system is linked to the electrical system electronically or through information sharing |
| | Logical | The system depends on the electrical system in a way that is not physical, cyber, or geographic |
| Types of IFI | Cascading | The disruption of the power system directly causes the disruption in the impacted system |
| | Escalating | The disruption of the power system exacerbates an already-existing disruption in the impacted system, increasing the severity or outage time |
| | Restoration | The power outage hampers the restoration of the impacted system |
| | Compound damage propagation | The power system disruption leads to a disruption that then causes serious damage in the impacted system |
| | Substitutive | A system is disrupted due to demands placed on it to substitute for the power system |
| Order | Direct | The IFI is a direct result of the power outage |
| | Second order | The power outage is once removed as the cause of the system disruption |
| | Higher order | The power outage is twice or more removed as the cause of the system disruption |
| System failure leading to this effect | See impacted systems' list | Electrical in the case of direct order events; the system that caused the disruption in the impacted system for second- and higher order events |
| Complexity | Linear | Expected and familiar interactions, often intended by design |

**TABLE 1 (*Continued*)**

| Characteristic | Values | Explanation |
|---|---|---|
| | Complex | Unplanned or unexpected sequences of events |
| Feedback | Yes | The impacted system affects the power system |
| | No | The impacted system does not affect the power system |
| Operational state | At capacity | The impacted system was operating at 100% when the power outage occurred |
| | Near capacity | The impacted system was operating above 90% when the power outage occurred |
| | Below capacity | The impacted system was operating at 90% or below when the power outage occurred |
| Adaptive potential | High | The system has ways to respond quickly in a crisis |
| | Low | An inflexible system that cannot quickly respond |
| Restart time | Minutes, hours, days, weeks | The amount of time required for the impacted system to return to preoutage operating capacity once electric power has been restored |

between systems. We make no such distinction in our framework, except for the inclusion of a feedback characteristic that indicates whether a particular IFI has a return effect on the power system.

The division into direct, second, and higher order effects is important due to the complex interactions that can occur between systems. Often the direct impacts of a power outage can be anticipated, such as electrical machinery and appliances not working. Failure to understand the higher order impacts leaves decision makers unprepared to effectively deal with these disruptions [1]. The final five characteristics in the framework as shown in Table 1, explained in Table 2, relate to the consequences of the IFI. These characteristics are most important for designing mitigation strategies, as will be shown in the analysis and comparison in Section 3 of two major outage events.

## 3 APPLICATIONS OF THE IFI FRAMEWORK

### 3.1 Database and Applications

This section discusses two applications of the framework described above. The intent is to explore how the patterns of $C(X_i)$ arise in real events, within a defined $\mathbf{X}$ for each event, where the triggering event $C(X_e)$ is a major electrical outage $X_{(e)}$ stemming from either an extreme event within or external to the electrical system. In order to characterize IFIs from various power outages, we constructed a database employing the characteristics

**TABLE 2 Consequence Characteristics**

| Characteristic | Value | Explanation |
|---|---|---|
| Severity | Minor | Minor modifications in daily routine or plans that cause negligible hardship to the person or entity |
| | Moderate | A few modifications in daily routine or plans that cause some hardship to the person or entity |
| | Major | Significant modifications in daily routine or plans that cause considerable hardship to the person or entity |
| Type | Economic, health, safety, social, environmental | Primary category under which the consequence falls |
| Spatial extent | Local | One city or area affected |
| | Regional | More than one city or area within a province or state affected |
| | National | More than one state or province affected |
| | International | More than one country affected |
| Number of people | Few | In the spatial extent of the consequence, one neighborhood or isolated individuals were affected |
| | Many | In the spatial extent of the consequence, up to 50% of the population was affected |
| | Most | In the spatial extent of the consequence, at least 50% of the population was affected |
| Duration | Minutes, hours, days, weeks | The amount of time the consequence endures, which may be greater than the restart time |

and values in the conceptual framework. Each record in the database consists of an observed IFI, from a societal standpoint, reported in major media or in technical reports. The database contains hundreds of IFIs from a number of recent outages, including the August 2003 Northeast blackout and the 1998 Quebec ice storm. Searches were conducted on the Nexus–Lexus database and other search engines to identify information and published sources related to the events. The data sources include major newspapers, such as the *Montreal Gazette*, *Ottawa Citizen*, *New York Times*, and *Toronto Star* and technical reports regarding these events (e.g. [20]).

Figures 1 and 2 illustrate the kinds of interactions and consequences in the database. The first figure characterizes the consequences of the 2003 Northeast blackout while the second portrays consequences that occurred during the 1998 ice storm. These diagrams show that we divide impacts by the infrastructure affected (e.g. transportation) and the specific subsystems (e.g. mass transit). Each also includes a table with a coding system to generally indicate the severity and extent of impacts.

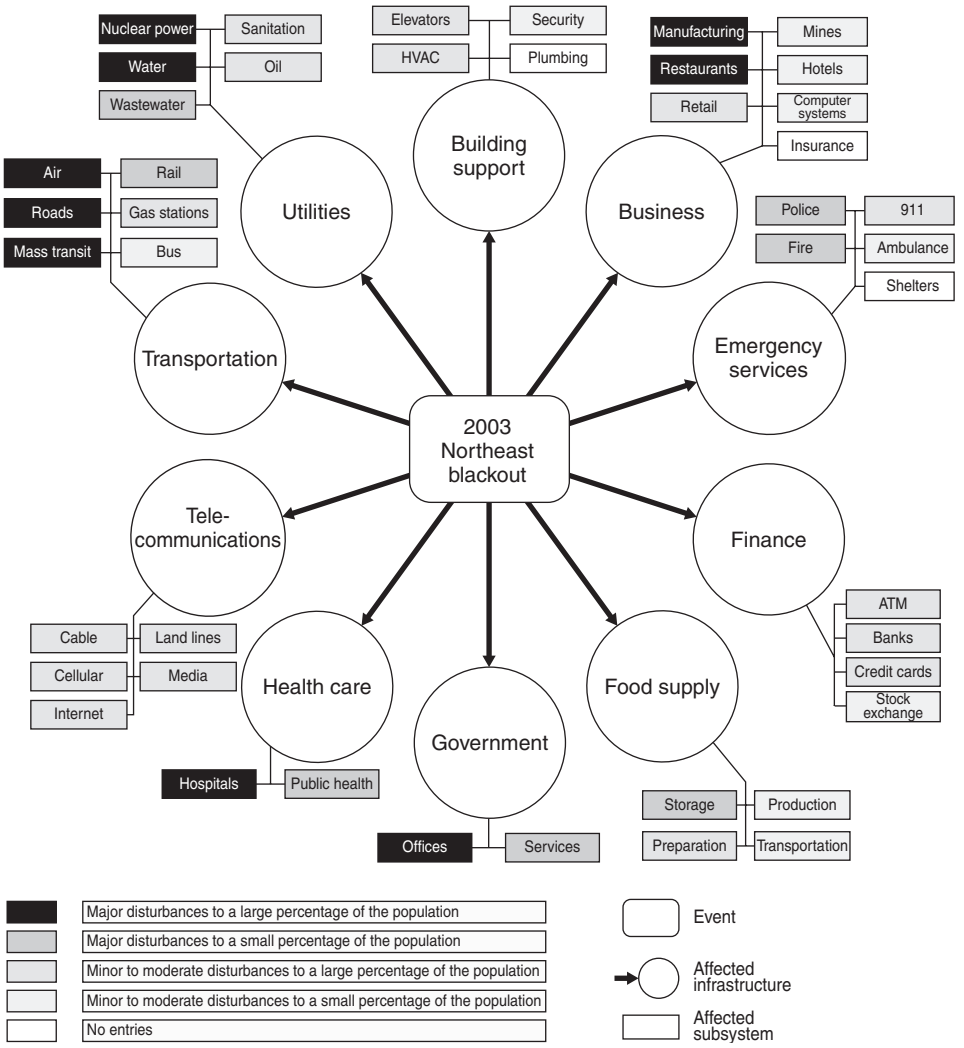



**FIGURE 1** Infrastructure failure interdependencies and their consequences for the 2003 Northeast blackout.

For analysis, we developed indices of consequences using the weights shown in Table 3. The weights were assigned in terms of subjective three-point scales (e.g. 1–3), and were treated as cardinal numbers to serve as a basis for differentiating the IFIs. The impact value (ranging from 1 to 9) is the product of the IFIs duration and severity weights. For example, a moderately severe IFI (weight = 2) that lasted for weeks (weight = 3) would have an impact value of 6. The midpoint for the scale is 5; hence values above that indicate more severe consequences with longer duration than those less than 5. The extent value (ranging from 1 to 9) is the product of the IFIs spatial extent and number of people affected. An IFI that affects only a few people (weight = 1) regionally (weight = 2) would have an extent value of 2. Values of extent greater than 5 indicate that large numbers of people were affected over an extensive geographic area. It is also

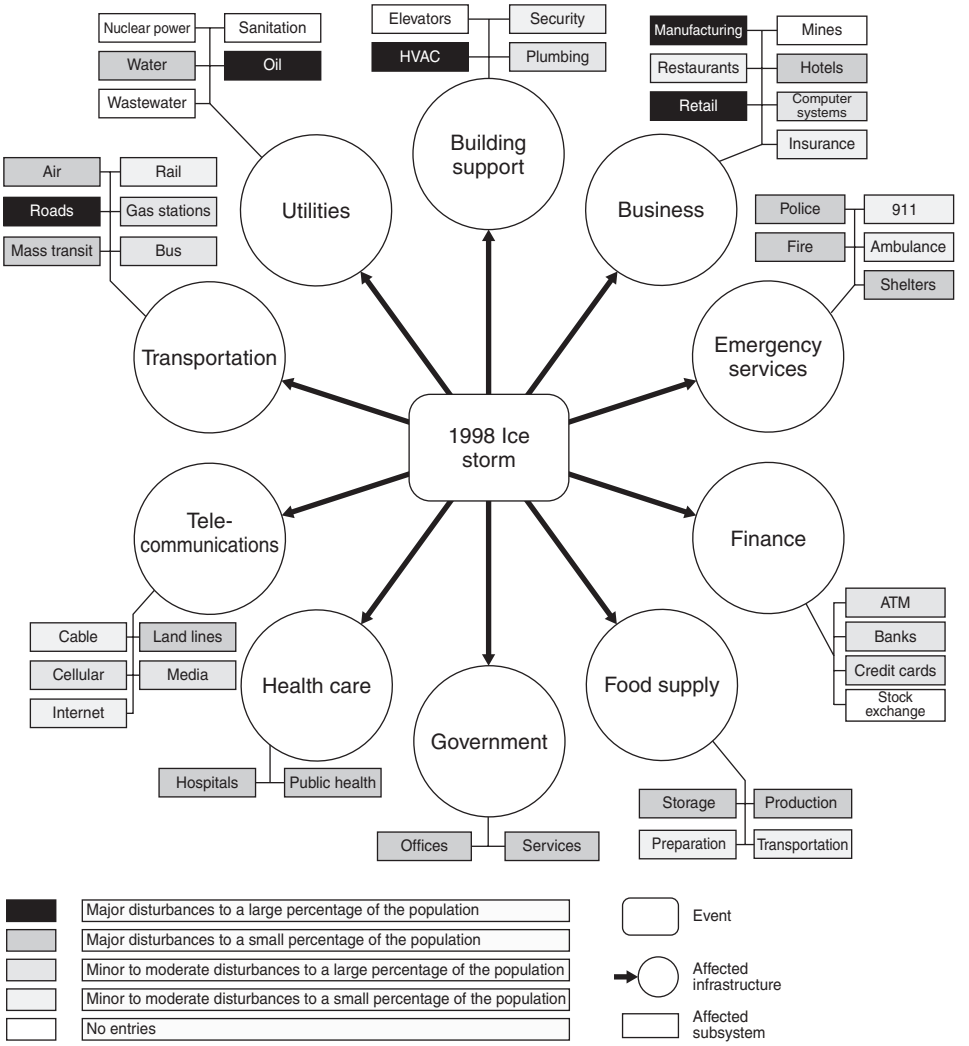



**FIGURE 2** Infrastructure failure interdependencies and their consequences for the 1998 ice storm blackout.

important to note that the impact and extent indices can only take on certain discrete values (i.e. 1, 2, 3, 4, 6 . . . , 9).

### 3.2 August 2003 Blackout

On August 14, 2003, the largest blackout in North American history occurred, with over 50 million people in Ontario, Canada, and parts of the Northeast and Midwest United States affected by the power outage. Our initial examination of this event has focused on the four major cities most affected by the blackout: New York City, Detroit, Cleveland, and Toronto. Figure 1 characterizes the 2003 Northeast blackout in terms of first and second order failure interdependencies and degree of disruption.

**TABLE 3 Weights for Consequence Indices**

| Weights | Duration | Severity | Spatial Extent | Number of People |
|---|---|---|---|---|
| **3** | Weeks | Major | International, national | Most |
| **2** | Days | Moderate | Regional | Many |
| **1** | Hours, minutes | Minor | Local | Few |

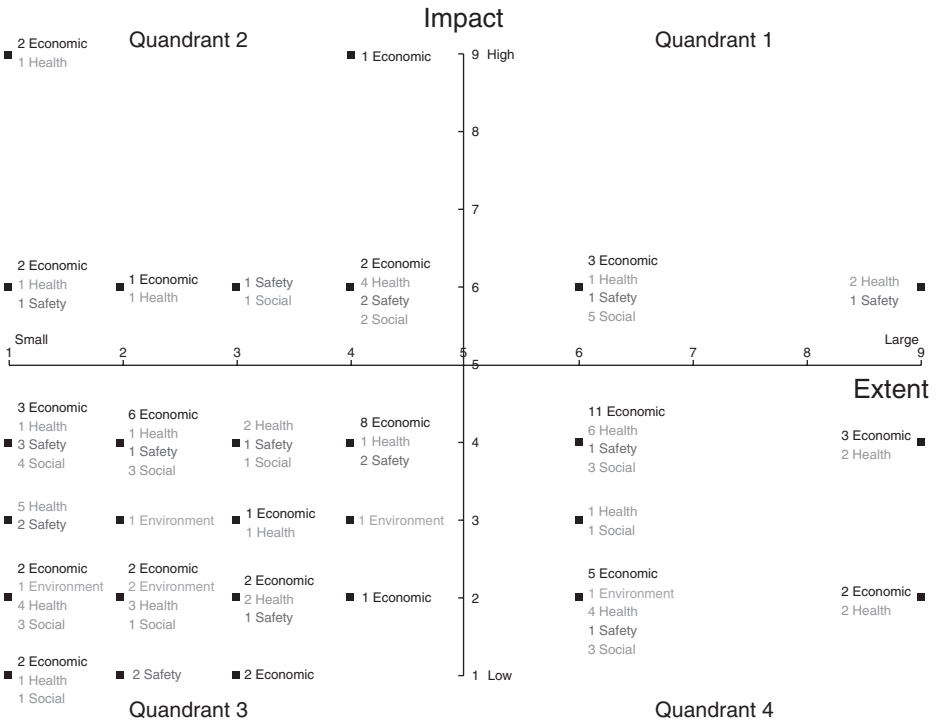



**FIGURE 3** Consequence indices for infrastructure failure interdependencies and their consequences for the 2003 Northeast blackout.

Figure 3 provides a compact summary of information in Figure 1, but disaggregated in terms of the nature of the consequences of the IFI. The colors indicate the types of consequences and the number indicates how many times that particular consequence was reported.

Figure 3 also separates the IFIs into four quadrants or categories. Axes separating the quadrants are located at the respective midpoint values of the potential range of impact and extent values (i.e. 5 on a scale of 1–9). Quadrant 1 represents major disturbances to a majority of the population, while Quadrant 2 includes major disturbances to a small percentage of the population. Quadrant 3 indicates minor inconveniences to a small percentage of the population. Quadrant 4 represents IFIs that caused minor inconveniences to a large percentage of the population. From a societal point of view, IFIs in Quadrant 1 are of greatest concern. This quadrant includes IFIs that have both high impact and broad extent of impact.

Out of the 162 IFIs in the database for the Northeast blackout, 13 are in Quadrant 1, which contain IFIs of large extent and high impact. In the far right of this quadrant are the three most serious IFIs. The two consequences to health are (i) water delivery systems malfunctioning or failing in some areas and (ii) the resulting boil water advisories that were issued. Compliance with the advisories was especially difficult for those who had electric stoves. Safety problems were created by numerous traffic signals being inoperable, resulting in traffic jams and collisions.

A joint US—Canadian task force traced the origin of the 2003 outage to northern Ohio, where a series of electrical, human, and computer incidents led to cascading failures in the North American electrical grid [21]. The next event analyzed was not caused by human and mechanical errors, but by a natural hazard.

### 3.3 Ice Storm

In January 1998, parts of Ontario, Quebec, and New Brunswick and the northeastern United States experienced one of the worst ice storms in recent history. The storm started on January 4 and continued for 6 days. In Canada, the weight of the ice caused 1000 transmission towers and 30,000 distribution poles to collapse [22], and at the peak of the outage, close to 1.4 million people in Quebec and 230,000 in Ontario were without power. Some people in rural areas went without power for more than 30 days. The ice storm consequences are summarized in Figure 4.

The ice storm database contains 102 IFIs, two of which are of large extent and high consequence in Quadrant 1. The two most serious IFIs in the ice storm were major employers shutting down for up to 2 weeks and communication problems for emergency services. In entering IFIs into the ice storm database, it was sometimes difficult to distinguish between problems caused by the storm itself and problems caused by the power outage. This is one of the differences between analyzing internally and externally initiated events. The next subsection has further comparison of the two events.

### 3.4 Comparative Analysis

In both these events, less than one percent of the total IFIs captured in the database are found in Quadrant 1; the majority of IFIs are contained in Quadrant 3. These are all minor disturbances that probably do not require mitigation attention but could become more serious in outages of longer duration. Reporting is also less likely to be complete with minor disturbances. In the financial system, for example, many bank branches were closed and bank machines did not work because of the outages. While this is an inconvenience if it lasts only for a short period of time, it could become a major disturbance in an outage of longer duration. Also, blood supplies dwindled in both events and could become a serious public health issue over a longer outage period.

Figure 5 shows the distribution of types of consequences for the two events. In the ice storm, there are more health consequences than any other type, while a higher percentage of consequences in the Northeast blackout are economic. The season and the longer duration of the ice storm outage are two possible explanations for this difference. IFIs associated with the ice storm outage had no environmental consequences, and the Northeast blackout very few, none of which are rated high on the impact index. The consequence characteristics, as explained in Table 3, are related to the direct, immediate effect the IFI has on people, instead of long-term effects that could result from environmental degradation.

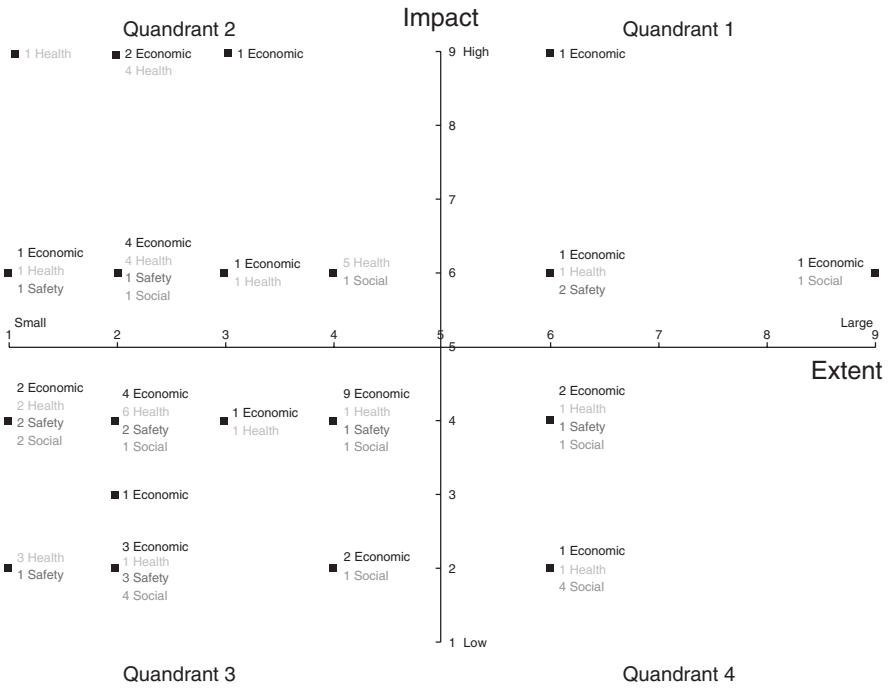



**FIGURE 4** Consequence indices for infrastructure failure interdependencies and their consequences for the 1998 ice storm.

Figure 6 compares the infrastructure systems disrupted by IFIs in Quadrants 1, 2, and 4 and shows notable differences between the two events. In the ice storm event, from the standpoint of societal impacts, emergency services and building support were the systems most affected by the blackout. Building support includes plumbing, heating, ventilation, and elevators, among other functions. The Northeast blackout had significantly more IFIs in the transportation system than did the ice storm event, which may be a result of the internal nature of the outage event. In an external event like the ice storm, weather causes initial problems in the transportation system that are only minimally exacerbated by the outage. Further analysis of these and other extreme events will help determine which systems are more likely to be affected by outages internal to the electrical system and those affected more by external events, such as storms and earthquakes.

## 4 DISCUSSION

We noted earlier that risk analysis often begins by asking what can go wrong, how it can go wrong, and what the consequences are. The analysis of the 2003 Northeast blackout and the 1998 ice storm is the first step in answering those questions, more specifically framed as follows.

What consequences matter most when examining the potential for failures in interconnected infrastructure systems? What consequences matter most for decisions about managing these failures?

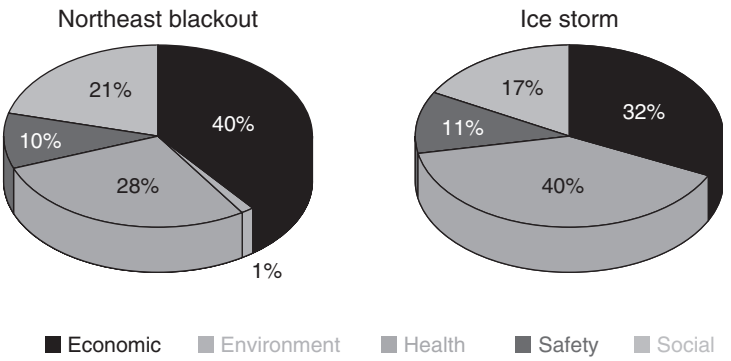



**FIGURE 5** Consequence indices for infrastructure failure interdependencies in Quadrants 1, 2, and 4 by type.

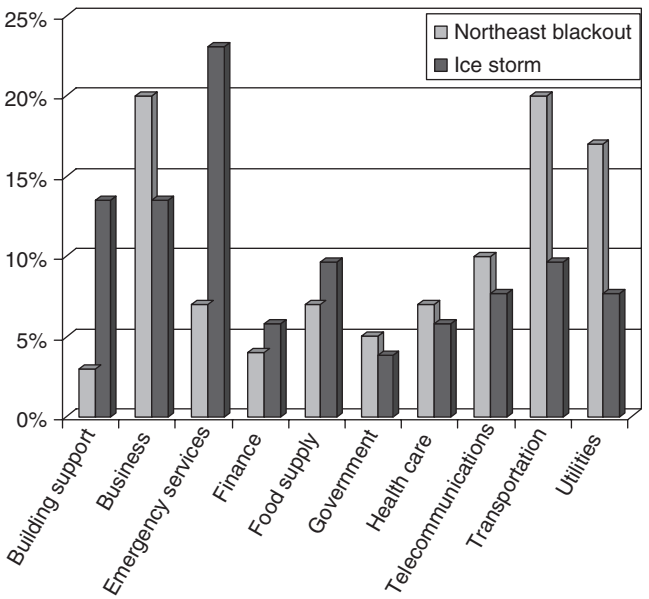



**FIGURE 6** Disruptions of infrastructure failure interdependencies in Quadrants 1, 2, and 4 by affected system.

How can one judge the severity of the consequences of IFIs?

What patterns of IFIs are the most significant sources of concern?

In order to answer Question 2, we developed the consequence indices, which took into account the severity, duration, spatial extent, and number of people affected by an IFI. These calculations were matched with the type of consequence and are shown in Figures 2 and 3 to answer Question 1. For Question 3, the comparative analysis of the two events in Section 3.3 is the initial step toward identifying patterns. Moreover, applications in two very different outage events—a summer short duration event originating in the electric power transmission system versus a winter long duration natural disaster

affecting primarily the power distribution system—provide many useful insights. While our particular focus here is on electric power failures, the framework could be generalized to any source of IFIs.

## 5 FUTURE RESEARCH

The analysis conducted thus far suggests several areas for further research. For example, duration of outage is a key difference that should be further explored. We have found that IFIs are expected to exhibit nonlinear and threshold effects in relation to power outage duration. Preliminary analysis also indicates that impacts on transportation tend to be severe and widespread across different types of outage events. The transportation system is therefore an important system to target for mitigation purposes. Further data collection and analysis across a broader range of disasters and disaster-affected communities will help develop more robust findings. Lastly, our analysis does not incorporate weights or value judgments across types of IFI impacts. Developing frameworks for addressing differences in types of consequences will be important in future research studies.

Some of the results produced by this study may also be of use to other similar research projects. For example, the empirical approach we adopted can be used to provide a complimentary approach (based on IFIs that have actually occurred) to probabilistic, system-based, and simulation models for power outages and their impacts. A robust empirical basis that incorporates experiences across a range of event and community types is also needed. Commonalties and differences in IFIs that occur across types of natural, technological, and willful disasters should also be explored. For example, identifying IFIs that occur in many types of events would be promising targets of mitigation from a multihazard perspective. Further, while this study focuses on IFIs deriving from electric power failure, the framework can be readily extended to assess other types of infrastructure interdependencies and for setting priorities about potential ways to mitigate the likelihood and the consequences of their interdependent failures.

## REFERENCES

1. Peerenboom, J. P., Fisher, R. E., Rinaldi, S. M., and Kelly, T. K. (2002). Studying the chain reaction. *Electric Perspect.* **27**(1), 22–35.
2. Robert, B., Senay, M.-H., Plamondon, M. È. P., and Sabourin, J. P. (2003). *Characterization and Ranking of Links Connecting Life Support Networks*, Public Safety and Emergency Preparedness Canada, Ontario.
3. Lave, L. B., Apt, J., Farrell, A., and Morgan, M. G. (2005). Increasing the security and reliability of the USA electricity system. In *The Economic Impacts of Terrorist Attacks*, H. W. Richardson, P. Gordon, J. E. MooreII, Eds. Edward Elgar Publishing, Inc., Cheltenham, pp. 57–70.
4. Amin, M. (2004). *North American Electricity Infrastructure: System Security, Quality, Reliability, Availability, and Efficiency Challenges and their Societal Impacts*, National Science Foundation, Arlington, VA.
5. Stewart, T. R., and Bostrom, A. (2002). *Workshop Report: Extreme Event Decision Making*, Arlington, VA.
6. Ezell, B. C., Farr, J. V., and Wiese, I. (2000). Infrastructure risk analysis model. *J. Infrastruct. Syst.* **6**(3), 114–117.

7. Haimes, Y. Y., and Horowitz, B. M. (2004). Modeling interdependent infrastructures for sustainable counterterrorism. *J. Infrastruct. Syst.* **10**(2), 33–42.
8. Thomas, W. H., North, M. J., Macal, C. M., and Peerenboom, J. P. (2002). *From Physics to Finances: Complex Adaptive Systems Representation of Infrastructure Interdependencies*, Naval Surface Warfare Center, Dahlgren Division Technical Digest.
9. Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Critical infrastructure interdependencies. *IEEE Control Syst.* 11–25, December issue.
10. Nozick, L. K., Turnquist, M., Jones, D., Davis, J., and Lawton, C. (2004). Assessing the Performance of Interdependent Infrastructures and Optimizing Investments. *Proceedings of the 37th Hawaii International Conference on System Sciences*, Hawaii, January.
11. Beir, V., Ferson, S., Haimes, Y., Lambert, H., and Small, M. (2004). Risk of extreme and rare events lessons from a selection of approaches. In *Risk Analysis and Society: An Interdisciplinary Characterization of the Field*, T. McDaniels, and M. Small, Eds. Cambridge, New York, pp. 74–118.
12. Asbeck, E., and Haimes, Y. (1984). The partitioned multiobjective risk method. *Large Scale Syst.* **6**, 13–38.
13. Haimes, Y. (1998). *Risk Modeling, Assessment, and Management*, Wiley, New York.
14. Haimes, Y. Y., and Jiang, P. (2001). Leontief-based model of risk in complex interconnected infrastructures. *J. Infrastruct. Syst.* **7**(1), 1–12.
15. Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Anal.* **1**, 11–27.
16. Pikus, I. (2003). Critical infrastructure protection: are we there yet? *J. Infrastruct. Syst.* **9**(4), 1–5.
17. Peerenboom, J., Fisher, R., and Whitfield, R. (2001). Recovering from disruptions of interdependent critical infrastructures. *CRIS/DRM/IIIT/NSF Workshop on* Mitigating the Vulnerability of Critical Infrastructures to Catastrophic Failures. Alexandria, Virginia.
18. Nojima, N., and Kameda, H. (1996). Lifeline interactions in the Hanshin-Awaji earthquake disaster. In *The 1995 Hyogoken-Nanbu Earthquake Investigation into Damage to Civil Engineering Structures, Committee of Earthquake Engineering*, Japan Society of Civil Engineers, Tokyo, pp. 253–264.
19. Yao, B., Xie, L., and Huo, E. Study effect of lifeline interaction under seismic conditions. *Proceedings of the 13th World Conference on Earthquake Engineering*. Vancouver, BC.
20. Argonne National Laboratory (2003). *Infrastructure Interdependencies Associated with the August 14, 2003, Electric Power Blackout*, Infrastructure Assurance Center, Argonne, Illinois.
21. U.S.-Canada Power System Outage Task Force (Task Force) (2004). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*.
22. Lecomte, E. L., Pang, A. W., and Russell, J. W. (1998). *Ice Storm '98*, Institute for Catastrophic Loss Reduction, Toronto.

## NOTATION

C = operability failure
IFI = *infrastructure failure interdependencies*
$A$ = matrix of interdependent relationships among systems
X = system of interdependent infrastructure systems
$X_{(e)}$ = electrical system outage

# MANAGING CRITICAL INFRASTRUCTURE INTERDEPENDENCIES: THE ONTARIO APPROACH

BRUCE D. NELSON

*Emergency Management Ontario, Ministry of Community Safety and Correctional Services, Toronto, Ontario, Canada*

## 1 INTRODUCTION

In Canada, the federal government has developed a draft national strategy for critical infrastructure (CI) protection, which respects the jurisdictional prerogatives of the provincial and municipal levels of government and the propriety interests of the private sector. As such, the federal government uses a collaborative risk management–based strategy that aims to increase the resiliency of the national infrastructure through the development of trusted partnerships, the adoption of an all-hazards risk management approach, and the timely sharing of information. The national strategy recognizes the prerogative of provinces and territories to develop their own CI activities or programs and, as such, is highly supportive of these initiatives.

Within this national context, the province of Ontario developed the Ontario Critical Infrastructure Assurance Program (OCIAP). To properly understand OCIAP's approach, we must understand the environment in which it was developed; the context of CI in Ontario's emergency management program; the relationship of the three functions of public safety: preparedness and response, counterterrorism, and CI; and the development of the program itself.

This article then describes a program whose aim is to make Ontario's CI more disaster resilient and sustainable during threats from all hazards through the collaboration effort of government and the private sector in a sectorial approach.

## 2 CANADIAN ENVIRONMENT

In Canada, the responsibility for civil emergencies lies with the regions (provinces and territories) and the principal responsibility for war-related preparedness and emergency planning rests with the Federal Government [1–3]. This has been established by the division of powers, which articulated the Constitution Act of 1867 and Memorandums of Agreement between the Federal Government and the regions.

Public Safety Canada (PS Canada) supports OCIAP through their regional office. The collaboration between this group and the Emergency Management Ontario (EMO) Critical Infrastructure Assurance Program (CIAP) Staff has aided the development and success of the Ontario Program.

PS Canada also supports the Ontario CI program through cost sharing arrangements that sustain sector working group (SWG) meetings, awareness workshops, the annual conference, the production of CI materials and tools, and a modeling project.

## 3 THE PROVINCE OF ONTARIO AS A MAJOR REGION

The Province of Ontario has the largest and most concentrated population compared to other provinces and territories of Canada. One third of all Canadians live in Ontario, most of those within an hour's drive of the Canada–US border. Ontario is home to the nation's capital in the city of Ottawa and 40% of the federal government's infrastructure.

Toronto, the capital of Ontario, is the largest city in Canada and the center for many head offices of major corporations. Ontario is Canada's manufacturing leader producing 58% of all manufactured goods that are shipped out of the country.

The US is Ontario's biggest trading partner: more than 90% of exports are sent there. Every day, more than $700 million in goods crosses the Ontario–US border by highway. Ontario has 14 Canada–US border crossings, the most of Canada's provinces and territories. Approximately, 110 million tonnes of cargo move between Canada and the United States via waterways and coastal ports every year.

Ontario is the largest nuclear jurisdiction in North America and more than 50% of Canada's chemical industry is located in Ontario.

Within this context, the development of the Ontario program occurred as a result of significant infrastructure failures, which required two other public safety functions to be addressed: CI and counterterrorism. Following the Eastern Ontario Ice Storm of 1998, EMO laid the foundation for an increase in capacity and the need to address CI; the September 11, 2001 terrorist attacks broadened the view of threats facing Ontario's infrastructure. Although the CI program was developing, the SARS epidemic and the Blackout of 2003 demonstrated the vulnerabilities of networks and their interdependencies. These events caused political leaders to engage actively in the EMO-led reforms.

At the heart of these reforms was the movement toward the adoption of comprehensive emergency management programs based on a risk management approach, including activities in the five core components of emergency management: prevention, mitigation, preparedness, response, and recovery.

As part of the reforms, Ontario requires provincial ministries and communities to develop, implement, and maintain comprehensive emergency management programs (Figure 1).

The Emergency Management Act requires ministries and municipalities to conduct hazard identification and risk assessment, as prescribed by the Act and Regulation, and identify CI. The Act went on to change the Freedom of Information legislation at the provincial and municipal level allowing for protection of CI information—recognizing the need to demonstrate its commitment to creating a secure and trusted information-sharing network amongst governments and the private sector.

## 4 GETTING STARTED

In March 2002, a planning team, ably assisted by my federal counterpart from the PS Canada regional office in Toronto, was established to develop and implement a CIAP

for the province. The program was to be a province-wide program that will identify and assess Ontario's key facilities, systems, and networks, and their interdependencies, and develop a strategy to protect their vulnerabilities from physical and cyber threats. In developing the program, it became readily apparent that we would have to reconcile the public safety functions of counterterrorism, emergency management, and critical infrastructure assurance into a coherent approach. This conceptual understanding of the mutually supportive interrelationship of functions has proven to be a valuable intellectual tool, particularly when engaging in discussions with police and intelligence agencies.

In Figure 2, time flows from the top to the bottom. The event line represents the moment that the adverse event occurs, whether that is a natural hazard, a technological failure, or a human-caused event. The three "circles" represent the three core functions of public safety and security that directly relate to the successful implementation of the program. Counterterrorism is a police and intelligence function that responds to human-induced threats. Most counterterrorism functions occur before the anticipated event. And, although consequence-based emergency management planning occurs before the anticipated event, most emergency management activities are consequence based, and occur as a response after the event takes place.

CI assurance is a science-based risk management analysis of specifically identified infrastructure to assure its continued functioning. Like counterterrorism, it is a prevention or mitigation strategy intended to reduce the impact of adverse events. CI assurance differs from counterterrorism in that it focuses on the overall vulnerability of systems rather than specific, imminent threats. However, as the diagram shows, there is considerable overlap among the three functions, emergency management, counterterrorism, and critical infrastructure assurance. The star indicates the position where the circles overlap

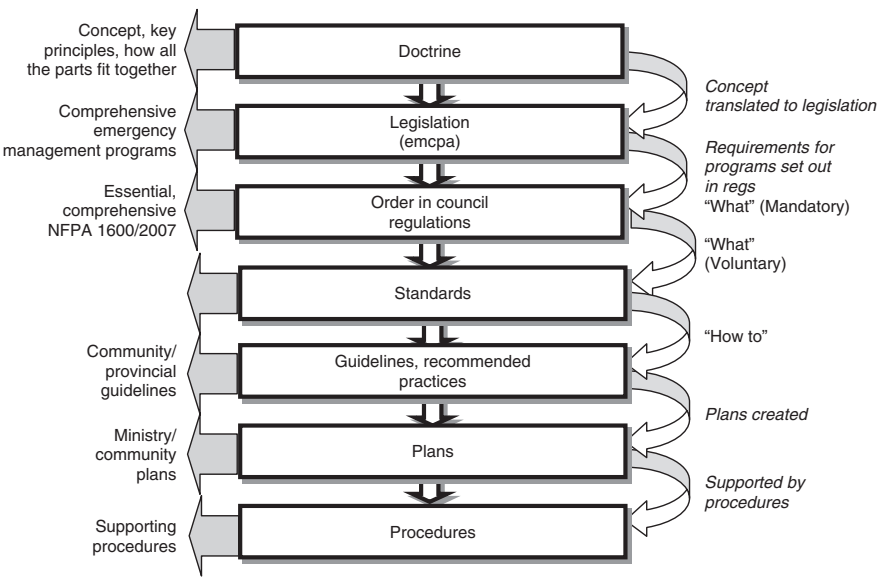



**FIGURE 1** Hierarchy of emergency management documents in Ontario.

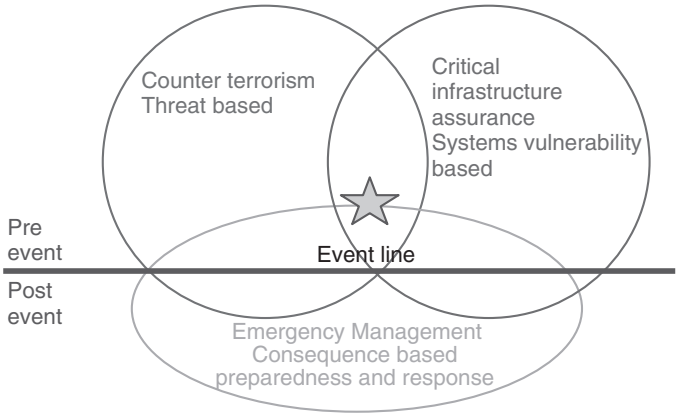



**FIGURE 2** The functional approach.

and it is at this position the decision makers, during an emergency, must bring the three circles together.

## 5 PROGRAM DEVELOPMENT—THE CONCEPT

The CIAP planning team started with a clean sheet and began researching CI programs nationally and internationally. The planners realized that it is more difficult and costly to protect against all hazards or threats than to take the business continuity process (BCP) approach and assure the continuance of key facilities. The program then became the CI assurance program addressing vulnerability and resilience. The program takes a strategic approach when it comes to sector working group (SWG) networks. The owner/operators retain the specific location of a networks' critical infrastructure; the program requires an understanding of the networks in general and their types of critical infrastructure in order to facilitate informed emergency management decisions, and enable senior leaders to set appropriate response priorities.

Determining that it takes a network to address a network, the program concept developed required a program that would bring the three levels of government together (federal, provincial, and municipal) with the private sector (owner/operators) to address critical infrastructure. The challenge is to remain within the requirements of legislation and, in particular, respecting the divisions of authority each government has and the regulatory requirements placed on the private sector. The program would bring regulators, inspectors, and owner/operators together as equals in a trusted information-sharing network.

The question of categorizing human resources and cyber as sectors remained an issue until they were determined to be enablers that play a key role in all sectors. The program stressed the need for key personnel and safeguards to the cyber component of systems and networks that permeate through all the sectors.

The CIAP concept was approved by management and moved to the implementation stage in the spring of 2003. The program continues to evolve as the sector work progresses.

## 6 THE CRITICAL INFRASTRUCTURE ASSURANCE PROGRAM

The following outlines the program as designed by the CIAP planning team.

### 6.1 Program Vision

*Ontario's critical infrastructure will become disaster resilient and sustainable during threats from all hazards through the collaborative effort of government and the private sector*.

### 6.2 Program Aim and Objectives

The aim of the OCIAP is to increase the resiliency of the province's critical infrastructure, so that it is more sustainable during an adverse event.

The central objectives of the OCIAP are to

- engage the owners and operators of critical infrastructure (public and private) in a comprehensive provincial approach;
- focus efforts to assure infrastructure assets of the greatest criticality and vulnerability;
- increase communication and collaboration within and between sectors to share information on critical infrastructure risks and interdependencies and to address threats and hazards; and
- collaborate with all levels of government and the private sector to develop and promote best practices to assure critical infrastructure.

### 6.3 Definitions

The following definitions were developed for the program:

> *CI defined as follows. interdependent, interactive, interconnected networks of institutions, services, systems, and processes that meet vital human needs, sustain the economy, protect public health, safety and security, and maintain continuity of and confidence in government*.

Since the Ontario program is an assurance program that assists practitioners in understanding the assurance concept, the following definition became important:

> *CI assurance defined as follows. the application of risk management and business continuity processes for the purpose of reducing the vulnerabilities of critical infrastructure by decreasing the frequency, duration, and scope of disruption and facilitating preparedness, response, and recovery*.

The program's key principles are risk management, business continuity, and collaboration. As part of comprehensive emergency management, the program is integral to the five components of emergency management: *prevention, mitigation, preparedness, response, and recovery*. However, the majority of work in critical infrastructure assurance occurs before an event, and the majority of the work addresses prevention and mitigation.

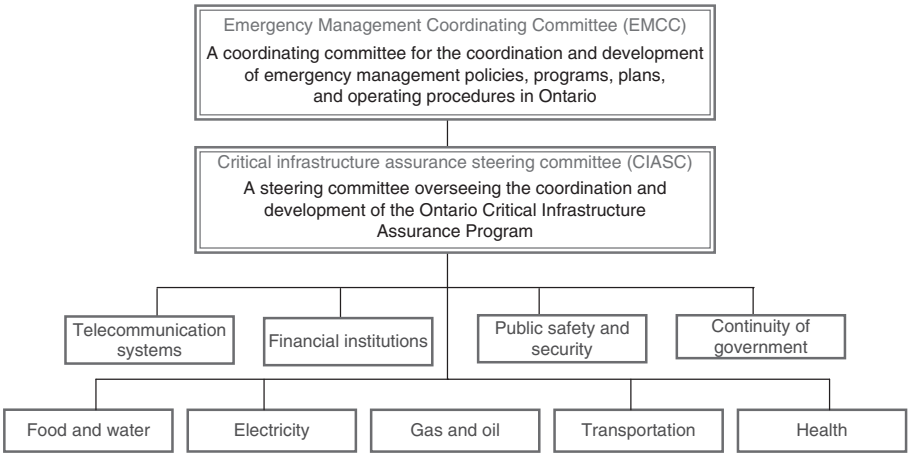



**FIGURE 3** Ontario's Critical Infrastructure Assurance Program Committee structure.

CI can be damaged, destroyed, or disrupted by natural hazards, negligence, accidents, criminal activity, and terrorist activity. Accordingly, the program assesses the potential likelihood and impact for both human-induced and natural hazards and relates this to the resiliency of the province's critical infrastructure.

### 6.4 Managing Interdependencies

Consistency of the CIAP with a comprehensive provincial emergency management program will be ensured through the following structure.

There will be an SWG for each of the identified critical infrastructure sectors. The program requires the SWG to meet four times a year at a minimum during the development stage. In practice, some sectors meet monthly to complete the required work. SWGs report to the Critical Infrastructure Assurance Steering Committee (CIASC), which oversees the coordination and development of the program.

The EMO Deputy Chief, Operations and Analysis, chairs the CIASC. The committee oversees the coordination and development of the program and addresses the issues concerning research and funding. It comprises EMO CI staff, SWG lead/coleads, representatives from PS Canada, and the provincial Ministry of the Attorney General to address freedom of information issues, Ministry of Infrastructure Renewal to address funding issues, and others as required. This committee meets four times a year.

The CIASC reports to the Emergency Management Coordinating Committee (EMCC), which is tasked with the coordination and development of emergency management programs, policies, plans, and procedures in Ontario. The Chair of the CIASC reports to the EMCC, (Figure 3).

## 7 SECTOR WORKING GROUPS

The SWGs are the key to the program and their composition reflects the federal, provincial, municipal, and private owner/operator stakeholders of their defined sector. The

**TABLE 1 The Sectors and their Respective Lead/Colead Ministries**

| | SWG Lead/Co-Lead Ministries |
|---|---|
| Food and Water Sector | Ministry of Agriculture and Food (food)<br>Ministry of the Environment (water) |
| Electricity Sector | Ministry of Energy |
| Transportation Sector | Ministry of Transportation |
| Gas and Oil Sector | Ministry of Energy |
| Financial Institutions Sector | Ministry of Finance |
| Telecommunication Systems Sector | Ministry of Economic Development and Trade Ministry of Government Services |
| Public Safety and Security Sector | Ministry of Community Safety and Correctional Services |
| Continuity of Government Sector | Ministry of Government Services |
| Health Sector | Ministry of Health and Long-term Care |

objectives for each SWG are to meet regularly to outline the industry within the sector, identify and assess they key elements of critical infrastructure within their particular sector having considered vulnerabilities, threats, and ensuing risks, identify assurance indicators, and facilitate mitigation to reduce the vulnerability or lessen the consequence created by a particular threat or hazard. All these will be documented in the model and assurance document for the sector. The assurance document is meant to provide senior management leaders comfort that the owners and operators are applying the appropriate due diligence to ensure that their systems are resilient to physical and cyber threats.

The success of the SWGs and ultimately the entire program will result in and depend upon the development of an open and trusting communication network of participants. CI information is protected under the *Emergency Management and Civil Protection Act* as indicated previously. It is important that information flow seamlessly among SWGs in order to address interdependencies; however, that information must be treated as confidential. To assist participants in the SWGs, the assurance document contains a section on communication protocol for SWG information sharing and communication protocols during an emergency.

The program identified nine broad CI sectors, and assigned a ministry lead, in some case coleads, to chair the sector and direct its activities. The determination of lead ministries was based upon the business lines and responsibilities (Table 1).

### 7.1 Establishing a Sector Working Group

Each sector lead and colead is responsible for forming the SWG, establishing their own individual protocols, and for keeping files and records related to the working group. SWG lead/coleads report to sit on the CIASC. The following steps have proved successful in forming the groups:

- The EMO Staff and PS Canada CI Coordinator (facilitating group) meet with the assigned lead representative and outline the concept of the program and their work. Program information and guide materials are provided.
- The facilitation group and the lead determine the ministries that should be involved and are invited to a CI information meeting with presentations by the facilitation group and the lead. The ministries participating then develop a relationship.

- The group now determines the federal representation based upon their normal business connections and existing federal responsibilities. The PS Canada CI Coordinator facilitates the inclusion of federal regional department representatives who would have a responsibility to the sector.
- The next step is to include the municipal representatives who have an interest in the sector.
- Finally, the private sector (owner/operators) is included. Because of the sheer number of potential representatives, the private sector is normally represented by regional associations.

## 7.2 SWG Deliverables

***7.2.1 Sector Model.*** The sector model is a generic systems map of the sector depicting its network, critical nodes, and dependencies/interdependencies. This model will provide decision makers with a better understanding of the sector and its interdependencies, as well as serve as a tool to work with scenarios during exercises and real-time emergencies. From this model, a risk matrix for the sector can be produced, which will show the vulnerable nodes in the sector; assurance solutions and best practices can then be developed to mitigate against those vulnerabilities. The model is then used in the interdependencies modeling software program under development at this time.

***7.2.2 Assurance Document.*** The assurance document outlines the sector industry, identifies CI, addresses vulnerabilities, identifies assurance indicators, and provides assurance solutions. The assurance document will give decision makers a good understanding of the sector, and its vulnerabilities and dependencies, and will ultimately aid in decision making during an emergency. EMO provides a template for the assurance document, which includes the following:

- vision and mandate
- resiliency statement
- background on the sector
- SWG participants list
- terms of reference
- communication protocol (SWG information sharing in committee and during an emergency)
- CI assurance indicators that support the resiliency statement
- sector risk management process
- assurance solutions/best practices (next steps).

## 7.3 Sector Working Group Interdependency Exercises

An important component to the program's development and the determining of sector dependencies/interdependencies and strength of relationships is the exercise component. The program conducts an annual fall conference, which includes an interdependency

exercise involving all sectors. The program also conducts smaller workshops where a number of sectors get together to address a particular vulnerability and determine best practices to increase the sectors' resiliencies. Scenarios at these exercises range from pandemic to fuel shortage.

### 7.4 Modeling Project

The program includes the Ontario Critical Infrastructure Modeling Project, which aims to produce a dynamic interdependencies model of Ontario's critical infrastructure. It is a 5-year joint pilot project with the federal government that ends in March 2010.

The primary software is RiskOutLook, a software developed in Canada for national level Y2K application and which is now being further developed to depict the cascading effects of interdependencies over time.

RiskOutLook creates a model of CI and its interdependencies, and using the assigned impact, vulnerability, and dependency ratings creates a risk matrix. The risk matrix identifies the CI with the highest impact, and the most vulnerable CI in the system; assurance solutions and best practices can then be developed to mitigate these vulnerabilities. The model will also allow for scenarios to be played out in order to study the impact of the disruption or destruction of a particular node of CI. Along with the assurance document, the model will provide a better understanding of Ontario's infrastructure and its interdependencies and will be used during emergencies and exercises to aid in decision making.

This project is dependent upon the mapping work done by the sectors. As each SWG provides input, a true determination of the software's capabilities can be documented.

## 8 CONCLUSION

The OCIAP is managing Ontario's complex interrelated infrastructure. The program's design allows it to start at a strategic level and become more granular as the program matures. With this approach, the program has had good support from the participants and they have not been overwhelmed by the complexity. The most important part of the program is the information-sharing network and from that network the SWG deliverables are attained. Senior managers have recognized work being done in the program and its importance as a prevention/mitigation program that provides input into the emergency management functions of preparedness, response, and recovery. Once implementation is completed, the program will be fully proactive identifying vulnerabilities and preventing/mitigating threats to raise the resiliency of Ontario's critical infrastructure.

## REFERENCES

1. Part VI, Constitution Acts 1867 to 1982, Distribution of Legislative Powers, Department of Justice, Canada, 1982.
2. Memorandum of Understanding on Emergency Planning between the Government of Canada and the Government of Ontario, February 25, 1985.
3. Emergency Management Doctrine for Ontario, Emergency Management Ontario, August 2005.

# ANALYSIS OF CASCADING INFRASTRUCTURE FAILURES

IAN DOBSON
*University of Wisconsin-Madison, Madison, Wisconsin*

## 1 SCIENTIFIC OVERVIEW

Cascading failure is the primary mechanism by which an attack or accident of limited scale can yield a major and widespread failure of networked infrastructures. For example, disabling a limited number of components of an electric power grid can induce a cascade of failures leading to a widespread blackout, and this blackout can lead to further failures in other infrastructures, such as transportation, communication, and water supply. The characteristic feature of cascading failure is that a series of failures weakens the system and makes further failures increasingly more likely as the failures become widespread. Cascading failure is of interest to terrorists because a modest attack on a suitably chosen set of system components can propagate via cascading failure to become a widespread failure that is much more visible and destructive. Strategies of preventing and deterring an attack need to be augmented with strategies of limiting the propagation of infrastructure failures consequent to the attack.

We think of cascading failure as having some initial failures that are followed by the propagation of a series of further failures. The failures may propagate within a single infrastructure or between infrastructures [1, 2]. The initial failures can arise from different causes, such as terrorism, sabotage, errors, accidents, weather, or system overload but the subsequent propagation of the failures is a property of the design and operation of the infrastructure. It is desirable to design and operate infrastructures to be resistant to cascading failure so that, regardless of the cause of the initial failures, the risk of the initial failures cascading to a much more widespread infrastructure failure is managed and minimized. To realize this goal, we need to be able to quantify the extent to which failures propagate and relate this to the risks of infrastructure failure. This chapter gives an overview of a method that is emerging to quantify failure propagation and estimate the risk of infrastructure failure from simulations of cascading failure. The method is first being developed and tested for cascading blackouts of large-scale electric power networks.

Catastrophic cascading events in large networked infrastructures are a challenge to risk analysis, as the astronomical number and variety of ways in which failures interact in realistic large networks preclude any exhaustive analysis of the detail of long and intricate sequences of cascading failures. Indeed, many of the ways in which failures interact in actual incidents are of low probability or unanticipated [3]. The reason these interactions occur in practice is owing to the vast number of possible rare or unanticipated interactions and the fact that good engineering practice tends to eliminate the likely and anticipated interactions. It is possible, with effort, to do a detailed analysis of the sequence

of failures *after* the cascade has occurred [4]. Indeed this is one useful way to identify weak components or problematic interactions in the system that could be upgraded or mitigated. However, one sample from a vast number of possibilities gives no guidance to predicting the overall risk of the other possible cascades. To quantify the overall risk, it is necessary to take a top-down approach that neglects many of the details and to study the essential and hopefully universal features of cascading failure.

### 1.1 Review Of Cascading

We briefly review the literature related to quantifying cascading failure in large interconnected infrastructures (the established risk analysis that applies to a smaller number of components and interactions that can be analyzed in detail is not addressed). Cascading failure leading to widespread loss of infrastructure is well recognized and there has recently been much progress both in modeling the physical and operational details of the interactions and in recognizing and qualitatively describing cascading between infrastructures as surveyed in [1, 5, 6]. There are several approaches to developing more quantitative methods.

An analytically tractable probabilistic model of cascading failure in which overloaded components fail and successively load other components is described in [7]. A critical loading of the model produces a probability distribution of the total number of failures with a power law region consistent with the observed frequency of North American blackout sizes [8] and blackout simulations [9–12]. The model can be approximated by a probabilistic branching process model [13]. Branching processes have been routinely applied to cascading processes in many fields such as epidemics, cosmic rays, and population growth but have only recently been applied to the risk analysis of cascading failure [13–16]. North American data for the distribution of electric power transmission line outages are fit with several probabilistic models, including an exponentially accelerating cascading model in [17].

There are Markov models for abstract graphs representing interactions between idealized system components [18]. The percentages of inoperability of interdependent infrastructures are obtained as a linear function of the disturbance by solving a Leontief input–output model in [19, 20]. A network of influence factors between system components is considered in [21] and ratios of infrastructure impacts are obtained in [2].

There are many simulations of electric power systems using Monte Carlo and other methods that can be used to estimate the risk of blackouts such as in [9, 10, 12, 22–24]. Another useful approach to blackout risk is to identify and mitigate only the high risk or likely failures as for example in [25]. There are complex system approaches to blackout risk [10, , 26–28] that account for self-organizing dynamics such as network upgrades.

There is an extensive literature on cascading in graphs surveyed in [29, 30] that is partially motivated by idealized models of propagation of failures in infrastructure networks such as the Internet. The dynamics of cascading is related to statistical topological properties of the graphs. Work on phase transitions and network vulnerability that accounts for forms of network loading includes the references [31–33].

***1.1.1 Galton–Watson Branching Processes.*** In this section, an informal and introductory overview of Galton–Watson branching processes for their application to the risk of cascading failure is given; for a detailed and elegant formal treatment of these classical probabilistic models, see [34, 35]. Galton–Watson branching processes apply to discrete

numbers of failures of system components. For simplicity, we suppose that the failure of only one type of component is being tracked. The failures are produced in stages or generations starting from some initial failures, and if the number of failures in a stage becomes zero, then all subsequent stages have zero failures and the cascade of failures stops. Each failure in each stage (a "parent" failure) produces a probabilistic number of failures ("children" failures) in the next stage according to the *offspring distribution*. For example, the offspring distribution can be a Poisson distribution. The children failures then become parents to produce the next generation and so on. A key property making branching processes tractable is that the parents in each generation produce their respective children in a manner statistically independent of each other. The intent of the modeling is not that each parent failure in some sense "causes" its children failures; the branching process simply produces random numbers of failures in each generation that can match the outcome of cascading processes. To model the initial disturbance produced by terrorism or otherwise, we assume an initial distribution of failures for the first stage that is different from the offspring distribution assumed for the generation of all the following stages.

A key parameter of the branching process is $\lambda$, which is the mean of the offspring distribution or the average number of children failure per parent failure. If $\lambda < 1$, then the cascading process will die out to zero failures at some stage and usually corresponds to an infrastructure failure of small or modest size. If $\lambda > 1$, then the cascading process can possibly die out, but it can also propagate to a catastrophe with all components failed. Another parameter is $\theta$, the mean number of initial failures.

We consider cascading failure in infrastructures with a large but finite number of interconnected components. Therefore, if all components fail, the cascade stops and is said to saturate. More generally, there may be a tendency for the cascades to be inhibited when a certain number of components $S$ less than or equal to the total number of components is reached and this can also be roughly modeled as a saturation.

The branching process produces a random total number of failures $Y$ considering all the stages; that is, $Y$ is the total family size. If we measure the disturbance size by $Y$, then the main data produced by the branching process model is the probability distribution of $Y$. If the cost of the disturbance as a function of $Y$ is known, then the distribution of risk as a function of disturbance size can be obtained by multiplying the distribution of $Y$ by the cost. The distribution of risk as a function of disturbance size is basic to a quantitative approach to managing the risk [26].

### 1.2 Behavior of A Cascading Model

We illustrate the qualitative behavior of the saturating branching process model of cascading failure as the amount of propagation $\lambda$ and the average number of initial failures $\theta$ are varied. This behavior is similar to the behavior of other probabilistic cascading failure models [7].

Suppose that the failures propagate in a large number of components $S$ so that each failure has approximately a small uniform probability of independently causing failure in a large number of other components. Then the offspring and initial failure distributions can be approximated by Poisson distributions, and the distribution of the total number of failures $Y$ has an analytic formula given by a saturating form of the generalized Poisson distribution [13, 14]:

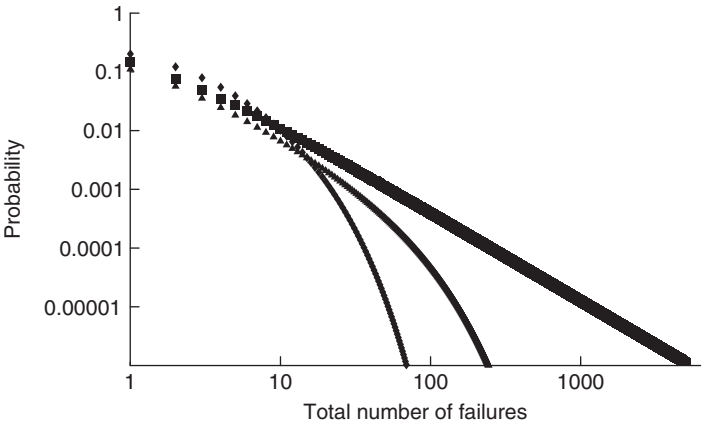



**FIGURE 1** Log–log plot of probability distribution of the total number of failures $Y$ in branching process model for three values of propagation $\lambda$. $\lambda = 0.6$ is indicated by the diamonds. $\lambda = 1.0$ (criticality) is indicated by the boxes. $\lambda = 1.2$ is indicated by the triangles (note the triangle in the upper right indicating a high probability of all components failing). The mean number of initial failures is $\theta = 1$ and there are $S = 5000$ components.

$$P[Y = r] = \begin{cases} \theta(r\lambda + \theta)^{r-1} \dfrac{e^{-r\lambda-\theta}}{r!(1 - e^{-\theta})}; & 1 \le r < S \\ 1 - \displaystyle\sum_{i=1}^{S-1} P[Y = i]; & r = S \end{cases} \tag{1}$$

First we assume a small initial attack with a mean number of initial failures $\theta = 1$. Then Figure 1 shows the probability distributions obtained for $S = 5000$ components and three values of propagation $\lambda$. For subcritical $\lambda = 0.6$ well below 1, the probability of a large number of failures less than 5000 is exponentially small. The probability of exactly 5000 failures (all components failed) is also very small. As $\lambda$ increases in the subcritical range $\lambda < 1$, the mechanism by which there develops a significant probability of large number of failures near 5000 is that the power law region of approximate slope $-1.5$ extends toward 5000 failures [36]. (A straight line of slope $-1.5$ on a log–log plot indicates the power relationship probability $\propto$ (number of failures)$^{-1.5}$.) For the near critical $\lambda = 1$, there is a power law region extending to 5000 failures. For supercritical $\lambda = 1.2$, there is an exponential tail. This again implies that the probability of large number of failures less than 5000 is exponentially small. However, there is a significant probability of exactly 5000 failures that increases with $\lambda$.

If we assume a fixed propagation $\lambda = 0.6$ and increase the mean number of failures in the initial attack to $\theta = 20$, then the distribution of the total number of failures changes as shown in Figure 2.

Consider in Figure 3 how the mean number of total failures $EY$ increases with increasing propagation $\lambda$. The mean number of total failures at first increases slowly and then increases much more rapidly at the critical point near $\lambda = 1$. It is called a critical point because the sharp change in gradient in Figure 3 and corresponding power law in the distribution of the number of failures in Figure 1 is analogous to a type 2 phase transition in statistical physics.

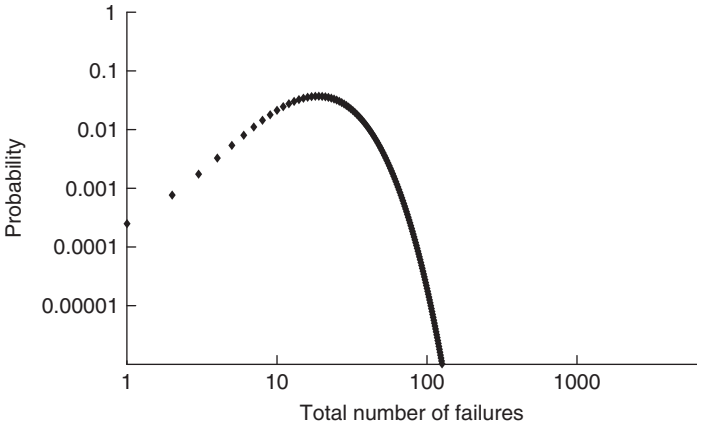



**FIGURE 2** Log–log plot of probability distribution of total number of failures $Y$ in branching process model for average number of initial failures $\theta = 10$ and propagation $\lambda = 0.6$. There are $S = 5000$ components.

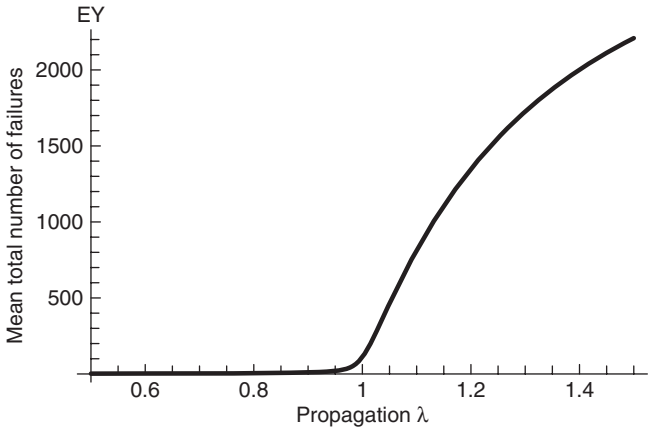



**FIGURE 3** Mean total number of failures $EY$ as a function of propagation $\lambda$.

### 1.3 Estimating Propagation from Simulations

There are many infrastructure simulations that can produce samples of cascading failures in stages. Without quantitative statistical analysis of these sample cascades, it is not clear how robust the infrastructure is to cascading failure. For example, if one of the sample cascades is a very large failure, does this indicate a vulnerable infrastructure, an unrepresentative rare event, or simply bad luck? We briefly indicate how propagation and the distribution of total failure size can be estimated from a relatively small sample of simulated cascades.

If we assume that the cascading in the infrastructure is approximated by a branching process model, we can estimate the parameters $\lambda$ and $\theta$ of the branching process model from the simulated cascades. In the branching process model, the propagation $\lambda$ is the mean of the offspring distribution or the average number of children failures per parent failure. In fact, $\lambda$ may be estimated from a sample of cascades by dividing the total

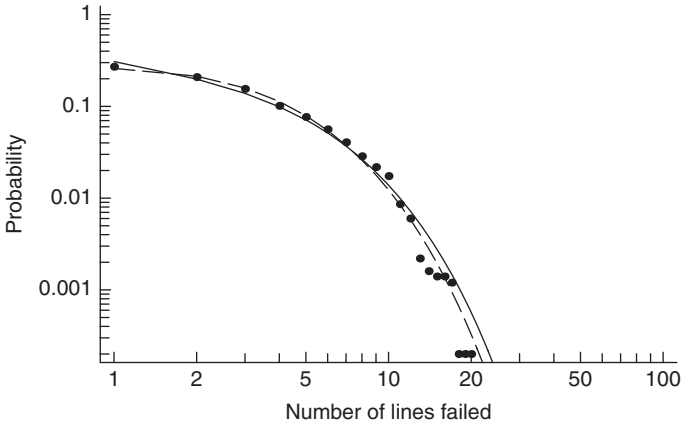



**FIGURE 4** Probability distributions of total number of electric power transmission lines failed obtained by different methods. The dashed line is obtained by estimating parameters ($\lambda = 0.4$ and $\theta = 1.5$) from simulation data and assuming a branching process model of the cascading. The dots are obtained empirically from the same simulation data. The simulation is the OPA model of cascading line outages in blackouts [9] and the test case is the IEEE 118 bus system with loading factor 1.0. Figure reprinted with permission from [15].

number of children failures in the sample cascades by the total number of parent failures. (Failures arising in stages after the first stage are children failures and failures arising in the stages before the last stage are parent failures. The last stage may be a stage with zero failures at which the cascade ends.) However, this standard computation [37, 38] may require adjustment to account for saturation effects [15]. The mean $\theta$ of the number of initial failures is estimated simply as the total number of initial failures divided by the number of sample cascades.

The propagation $\lambda$ and mean initial failures $\theta$ are useful metrics describing the cascading in the simulation data. Moreover, estimation of these parameters provides an estimate of the distribution of the total number of failures using equation (1). This provides a way to verify the assumption that a branching process approximates the simulation results. One can simply run the simulation exhaustively to obtain an empirical distribution of total number of failures. This empirical distribution can then be compared to the estimated distribution of the total number of failures. If the match is acceptable, then the estimation via the branching process can be used to approximate the estimated distribution of total number of failures. An example of the match obtained in a subcritical test case from [15] is shown in Figure 4.

Why use an approximate estimation of the distribution of the total number of failures by estimating $\lambda$ and $\theta$ when an empirical distribution can be produced simply by running the simulation exhaustively? The estimation of the distribution via estimating $\lambda$ and $\theta$ is much more efficient in that it requires many fewer simulated cascades. The distribution of total number of failures for a cascading process can have a heavy tail (power law region of exponent about $-1.5$). Estimating these heavy tails takes a large number of simulated cascades to obtain accurate statistics. On the other hand, the offspring distribution does not have a heavy tail and each stage of each cascade contributes data about the offspring distribution. Moreover, if the form of the offspring distribution is known (for example, a Poisson distribution), then estimating the mean of the distribution is quicker

than estimating the entire offspring distribution. Therefore, estimating the mean of the offspring distribution $\lambda$ and thereby computing the distribution of total number of failures is expected to require much fewer simulation runs [15].

### 1.4 More General Branching Processes

Tracking the numbers of one type of component that have failed in each stage of the cascade gives an integer number of failures in each stage. This is modeled by the Galton–Watson branching process explained above. However, it is also useful to track continuously variable quantities in each stage of the cascade, especially those quantities that determine the impact of the failures. For example, in a blackout one can track the electrical power that is disconnected. Cascades of continuously varying quantities are modeled by continuous state branching processes [39, 40]. These can be applied in a similar way to estimate branching process parameters and compute the probability distribution of the quantity determining the impact of the failures [16].

There are many generalizations of branching processes that could potentially model such factors as multiple types of component and variations in amount of propagation. The initial work is investigating and testing the simplest modeling assumptions. The limits of application of the method and the potential need for more sophisticated models are not yet clear.

## 2 CRITICAL NEEDS ANALYSIS

Cascading failure is fundamental to the rare but high-impact failures of substantial portions of infrastructures. Although there has been considerable progress in detailed modeling and qualitative descriptions of cascading failure in and between large networked infrastructures, there remains a need to understand and quantify the essential features of cascading processes and deduce the probability and risk of various sizes of failure events. To manage the risk of cascading failure, it is necessary not only to inhibit the initial attack or accident, but also to design and operate the system to limit the propagation of failures so that initial failures are less likely to propagate much further.

It would be valuable to be able to efficiently predict the distribution of cascade sizes from a modest number of simulated cascades and also to monitor real infrastructure failures to determine the extent to which failures propagate after an initial attack or accident. Note that although the initial failures may differ for an intentional attack and an accident, the extent to which the failures propagate after the initial failures should be similar. Thus, estimates of propagation of infrastructure failure arising from accidents should be effective in estimating how much the rarer terrorist attacks are magnified by cascading.

## 3 RESEARCH DIRECTIONS

Initial work on cascading in simulations of electric power system blackouts shows how overall cascading failure risk could be quantified. We have proposed the simplest branching process models of cascading failure and can fit parameters to quickly determine the

amount of propagation of failures and the distribution of total failure size. Initial testing is promising but much more testing and development is needed on more elaborate simulations of blackouts and on more general models of cascading infrastructure failure. Once efficient methods for predicting cascading failure risk from simulated cascades are established, the next step is to adapt these methods to monitor cascading failures in the actual infrastructures. The observed data would provide a benchmark for the necessarily simplified simulation models. The monitoring would in effect predict the frequency of catastrophic infrastructure failures much more quickly than the empirical approach of simply waiting for a very long time for enough rare catastrophic events to occur in order to get accurate statistics to quantify the risk.

## REFERENCES


1. Rinaldi, S. M., Peerenboom, J. P., and Kelly T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Contr. Syst. Mag*. **21**, 11–25.
2. Zimmerman, R., and Restrepo C. E. (2006). The next step: Quantifying infrastructure interdependencies to improve security. *Int. J. Crit. Infrastruct*. **2**(2/3), 215–230.
3. Perrow, C. (2002). *Normal Accidents*, Princeton University Press, Princeton.
4. U.S.-Canada Power System Outage Task Force. (2004). *Final Report on the August 14th blackout in the United States and Canada*. United States Department of Energy and National Resources, Canada.
5. Peerenboom, J. P., and Fisher, R. E. (2007). Analyzing cross-sector interdependencies. *40th Hawaii International Conference on System Sciences*. January, Hawaii.
6. Kröger, W. (2006). Critical infrastructure at risk: Securing electric power supply. *Int. J. Crit. Infrastruct*. **2**(2-3), 273–293.
7. Dobson. I., Carreras, B. A., and Newman D. E. (2005). A loading-dependent model of probabilistic cascading failure. *Probab. Eng. Inform. Sci*. **19**(1), 15–32.
8. Carreras, B. A., Newman, D. E., and Dobson, I., Poole A. B. (2004). Evidence for self organized criticality in a time series of electric power system blackouts. *IEEE Trans. Circuits-I*. **51**(9), 1733–1740.
9. Carreras, B. A., Lynch, V. E., Dobson, I., and Newman D. E. (2002). Critical points and transitions in an electric power transmission model for cascading failure blackouts. *Chaos*. **12**(4), 985–994.
10. Carreras, B. A., Lynch, V. E., Dobson, I., and Newman, D. E. (2004). Complex dynamics of blackouts in power transmission systems. *Chaos*. **14**(3), 643–652.
11. Nedic, D. P., Dobson, I., Kirschen, D. S., Carreras, B. A., and Lynch, V. E. (2006). Criticality in a cascading failure blackout model. *Int. J. Electr. Pow. Energy Syst*. **28**, 627–633.
12. Chen, J., Thorp, J. S., and Dobson, I. (2005). Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. *Int. J. Electr. Pow. Energy Syst*. **27**(4), 318–326.
13. Dobson, I., Carreras, B. A., and Newman, D. E. (2004). A branching process approximation to cascading load-dependent system failure. *37th Hawaii International Conference on System Sciences*. January, Hawaii.
14. Dobson, I., Carreras, B. A., and Newman, D. E. (2005). Branching process models for the exponentially increasing portions of cascading failure blackouts. *38th Hawaii International Conference on System Sciences*. January, Hawaii.

15. Dobson, I., Wierzbicki, K. R., Carreras, B. A., Lynch, V. E., and Newman, D. E. (2006). An estimator of propagation of cascading failure. *39th Hawaii International Conference on System Sciences*. January, Kauai, HI.
16. Wierzbicki, K. R., and Dobson I. (2006). An approach to statistical estimation of cascading failure propagation in blackouts. *CRIS, Third International Conference on Critical Infrastructures*. September; Alexandria, Virginia.
17. Chen, Q., Jiang, C., Qiu, W., and McCalley, J. D. (2006). Probability models for estimating the probabilities of cascading outages in high-voltage transmission network. *IEEE Trans. Pow. Syst*. **21**(3), 1423–1431.
18. Roy, S., Asavathiratham, C., Lesieutre, B. C., and Verghese, G. C. (2001). Network models: growth, dynamics, and failure. *34th Hawaii International Conference on System Sciences*. Hawaii, 728–737.
19. Jiang, P., and Haimes, Y. Y. (2004). Risk management for Leontief-based interdependent systems. *Risk Anal*. **24**(5), 1215–1229.
20. Reed, D., Chang, S., and McDaniels, T. (2006). Modeling of infrastructure interdependencies. *CRIS, Third International Conference on Critical Infrastructures*. September, Alexandria, Virginia.
21. Vamanu, B., and Masera, M. (2006). Vulnerability of networked infrastructures: anomalies, errors, interdependencies. *CRIS, Third International Conference on Critical Infrastructures*. September, Alexandria, Virginia.
22. Hardiman, R. C., Kumbale, M. T., and Makarov, Y. V. (2004). An advanced tool for analyzing multiple cascading failures. *Eighth International Conference on Probability Methods Applied to Power Systems*. September, Ames, Iowa.
23. Kirschen, D. S., Jawayeera, D., Nedic, D. P., and Allan, R. N. (2004). A probabilistic indicator of system stress. *IEEE Trans. Pow. Syst*. **19**(3), 1650–1657.
24. Anghel, M., Werley, K. A., and Motter, A. E. (2007). Stochastic model for power grid dynamics. *40th Hawaii International Conference on System Sciences*, Hawaii, January.
25. Ni, M., McCalley, J. D., Vittal, V., and Tayyib, T. (2003). Online risk-based security assessment. *IEEE Trans. Pow. Syst*. **18**(1), 258–265.
26. Carreras, B. A., Lynch, V. E., Newman, D. E., and Dobson, I. (2003). Blackout mitigation assessment in power transmission systems. *36th Hawaii International Conference on System Sciences*. January, Hawaii.
27. Dobson, I., Carreras, B. A., Lynch, V., and Newman, D. E. (2007).Complex systems analysis of series of blackouts: cascading failure, criticality, and self-organization. *chaos*. **17**, 026–103.
28. Newman, D. E., Nkei, B., Carreras, B. A., Dobson, I., Lynch, V. E., and Gradney, P. (2005). Risk assessment in complex interacting infrastructure systems. *Thirty-eighth Hawaii International Conference on System Sciences*. January, Hawaii.
29. Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Rev*. **45**(2), 167256.
30. Boccaletti, S., Latora, V., Moreno, Y., Chavez, M., and Hwanga, D.-U. (2006). Complex networks: structure and dynamics. *Phys. Rep*. **424**, 175–308.
31. Watts, D. J. (2002). A simple model of global cascades on random networks. *Proc. Natl. Acad. Sci. USA*. **99**(9), 5766–5771.
32. Motter, A. E., and Lai, Y.-C. (2002). Cascade-based attacks on complex networks. *Phys. Rev. E*. **66**(6), 065102.
33. Crucitti, P., Latora, V., and Marchiori, M. (2004). Model for cascading failures in complex networks. *Phys. Rev. E*. **69**, 045104(R).
34. Harris, T. E. (1989). *Theory of Branching Processes*, Dover Publications, New York.

35. Athreya, K. B., and Ney, P. E. (2004). *Branching Processes*, Dover Publications, New York; (Reprint of Springer-verlag Berlin 1972).
36. Dobson, I., Carreras, B. A., Lynch, V. E., Nkei, B., and Newman, D. E. (2005). Estimating failure propagation in models of cascading blackouts. *Probab. Eng. Inform. Sci*. **19**(4), 475–488.
37. Dion, J.-P., and Keiding, N. (1978). Statistical inference in branching processes. *Branching Processes*, A. Joffe, and P. Ney, Eds. Marcel Dekker, New York.
38. Guttorp, P. (1991). *Statistical Inference for Branching Processes*, Wiley, New York.
39. Kallenburg, P. J. M. (1979). *Branching Processes with Continuous State Space*. Mathematical Centre Tracts 117, ISBN 90 6196 188 2, Mathematisch Centrum, Amsterdam.
40. Nanthi, K. (1983). *Statistical estimation for stochastic processes*. Queen's papers in pure and applied mathematics. 62.

# WATER INFRASTRUCTURE INTERDEPENDENCIES

NEIL S. GRIGG
*Colorado State University, Fort Collins, Colorado*

## 1 INTRODUCTION

Managers of water and electric systems are more concerned about security failures of the infrastructures they depend on than about failures in their own systems. Their concerns were reported in a workshop on water, electricity, and transportation managers, where they expressed confidence in their own security plans but sought guidance on managing interdependencies [1]. This article identifies the interdependencies among water and other infrastructure systems and explains how to reduce the corresponding risk and improve infrastructure security. Other articles in the volume explain the nature of water infrastructure and how to address direct security issues.

## 2 OVERVIEW OF WATER SYSTEM INTERDEPENDENCY

As other articles in this volume explain, water system managers face threats to their systems from natural causes such as earthquakes and from human-induced causes such as attacks on their supervisory control and data acquisition (SCADA) systems. To respond,

these managers must assess vulnerabilities and mitigate risk by multiple actions to strengthen emergency plans and response capabilities.

Water system managers also face vulnerabilities from interdependencies with elements of the water infrastructure that they may not control (such as their raw water supplies) and with other infrastructures (such as with electric power). These two sources of vulnerabilities represent different situations that require distinct types of responses. In addition, water system managers must take actions to reduce the risk that failures of their systems will harm those that depend on them.

Study of these interdependencies involves relationships between elements and levels of systems. Interdependency can be explained at a high level of systems aggregation, but security threats and responses require explanations at detailed levels to create a valid picture. The many types of interdependencies do not fit well into a classification system, and discussions about them can seem ad hoc and without unifying themes. To clarify these interdependencies, the article uses two models to explain the situations that water managers face.

The first model explains interdependencies among elements of the water infrastructure itself and those between the water infrastructure and other infrastructures. For the purposes of this article, these are named *intrasystem interdependencies* among water system elements and *intersystem interdependences* where water systems have relationships to other infrastructures.

The framework of the model is shown in Figure 1, which illustrates the two types of interdependencies. On the left side of the figure, water infrastructure is shown as having five parts or subsystems. These illustrate the supply chain of the water supply system and shows how irrigation is linked to the water supply system in parts of the nation.

On the right hand side of Figure 1 are shown five infrastructure sectors with close links to water. These are the sectors from among the critical infrastructures and key resources identified in the National Infrastructure Protection Plan that exhibit the greatest degrees of interdependence with water infrastructure [2].

The terms (intrasystem and intersystem) can be confusing, but the concept of interdependency is inherently complex and the concepts are explained in Figure 1.

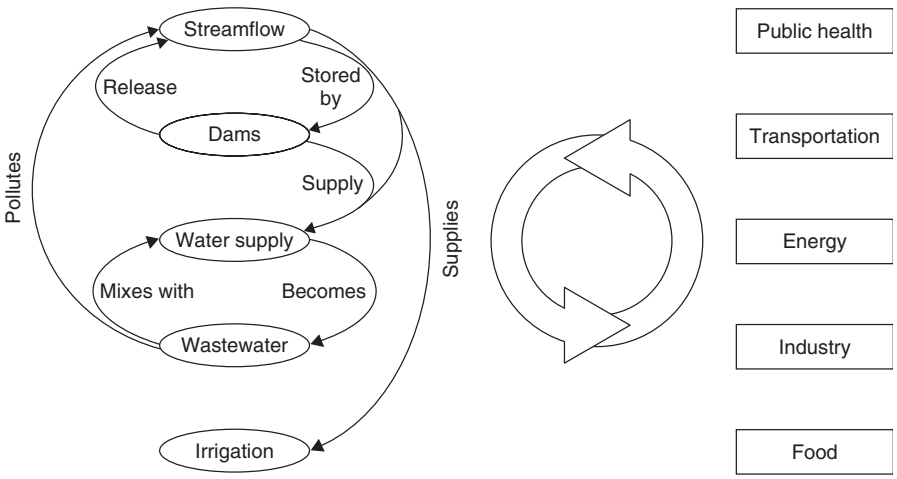



**FIGURE 1** Water infrastructure interdependency model.

The second model maps the supply chain of water production and the provision of direct and indirect water services to customers. This enables the explanation of interdependencies that arise from supply chain disruption and impacts on other sectors from failures in water services. This model will be illustrated later.

## 3 KNOWLEDGE BASE ABOUT INTERDEPENDENCIES IN THE WATER SECTOR

The knowledge base about interdependencies among water sector elements resides in the broad field of water resources management. In this field, the concept of integrated water resources management (IWRM) has been developed to explain the many interdependencies that arise in water systems management [3]. Managers of water systems are aware of these, and have formulated conceptual frameworks to explain them, but the institutional capacity to respond is lacking [4].

The knowledge base about technologies for integrated water resources management is rich, and includes advanced computer-based methods involving large databases and simulation models. For example, the State of Colorado is developing an extensive set of advanced decision support systems for management of its river basins [5]. The serious knowledge gap is in development of institutional responses to overcome barriers among water system managers and their governing boards [6].

International research about needed institutional responses focuses on shared governance, but achieving effective methods for it involves overcoming political challenges. Examples can be seen in the many water wars and transboundary conflicts that arise over sharing of water supplies. Given these institutional difficulties, water system managers are forced to develop security plans that do not depend on the success of their partners in managing shared waters.

Research about relationships between water and other infrastructures focuses on intergovernmental relations. Current trends toward privatization and downsizing of government work against the kind of cooperative planning and mutual aid arrangements needed to bolster intersystem security. The responsibilities of water system managers to address cross-system issues differ from those of their water system partners.

## 4 INTRASYSTEM INTERDEPENDENCIES

Although they are operated as distinct utility services, water and wastewater systems are inextricably linked to other elements of the overall water system. This overall water system includes a number of subsectors as follows [7]:

- municipal and industrial water supply and wastewater;
- irrigation and drainage for farming and landscaping;
- environmental water for natural systems or habitat;
- water-based recreation;
- dam and reservoir management;
- aquifer management for groundwater systems;
- hydropower generation;

- waterborne transportation and navigation;
- stormwater and flood control.

Management of water resources within the subsectors involves links among hydrologic subsystems, between water quantity and quality, and between the physical processes of water use. The left side of Figure 1 shows a simplified view of these.

Water and wastewater utilities are the organized units with the most influence on overall water management. In the United States, there are over 50,000 water supply systems and nearly as many wastewater systems. Although most of these are small, they are the management organizations with most authority and responsibility to manage water through its hydrologic cycle. The other group with great influence comprises the agencies that manage the nation's some 75,000 dams and reservoirs. These involve a much smaller number of management units, such as the Corps of Engineers, Bureau of Reclamation, and many hydroelectric producers, among others [8].

The interdependences among these elements of the overall water resources system occur because water flows under natural forces through its hydrologic cycle. This cycle takes water from the atmosphere, deposits precipitation that becomes runoff or ground water and flows to various receiving waters, from which it is evaporated. Sometimes the water is diverted from one basin to another using tunnels and other infrastructure. However the water flows, its continually flowing nature creates intrasystem interdependences.

Briefly, streamflow is stored in reservoirs by dams, which are in turn operated to control the release of flows downstream. Streamflow and dam releases provide raw water supplies to cities, industries, and irrigators. Water supply releases become wastewater that affects the quality of streamflow and mixes with water supply through discharge–diversion sequences. These elements may be operated by different management agencies and require numerous administrative arrangements and communication channels to identify vulnerabilities and manage risk. For example, a federal agency may operate a reservoir that provides water supply to a city. The city is thus dependent on the agency to deliver raw water reliably.

Many details must be supplied to describe these interactions fully. Although a valid watershed model can illustrate the important linkages among subsystems, it will not be able to replicate all processes at the micro level. For example, groundwater–surface water interactions are important but difficult to model accurately.

The interactions shown in Figure 1 illustrate important intrasystem interdependencies and vulnerabilities. For example, raw water must be available and transported to points of storage, treatment, and/or use. Wastewater systems also involve treatment plants and pipes, and have vulnerable components. However, their purposes differ from drinking water and the consequences of security breaches are different. Their security is addressed in a separate article in this volume. Irrigation systems can be disrupted but the direct consequences to water systems are normally not as critical as they are for drinking water.

Examples of important intrasystem interdependences among parts of the overall water system are shown in Table 1.

## 5 INTERDEPENDENCIES WITH OTHER INFRASTRUCTURES

Although, at a high level, water has clear interdependencies with other infrastructures, the nature of the relationships must be defined at the subsystem level. The discussion in

**TABLE 1 Examples of Intrasystem Interdependencies for Water Systems**

| Intrasystem Interdependency | Example |
|---|---|
| Disruption of transportation routes for raw water | An earthquake might block a tunnel and cut off raw water supplies |
| Drought to reduce raw water supplies | Water supply systems can extend for long distances, and drought in an upper basin can reduce supplies lower down |
| Flood to damage water handling facilities | River flooding may disrupt operation of raw or treated water facilities |
| Intentional or unintentional contamination of raw or treated water | Intentional contamination of treated water is an obvious threat. Contamination of raw water supplies is normally not a major threat because of its volume, but it is important to keep watersheds clean and contaminated reservoirs are difficult to clean |
| Dam safety | Security of dams is critical because their failure can affect water supplies, public safety, and the environment. Dams can be threatened by sudden events or lack of maintenance |
| Treated water systems | Treated water may be distributed to wholesale customers, thus disruptions can propagate through the systems. Security of treated water is addressed in a separate article in this volume |

this section is organized around the six critical infrastructure sectors shown on the right side of Figure 1.

The water service most closely aligned with public health is drinking water. Wastewater and irrigation water are also linked to health issues. Contaminated drinking water or failed water systems have many links to public health, which are explained in another article. The public health system also presents threats to water systems. For example, a source of pharmaceuticals in drinking water is the disposal of outdated medicines in hospitals and other health care facilities. Another example is that inadequate regulation of public activity in swimming and fishing areas can pollute water that the public is exposed to.

Food security is another health-related water issue because water is an ingredient in food, from the farm to the dining room table. Contaminated irrigation water can create hazards up the wholesale to retail chain and lead to outbreaks of waterborne disease. Failure of raw water systems can also lead to crop failures and economic hardship.

Water and industry exhibit interdependencies because industrial production requires large inputs of high quality water. This dependency can be quickly noted by examining categories of NAICS industries as published by the US Census Bureau. NAICS is the North American Industry Classification System, see Reference [9] for an explanation. In particular, the chemical industry exhibits interdependencies with water in several ways. It produces water treatment chemicals such as phosphates and chlorine gas. Shortages of these will impede water treatment and transportation of some of them can create hazardous conditions, as with transportation of chlorine gas to water treatment plants. Water

is also linked to critical industries. For example, during World War I, the Muscle Shoals dam facility on the Tennessee River produced nitrates for ammunition and explosives. The facility is now part of the Tennessee Valley Authority system.

As water must be transported to points of use, its infrastructure has a number of interdependences with transportation systems. For example, vulnerable bridges and tunnels may form part of water conveyance systems. If a dam fails, it will often fail downstream transportation arteries. If roadways and bridges are not protected against floods, they can be failed by water forces. Waterborne transportation has obvious links to water management. During drought, water utilities often call for reduced navigation flows for barges that may be used for transporting vital commodities.

Energy systems and water are linked because if raw or treated water is pumped, the systems are vulnerable to power outages. Also, control of many water systems has become automated and loss of energy can fail critical monitoring and control systems. Hydroelectricity is produced from flowing water. Cooling water is required for all electricity generation, and thermoelectric cooling is a large user of water for once-through cooling and cooling towers.

## 6 RESPONSES TO INTERDEPENDENCIES

Although water system interdependencies are inherently complex and difficult to manage, they can be explained with the metaphor of the business corporation's supply chain and customer relations. The supply chain models the water utility's ability to produce high quality finished water using inputs of raw water, electric power, chemicals, and other resources. The customer base comprises direct and indirect water users. Direct water users are people who drink water, swim in it, cook with it, or use it for other purposes. Indirect users are people who use any product that requires water as an input, such as food that is produced through irrigation.

This model can be illustrated with a simple diagram (Figure 2) that shows the producer of water services as receiving supply chain inputs from within the water industry (such as raw water) and from outside the industry (such as electric power or chemicals). The producer then provides water services to its customers, who will be impacted by any failures in water quantity or quality. These customers will then produce their products, which often depend on high quality and reliable water.

As shown in Figure 2, water service providers often lack control over all the resources they require. This is the same situation faced by any production unit that relies on others for its supply chain. The water utility normally cannot gain ownership and complete control over all of its supply chain, and coordination strategies are its main tool to strengthen security of supply chain interdependencies. These strategies will involve different measures and combinations of stakeholders for intrasystem water elements, such as between raw water and treated water, than they will for intersystem infrastructures, such as between water and its electric power inputs.

Coordination can be modeled by forms of business organization based on relationships between a business and its suppliers and production units. Three types of supply relationships help visualize interdependencies:

- A vertically integrated water utility with its supply chain within the span of control of one executive. An example could be a water supply utility serving 50,000 customers in a single city.

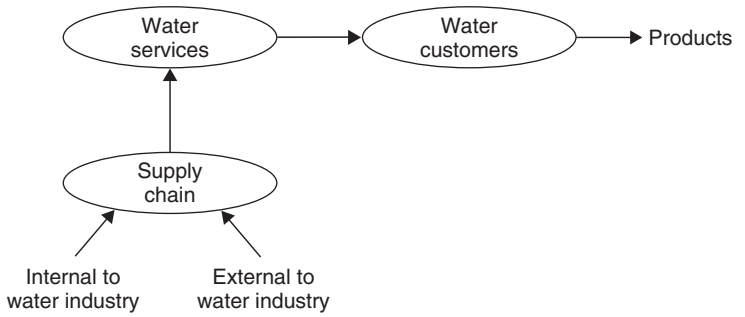



**FIGURE 2** Supply chain and outputs of water service providers.

- A horizontally integrated water utility with divisions under separate executives who treat each other as "customers." An example could be an integrated utility with its own raw water supplies, treatment and distribution systems, and wastewater services.
- A water utility that contracts with suppliers in independent organizations in similar and different industries. An example could be a water utility that performs business operations but does not own or control its own water or infrastructure.

Supply chain interdependencies must be managed through relationships between water system managers and their suppliers. For a smaller, vertically integrated utility, these relationships can probably be managed through day-to-day meetings and shared problem-solving. For larger, horizontally integrated utilities it is more difficult to achieve effective communication and it might be necessary to make more formal arrangements through contracts and working agreements that are audited through performance reports. When the water utility operates by contracting with independent organizations for its supply chain, formal contracts and agreements become essential.

Coordination does not have to occur in formal and informal venues inside of organizations. When water services are provided by different agencies, the participants may see each other in regional planning meetings, at professional associations, and at other occasions.

Coordination presents different challenges, as in the case of intersystem infrastructures where the managers may not know each other at all. For example, public health officials who receive reports of waterborne disease outbreaks are normally not in touch with water officials on a regular basis. By the same token, the chain-of-responsibility for food contamination from irrigation water is long and convoluted. Even the more direct link between electric power and water systems does not involve regular communications between managers. It is not reasonable to rely simply on more communication and coordination among managers of disparate infrastructures to improve security. Rather, managers of these infrastructures must take matters into their own hands to mitigate threats from failures in the infrastructures they depend on. They must assess the risk of failure of other systems and take measures to mitigate the risk or create redundancies.

Barriers to coordination occur among interdependent water systems from the same problems that occur within organizations, where coordination requires frequent communication, meetings, sharing of information, and other means to improve cooperative work. Coordination and communication are always more difficult between organizations than

within them, but both cases present barriers. Examples of barriers might include not being aware of interdependencies, being busy and overloaded with other work, not wanting to work together, and lack of incentives from governing boards.

## 7 CRITICAL NEEDS ANALYSIS

The model of water system risk used in the article shows vulnerabilities from interdependencies among elements of the water infrastructure and between water and other infrastructures. The interdependencies go two ways: those that affect the supply chain of water and those that exhibit impacts on others from water system failures.

One example of intrasystem interdependency is failure of raw water supplies, which prevents water treatment organizations from performing their missions. Another would be uncontrolled river flooding that disrupts operation of water infrastructures. An example of a supply chain failure from another category of infrastructure is loss of electric power to a water system.

Examples of impacts from failure of water services include public health incidents and contamination of food supplies from polluted water. Also, industrial and energy systems depend on reliable water supplies to function.

Planning for interdependencies requires the water system manager to recognize categories of relationships that include supply chain inputs from within and outside of the water industry. These supply chain interdependencies must be managed through coordination among water system managers and their suppliers. The coordination can range from informal arrangements to formal contracts and agreements.

In the case of intersystem infrastructures, managers may not be able to coordinate well because they are not in frequent contact and may not even be aware of each other's activities. In these cases, infrastructure managers must take matters into their own hands, and consider threats from failures in other infrastructures just the same as other uncontrolled threats.

Regardless of the type of interdependency, threats from failures within the water industry or outside of it can be included in a vulnerability analysis. To include them, the analyst must recognize the threats from interdependencies in the same way as a direct threat is recognized, whether from natural or human causes. Once the threats are recognized, they can be mitigated by direct actions or coordinated arrangements with partner organizations.

## 8 RESEARCH DIRECTIONS

Management of threats that arise to water systems from interdependencies among themselves and with other infrastructures requires responses in technological, management, and institutional arenas. The technological responses involve the same types of instrumentation, control devices, and other tools that are needed for ongoing security programs and have been described in Reference [10].

Required management responses range across governance, organizational planning, data management, coordination with partnership organizations, and reporting. Research into these topics is robust for business and government organizations but little research has been conducted specifically for water utilities and their interdependencies [11].

The most difficult arena for enhanced security is in institutional responses that include organizational structures, incentives, and relationships. For example, the United States has some 85,000 units of local government, many of which are involved in infrastructure services [12]. In addition to working effectively among themselves, they must work with many independent private water and energy companies. The regulatory structure that governs water and related infrastructures involves a patchwork of federal and state agencies and local governing boards. Research needed focuses on improving intergovernmental arrangements within the existing structure of the water industry as it relates to the management structure of other infrastructures.

## REFERENCES


1. Department of Homeland Security (2008). *National Infrastructure Protection Plan*. US Government, Washington, DC, August 23, 2008. http://www.learningservices.us/DHS/NIPP/.
2. Colorado State University (2003). *Workshop Summary: Infrastructure in Northern Colorado: Measuring Performance and Security for Water, Electricity, and Transportation Systems*. Colorado, Fort Collins, CO.
3. Global Water Partnership (2008). *Managing Water*, Accessed August 25, 2008. http://www.gwpforum.org/.
4. Grigg, N. S. (2008). *Total Water Management: Practices for a Sustainable Future*, American Water Works Association, Denver, CO.
5. Colorado Water Conservation Board (2008). *Colorado's Decision Support Systems*, August 25, 2008. http://cwcb.state.co.us/WaterInfo/DecisionSupport/dss.htm.
6. Young, J. (2006). Challenges and benefits of total water management. *J. Am. Water Works Assoc*. **98**(6), 32–34.
7. Grigg, N. S. (2005). *Water Manager's Handbook*, Colorado, Aquamedia Publications Denver, CO.
8. Grigg, N. (2007). Water sector structure, size and demographics. *J. Water Resour. Plann. Manage*. **133**(1), 60–66.
9. U.S. Census Bureau (2008). *North American Industry Classification System*, August 23, 2008. http://www.census.gov/epcd/www/naics.html.
10. Department of Homeland Security (2005). *CIP R&D Workshop for Academic and Federal Laboratory R&D Providers*, June 29, 2005 Session Report. September 2005.
11. US Government Accountability Office (2005). *Protection of Chemical and Water Infrastructure. Federal Requirements, Actions of Selected Facilities, and Remaining Challenges*, GAO-05-327 Washington, DC. March 2005.
12. USBOC (2008). *Census of Governments*. May 6, 2008. http://www.census.gov/govs/www/cog2002.html.


## FURTHER READING


American Water Works Association (2004). *Emergency Planning for Water Utilities*. Colorado, Denver, CO.

American Water Works Association Research Foundation (2004). *Security Practices Primer for Water Utilities*. Colorado, Denver, CO.

# INFRASTRUCTURE DEPENDENCY INDICATORS

THERESA BROWN
*Sandia National Laboratories, Albuquerque, New Mexico*

## 1 INTRODUCTION

Interdependencies are created by multiple dependencies between two or more infrastructures. Hence, dependencies are the fundamental building block of interdependencies and models of these interconnected, interdependent systems. This article provides an overview of the state of the art in identifying infrastructure dependencies and analyzing their importance with respect to infrastructure protection measures.

## 2 SCIENTIFIC OVERVIEW

Infrastructures evolved with society and technology. Infrastructure dependency analysis for homeland security applications is a relatively new field of study encouraged in the United States by the National Research Council [1], endorsed and funded by the federal government [2]. Funding over the last 6–10 years, primarily by government agencies, produced new interdisciplinary programs and centers at universities (e.g. Department of Homeland Security Centers of Excellence at Michigan State University, University of Southern California, John Hopkins University, University of Minnesota, Texas A&M University, and the University of Maryland; the Critical Infrastructure Modeling and Assessment Program at the Virginia Tech Center for Energy and the Global Environment); new analysis centers at national laboratories (e.g. National Infrastructure Simulation and Analysis Center at Sandia and Los Alamos National Laboratories and Infrastructure Assurance Center at Argonne National Laboratory); and private research organizations. Each of these research and analysis centers is focused on improving our understanding of infrastructures, how they interact and influence one another, the overall well-being of the populations they serve, and the economies they support. Since this is a new area of study, there are relatively few publications devoted to the broad field of infrastructures. Two journals, *Journal of Infrastructure Systems* published by the American Society of Civil Engineers (since 1984) and *International Journal on Critical Infrastructures* published by Inderscience (since 2004), focus on new contributions to infrastructure design, protection, and management. The literature for this field is just developing.

Rinaldi et al. [3] provide a useful classification system for infrastructures, defined by four major categories of interdependencies: geographical, physical, logical, and cyber. Since interdependencies imply multiple, interrelated dependencies between two or more elements, dependencies are the more fundamental relationship. Dependencies can be classified using the same categories as interdependencies, or in this case, with cyber

dependencies as a subset of physical dependencies. The fundamental indicators of dependencies can also be classified as geographical, physical, and logical. In the following sections, examples of work in the area of infrastructure dependency identification and analysis are provided, along with areas for improvement.

## 3 GEOGRAPHICAL DEPENDENCY INDICATORS

The easiest dependencies to identify are geographical dependencies, when elements of multiple infrastructures are close enough to be damaged by the same event. The only complication in identifying these dependencies is in defining the events of concern, including the location or potential locations and obtaining locations for all of the nearby infrastructure elements to identify which are the ones within the potential damage zone. For many events, the infrastructure elements must be in very close proximity for geographical dependencies to exist. When infrastructures use a common right-of-way, such as a dam, bridge, tunnel or sewer pipeline, catastrophic accidents or failures at those locations can disrupt multiple infrastructures at the same time. The presence of multiple infrastructures in a single location (colocation) is the indicator of geographic dependency for isolated incidents (e.g. tanker truck accident and explosion that leads to the collapse of a bridge). As we understand the potential threats, the vulnerability of infrastructure elements to each of those threats, and the likelihood of the threat at any location, we can develop risk-based indicators of dependencies.

Large, destructive events such as hurricanes create geographical dependencies across multiple infrastructures, populations, industries, and commercial sectors due to damage and injuries caused by high winds and flooding. The map in Figure 1 depicts the relative risk (by county) posed by hurricane strikes. A risk indicator was calculated by multiplying a likelihood factor by a consequence factor. The likelihood factor is a combination of the probability of hurricane occurrence and probability of damage to infrastructure. An estimate of the probability of a hurricane impacting a county is based on the historic frequency of hurricanes. The probability of damage to infrastructures within each county was estimated using a wind damage contour for each historical hurricane path based upon its intensity. A consequence factor was developed as a function of the population living in each county.

$$\text{Risk indicator} = \text{population}[1000\text{s}] \times \text{hurricane frequency} \times \text{damaging-wind frequency}$$

The result is a geographical distribution of the risk of direct damage due to hurricanes.

Similar indicators exist for other natural threats, such as seismic activity, flooding, landslides, and wild fire. The US Geological Survey publishes seismic hazard maps that can be used in conjunction with fragility curves for specific engineered structures to estimate the risk of damage due to ground motion. The Federal Emergency Management Agency provides maps of flood, fire, geologic, and other hazards in the United States.

More refined indicators can be developed to represent the risk to specific infrastructures or assets, the duration of the expected disruption, or the total consequences. These refinements would be the first step toward developing indicators of the risk due to propagating effects created by physical and logical dependencies.

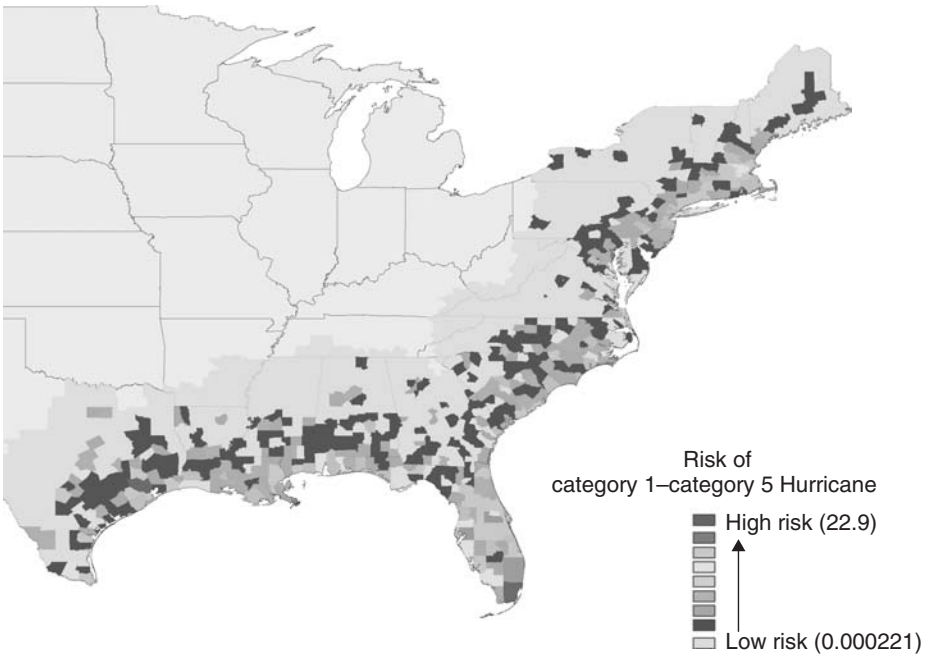



**FIGURE 1** Geographical dependency indicator: relative risk to infrastructure by county due to hurricane; on the basis of frequency of occurrence, category of hurricane and population density (risk indicator developed by the National Infrastructure Simulation and Analysis Center in 2006 for prioritizing off-season hurricane planning scenarios and analyses).

## 4 PHYSICAL DEPENDENCY INDICATORS

Physical dependencies are created when two or more systems are physically connected and one is dependent on the other to function. Interdependencies are created if there are mutual dependencies or if the state of their interaction influences the state of another infrastructure. Connectedness is the basic physical dependency indicator. If a compressor station for a natural gas pipeline is connected to the electric power distribution system, the compressor is likely electric powered. However, it does not indicate if electric power is the primary or only energy source for the compressor or how the loss of power at that compressor station influences the flow of gas in the pipeline. Connectedness only indicates the potential for dependency.

Even simple indicators like connectedness may be difficult to verify on a large scale, because many forms of connection cannot be easily observed (underground utilities), alternative sources may exist (e.g. backup electric power generation capabilities, fuels in onsite storage, and water storage system), and utility data are generally proprietary. In some cases surrogate information exists, such as economic supply and demand data, allowing inference of physical or logical connections. Developing more refined indicators of physical dependencies requires knowledge of the operational impacts of infrastructure input disruptions.

The most connected infrastructures, the ones that create the greatest number of dependencies, are energy (includes electric power, coal, natural gas, nuclear fuels, and petroleum, oils, and lubricants (POL)), communications (includes telecommunications,

information systems, and broadcast), transportation (includes water, rail, pipeline, road, and air transportation systems), and banking and finance (includes federal and commercial banking systems, insurance, commodity markets, and other financial institutions) [4–6]. The overall connectivity of the network is an indicator of system robustness. Abstract models of power networks with different topologies indicate that the greater the overall connectivity, the more robust the network [6]. This implies that while the connected systems are more dependent on each other, the dependency comes with a benefit if it leads to greater connectivity. The connectivity within each of these systems and with other infrastructures depends on which systems and locations are evaluated. The road system in the United States is one of the most highly connected networks, yet it has zones of low connectivity at the edges and in isolated portions of the network. In models of banking transactions, the topology and behaviors are required to estimate system robustness [7].

A general understanding of specific infrastructure processes allows us to develop dependency models and begin the process of refining dependency indicators to include the dynamics of the problem. Only a few of the physical dependencies for energy, telecommunications and transportation, and indicators of those dependencies are provided here.

### 4.1 Electric Power Dependencies

Electric power generation and system control are the processes creating dependencies for the electric power infrastructure. Hydroelectric generation is dependent on the sufficient supply of water and environmental conditions that allow the release of water. Other types of power generation are dependent on water for cooling, specific fuels (coal, natural gas, nuclear, and refined products e.g. diesel and jet fuel), regulatory limits on emissions, and the transportation of fuels from the production region to the generator facility. Indicators of dependencies between electric power generation in a particular location (or region) and fuel production in another location (or region) are developed based on the type of generator(s) and connectivity of the generator to the production region via feasible transportation system(s) for the fuel or fuels.

Transport feasibility requires an economically viable route and mode. In this case, connectivity occurs via the transportation network, making electric power generation dependent on transportation and fuel production. If the generator is connected to multiple fuel production locations (or regions) the dependency on a specific fuel source or specific transportation route is reduced. Figure 2 shows the natural gas pipelines (transportation) and electric power generation plants in the Midwest, focusing on Illinois. The region is able to import natural gas from Canada and the central and southeast regions of the United States. Even more crucial is the fact that natural gas generation is not the primary source of power in this area. Coal-fired generation and nuclear power plants provide most of the power in Illinois [8].

The dependency of a specific facility or region on a specific electric power generator is a little more difficult to quantify than a geographical dependency because of all the factors that influence the steady supply of electric power. First, it must be determined whether the generator has or could have a substantial impact on the electric power supply in the region of concern. In order to understand the influence of a single generator, knowledge about the state of the system is required. The best indicator is the ratio of the plant's generation capacity to the region's reserve margin (the expected amount of

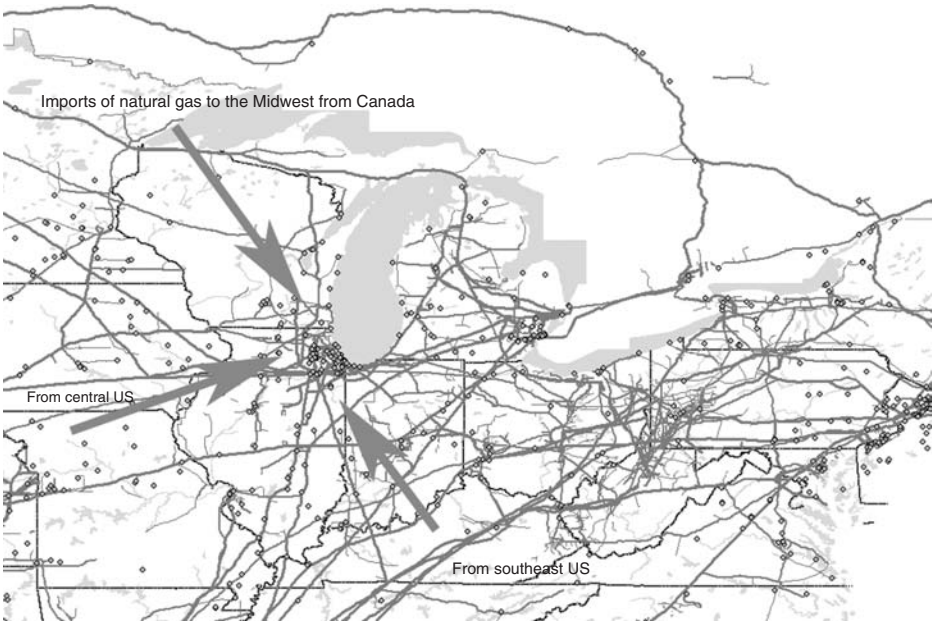



**FIGURE 2** Natural gas pipelines ($\geq$ 10 in. in diameter) and natural gas fired generation in the Midwest US illustrates connectivity to multiple supply regions (based on 2005 data from Plants (power plants) and Penwell (on-shore pipelines)).

available capacity that is greater than the expected peak demand). The reserve margin is an indicator of the state of the electric power system within a specific region, reflecting the likelihood that the region is self-sufficient, can export power to other regions, or will be dependent on power imports from other regions. The indicator for specific generators provides an estimate of how close the system would be moving from one state to another (e.g. self-sufficient to power importer) if that particular generator is taken off-line. Peak demand is used to provide a bounding case, since the regional demand for electric power varies diurnally and seasonally. The indicator has to be updated because peak demand and aggregate generation capacity change over time as changes in population, behaviors, and technology alter power demands and as generation capacity is built or taken off-line (for repairs or permanently retired).

Electric power transmission and distribution system operations are highly automated, human-in-the-loop, remote control systems. Control systems are dependent on reliable communications and data. The power outage in the northeastern United States in August 2003 was due in part to unreliable and missing information [9].

### 4.2 Communication Dependencies

Communication systems can change state very quickly due to a wide variety of reasons, tied to both logical and physical dependencies. Within the telecommunication system there are a large number of system operators that constantly monitor to anticipate conditions that may lead to sudden, prolonged high call volume that creates network congestion and call blocking. It is not clear whether the telecommunication operation indicators will

be of use for the power operation systems, because power operation systems utilize multiple communication systems that are not part of the public telecommunication network. The difference between data system dependencies and other physical dependencies is that data systems are vulnerable to more threats, such as denial of service attacks or malicious software programs (sent from remote sites, using information or wireless communication networks) or electromagnetic disturbances.

The best indicator of dependency on specific communication assets is geographical, local service areas called *local access and transport areas* (*LATAs*). Maps of publicly available LATAs are relatively well known. They correspond to the region of an area code, but some have multiple area codes.

The impact of telecommunication disruptions on the operation of other infrastructures requires more evaluation, but may depend on whether the systems have sufficient volume of critical inputs. Just-in-time management of inventories creates systems that are less robust to supply disruptions [6].

### 4.3 Transportation Dependencies

Transportation systems are dependent upon the physical transportation networks (pipelines, roads, rail, and waterways), fuels for the combustion engines that power the transport (natural gas or electric power for pipeline compressors; diesel for trucks, tankers, and barges; jet fuel for airplanes), specialized labor (commercial drivers, pilots, longshoremen, engineers, and airline pilots), and communication systems for logistics. Given the ubiquity and connectedness of most of the transportation networks anything more than delay in transportation is unlikely for any of the modes, with a few exceptions at the edges and in sparsely populated regions of the networks. Multiple transportation modes mean demand can shift to another mode. Whether that shift occurs, depends on the economics of the shift relative to the cost of the delay.

Fuel supplies are also difficult to disrupt on a large scale because there are significant amounts of fuel of all types distributed around the country in storage systems. Price may be the best indicator of fuel supply, or at least the perceived risks of short supply, and transportation costs. Local fuel shortages can occur when perceived shortages in supply or concern about the reliability of supply lead to hoarding (a logical dependency).

## 5 LOGICAL DEPENDENCY INDICATORS

Logical dependencies, when one infrastructure influences another without being physically connected, are due to human decisions and actions. The state of, or perceived risks in, one infrastructure could influence behaviors/operations in another infrastructure due to loss of confidence in supply; through competition for labor or market share; or due to shifts to alternate inputs as a result of price or regulatory changes.

Economic relationships represent logical dependencies. Input–output models based on sales and production data compiled by government agencies provide indicators of long-term equilibrium conditions between sectors of the economy. They are often used to evaluate the net economic impact of the decline or loss of output in one sector on the other sectors and country or region as a whole. They indicate logical dependencies for a specific period of time, but do not account for production limitations, the ability to offset disruptions through withdrawals from storage, or other adaptations. Without

physical connections, logical dependencies can change suddenly, creating uncertainty and significant instability in supply that ripples through the connected systems. Inventory or production oscillations can be caused by unexpected time delays in receiving shipments or orders [9].

Labor is a logical dependency for all infrastructures. Local labor shortages have occurred during renegotiation of union contracts due to labor walkouts and/or lockouts. Labor has been impacted on a broader scale by large military deployments (World War II and the call for women to enter the manufacturing workforce to offset labor shortages) and pandemics. Infrastructures have continued to function through all those situations because of adaptive behaviors.

Change in demand due to price (demand elasticity) is an indicator of the logical response that moderates the impacts' supply disruptions. Demand elasticity for infrastructure services may be a function of the capability to switch to an alternative supply, implementation of conservation measures, or delaying purchases or production.

Unless a situation has historical precedent, it is difficult to develop proven indicators for this class of dependency. If the event has historical precedent, the reactions may be vastly different, given the knowledge of the previous event or events. And, if the disruption had caused severe problems, effective protective measures may have been put in place. It is not clear that system dynamics models of logical dependencies are predictive but they provide a better indicator of possible outcomes because they are able to represent all types of dependencies in a single, functioning, representation of the complex system. Figure 3 shows the structure of the dependencies in a model developed to evaluate the

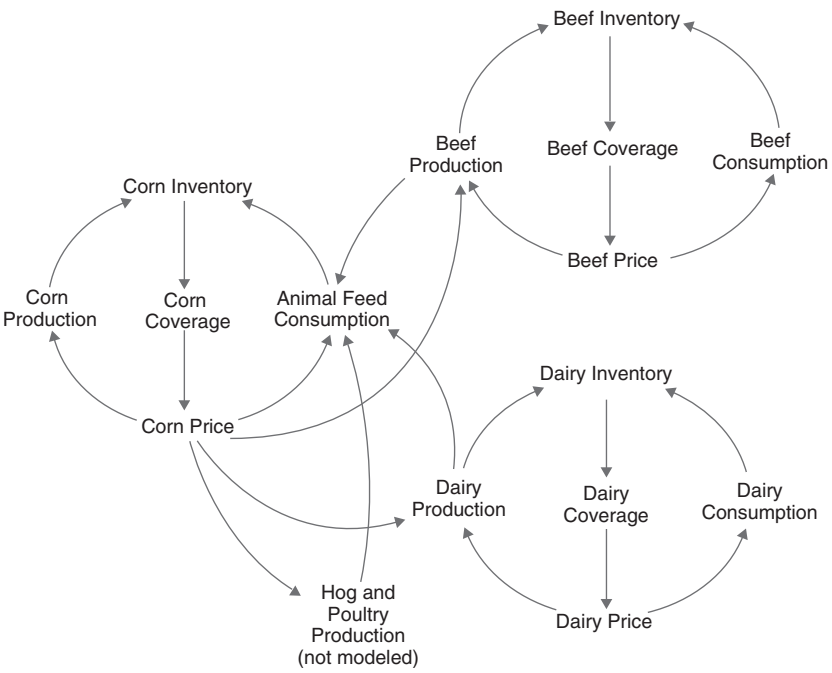



**FIGURE 3** Model structure of dynamic dependencies between livestock, corn, and dairy production showing the logical dependencies between production sectors, created through the price of feed, influencing the characteristics of each production cycle.

dynamic dependencies between beef, dairy, and corn production. The beef–dairy–corn dynamics model was developed as part of the National Infrastructure Interdependency Model in the Critical Infrastructure Protection Decision Support System (CIPDSS) by Sandia, Los Alamos, and Argonne National Laboratories for the Department of Homeland Security Office of Science and Technology, to evaluate the impacts of disease outbreak in the beef cattle industry. The interactions between the three sectors shown in Figure 3 illustrate some of the new, logical dependencies developing between agriculture and energy.

Recently, concern over crude oil prices and supply led to increased use of corn for ethanol production [10], which has increased the price of corn for animal feed. This is causing a switch to cheaper, soy-based feeds in livestock industry. Soy and corn are grown in the same fields (a geographical dependency); high prices for corn reduced the amount of soy grown (a logical dependency) [11]. Short supplies increase soy prices, putting increased pressure on the livestock industry. Beef prices increase. The result being, the prices of all commodities depending on fuels or transportation, physically and logically, increase. The only way to anticipate all these changes is to understand the dependencies and dynamics of this system. Simple indicators do not provide that kind of insight.

## REFERENCES


1. National Research Council. (2002). *Making the Nation Safer*, National Academy Press.
2. Department of Homeland Security. (2006). *National Infrastructure Protection Plan 2006*, Department of Homeland Security.
3. Rinaldi, S., Peerenboom, J., and Kelly, T. (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Syst. Mag.* **21**, 11–25.
4. Min, H.-S. J., Beyeler, W. E., Brown, T. J., Son, Y. J., and Jones, A. T. (2007). Toward Modeling and simulation of critical national infrastructure interdependencies. *IIE Trans.* **39**, 57–71; Special issue on Industrial Engineering of Operations Research in Homeland Security.
5. Beyeler, W. E., Conrad, S. H., Corbet, T. F., O'Reilly, G. P., and Picklesimer, D. D. (2005). Inter-infrastructure modeling–ports and telecommunications. *Bell Labs Tech. J.* **9**(2), 91–105.
6. Conrad, S. H., and O'Reilly, G. P. *An Overview of Energy and Telecommunications Interdependencies Modeling at NISAC*.
7. Beyeler, W. E., Glass, R. J., Bech, M., and Soramäki, K. (2007). Congestion and Cascades in payment systems, *Physica A*.
8. Energy Information Administration. (2007). *Electric Power Monthly Data*, for February (downloaded from EIA website http://www.eia.doe.gov/cneaf/electricity/epm/epm_ex_bkis.html) in May 2007.
9. U.S.-Canada Power System Outage Task Force. (2003). Final Report on the August 14, *Blackout in the United States and Canada: Causes and Recommendations*, pp. 18–19. U.S. Department of Energy and Natural Resources Canada.
10. Baker, A., and Zahniser, S. (2007). *Ethanol Reshapes the Corn Market*, Amber Waves: Special Issue 66(5). Economic Research Service/USDA (WWW.ERS.USDA.GOV/AMBERWAVES).
11. Ash, M., and Dohlman, E. (2007). *Oil Crops Outlook*, Economic Research Service Report OCS-07d, May 14, USDA (WWW.ERS.USDA.GOV).

# OBJECT-ORIENTED APPROACHES FOR INTEGRATED ANALYSIS OF INTERDEPENDENT ENERGY NETWORKS

RODRIGO PALMA-BEHNKE AND LUIS S. VARGAS
*Department of Electrical Engineering, University of Chile, Santiago, Chile*

## 1 INTRODUCTION

In many fields, there is a growing interest for tools to study the interdependencies of different areas of activity or production. Driven forces in this process have been security, economy, and environmental problems, where the cross effects of policies are highly linked [1]. In the literature, an important part of the investigation is dedicated to the study of critical infrastructure in order to prevent possible catastrophes [2], whereas another line of research is given by environmentally sustainable development [3, 4]. The underlying objective of those works is to study the cross effects of policies in different fields in order to measure their effect on environmental conditions [5]. All these studies recognize the high complexity of the problem, which is characterized by multiple agents and decision makers, large-scale systems with numerous components, nonlinear coupled subsystems, spatially distributed, adaptive in time, and investment decisions of discrete nature. Another aspect of complexity is the need of know-how integration of different disciplines. The mathematical formulation of these problems usually leads to extremely complex systems. In addition, the trend of market liberalization toward decentralized decision process has increased even further the complexity of the problem [6, 7].

This article is organized in seven sections. Section 2 presents the general models used to represent the transportation and energy networks. Section 3 presents the classes and objects relationship. Section 4 describes the software developed according to the system models. In Section 5, the methodology to state the scenarios for the studies is presented. In Section 6, a case study considering the network in the Chilean territory is developed. Finally, in Section 7, the main conclusions of this section are summarized.

## 2 SCIENTIFIC OVERVIEW

In the literature, an important part of the investigation is dedicated to the study of critical infrastructure in order to prevent possible catastrophes [8]. This topic was particularly sensitive during 1999 due to the Y2k effect. Another line of research is given by environmentally sustainable development, where the cross effects of policies in different fields on the improvement of environmental conditions are studied [9]. It is recognized that the high complexity of the problem is characterized by

- large-scale systems with numerous components;
- hierarchical multiple noncommensurable, conflicting, and competing objectives;
- multiple agents and decision makers;
- multiple governmental agencies with different missions, resources, timetables, and agendas;
- multiple constituencies;
- multiple transcending aspects and functions;
- nonlinear coupled subsystems;
- spatially distributed, adaptive in time; and
- investment decisions of discrete nature.

Overall, analysis and design of complex, large-scale nonlinear dynamic interacting systems constitute an open theoretical challenge.

The object-oriented programming (OOP) offers a methodological alternative to deal with the problem of interactions among energy and transportation. Specifically, in this article the development of activity models for each sector and a method for studying their effects on the environment is proposed. This methodology should be capable of measuring the impact due to the future implementation of technological improvements and policies at a country-wide level.

## 3 SYSTEM MODELING

The modeling approach presented in this section is inspired by previous research work [6, 7, 10] based on two main criteria. The first criterion imposes that the main feature of the modeling technique is versatility, that is, it must be capable of being used for the electricity, fuel, and transportation sectors. In addition, a systematic approach to deal with the problem of interdependencies among those sectors is required. To achieve these tasks, the modeling must fulfill the following needs:

- consistent system and component modeling (scaling, databases, and granularity);
- well-defined system frontiers;
- adequate modeling of the interdependencies among different sectors;
- activity models and tools (i.e. agent-based and game theory) inside each sector;
- data mining and visualization.

In the field of software development, two advancements have gained wide spread importance and acceptance: the OOP [11, 12] and the graphical user interface (GUI) [13]. The OOP has recognized advantages that concern flexibility, expandability, maintainability, and data integrity. In this field, the unified/universal modeling language (UML) is a standardized visual specification language for object modeling. UML is a general-purpose modeling language that includes a graphical notation used to create an abstract model of a system, referred to as a *UML model* [10, 12]. This approach is the conceptual base for several popular OOP languages.

Likewise, the GUI improves the user interaction with the computer allowing a more comprehensive analysis tools manipulation and data interpretation. Accordingly, this work

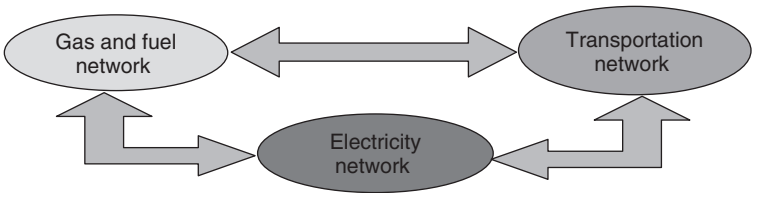



**FIGURE 1** Interdependencies among large-scale infrastructures.

applies an OOP methodology to the new energy market structure in order to create a simulation software package.

The second criterion states that, from a physical point of view, the interdependencies among large-scale infrastructures, such as electric power, transportation, and fuel sectors, often have a network structure (Fig. 1).

This structure reflects an explicit, physical set of network interconnected devices. Also, it can handle implicit interconnections created by communications, control, and functional dependence. Thus, according to the above criteria a model based on the object-oriented (OO) paradigm was chosen in this work. The large box in the center of Figure 2 represents the physical models (urban and interurban) where each network physically and functionally interacts. The regulatory, economic, and technological frameworks are also highlighted as relevant inputs to the two major models. The outputs of the modeling framework are the transport activity levels that are used to compute the fuel and energy consumptions and the environmental impact of the emissions resulting from future economic and technological developments.

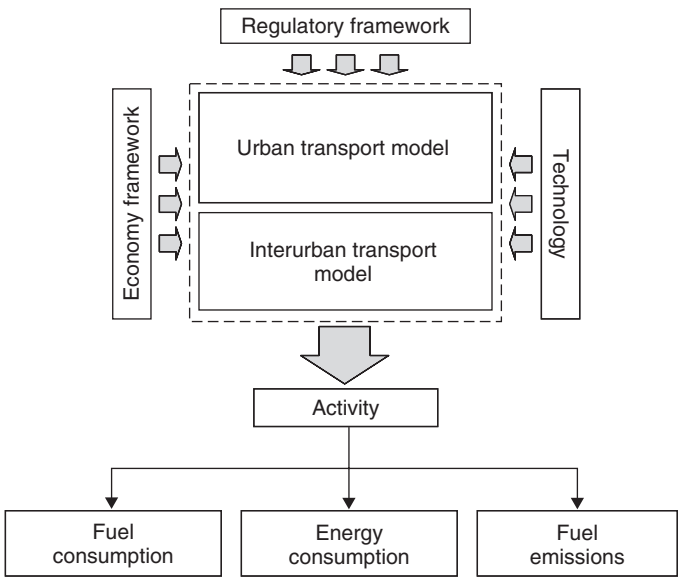



**FIGURE 2** System network model.

The individual characteristics of power, fuel, and transportation components are described by object attributes. On the other hand, the information exchange among objects is represented by messages following the OOP paradigm.

The object modeling technique has been used for developing the object models for each network.

They are shown in Figure 3.

In the OOP terminology, generalization of a data object along with its data variables and methods is a class of data objects. The data variables are referred to as *class attributes* and an instance of a class is called an *object*. The concept of inheritance makes it possible to define subclasses of a class, which share characteristics of the parent class and so on.

The proposed modeling breaks down a "system component" object into three subclasses: namely, "fuel component", "power component", and "transportation component". Each of these components makes a further use of inheritance to encompass all the components of its network. For example, the power system is represented by 1-pole and 2-pole elements.

In the list of attributes for each object, there are emission factors in order to estimate their environmental pollution features. The pollutants considered in this work are CO, HC, No*x*, particle material (MP)10, $SO_2$, $CH_4$, $N_2O$, $NH_3$, and $CO_2$.

## 4 CLASSES AND OBJECTS RELATIONSHIPS

In this section, a description of the classes together with the interdependencies among them is presented.

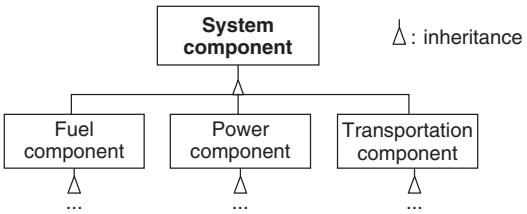



**FIGURE 3** Object model of the system.

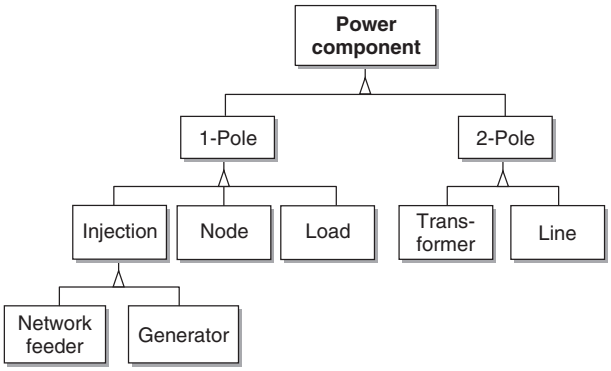



**FIGURE 4** Hierarchy chart of power system classes.

### 4.1 Power System Classes

Figure 4 shows the hierarchy chart of the power system classes, which corresponds to a simplified version of the hierarchy presented in Ref. [12]. Power component is the most general class and its attributes and methods are available for all subclasses [10–12]. Since simulation models are typically based on a node/branch-representation, these classes are explicitly included in the OO data model. The *1-pole* subclass encompasses all elements connected between a bus and the neutral (or ground). The subclass *2-pole* contains all branch facilities having impedance such as transmission lines and transformer subclasses. Note that a three winding transformer may be represented by the *2-pole* subclass by using a wye-star transformation. Some Flexible Alternate Current Transmission Systems (FACTS) devices like UPFC can also be modeled through this concept [14].

All the technical parameters of the power system devices are stored in attributes. These attributes include location, economical data, and the set of emission factors.

### 4.2 Hydro Database

Catchment models that are very important in hydrothermal power systems can be incorporated as an additional OO class hierarchy. The set of classes that compound the hydro database (HDB) is depicted in the hierarchy class of Figure 5. With it, it is possible to model the hydrographic basin or catchments involved in hydro generation in a simplified way. An inflow of water in a natural regime is characterized by the "natural inflow" class, so objects of this kind usually stand at the head of a basin. The "hydro unit" constitutes a decision or an action taken over the water flow, a decision that is specialized in child classes. From the connectivity point of view, the "natural inflow" objects have one output and the "hydro unit" has one input and two output attributes, while the connection between input–output pairs is performed by a "link" object. Following the hierarchy, the "hydro unit" is split into three classes to implement the hydrothermal coordination modeling. While a "series unit" allows full connectivity and could be associated to an network database (NDB's) "generator", an "isolated run of the river" can only receive water from a "natural inflow" and must be associated to a "generator". On the other hand, the "irrigation constraint" class represents extractions from a river course with irrigation purposes, so neither can be related to electrical generation nor can the extractions be the inflow of another object. A more specialized class is the "reservoir unit", which adds to

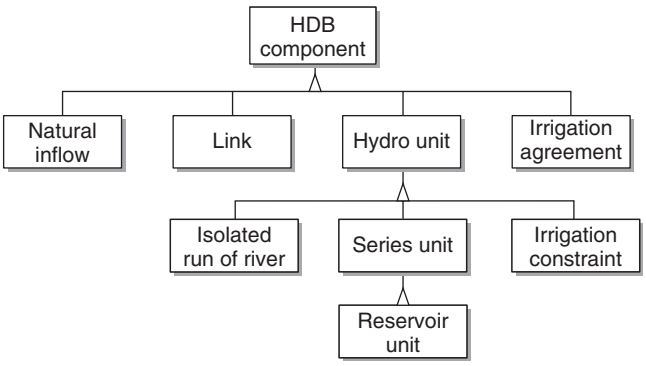



**FIGURE 5** Hierarchy chart of the hydro database (HDB).

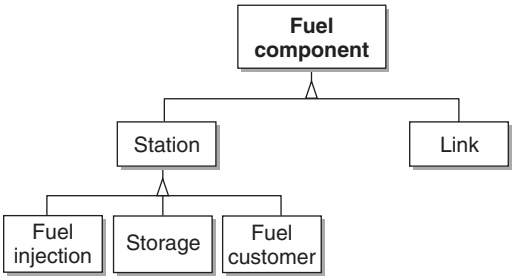



**FIGURE 6** Hierarchy chart of fuel network classes.

the "series unit" the capability to store water attributes. Finally, an abstract class "irrigation agreement" has been created to include a set of rules that comprise water use rights. An "irrigation agreement" object usually restricts the administration of reservoirs and drives the extractions of "irrigation constraint" based on information such as reservoir storage height, period of the year, and caudal measurements at predefined basin points.

### 4.3 Fuel Network Classes

The hierarchy chart of the fuel network classes is shown in Figure 6. Two abstract classes and four final subclasses represent the whole network. A fuel injection system, a storage system, and a customer system can be generalized in a *station* class with common attributes like position and capacity.

A *fuel injection* subclass manages simultaneously different fuel sources in the network. This model can handle 27 different fuel types such as crude oil, city gas, liquefied petroleum gas (LPG), natural gas (NG), gas oil, gasoline (81, 86, 91, 93 lead and unlead), different diesel types, and petcoke.

A *storage object* subclass manages just one of the fuel types. It keeps an initial, current, and final state of stored volume. A more realistic model of a storage can be built with several storage objects.

A *fuel customer* subclass is characterized by the type and amount of each fuel. It can manage simultaneously all possible fuel types coming from the fuel stations.

The *link* represents a union element between two *station* objects. The main attributes are the fuel type, the capacity, and length. Additional *links* are differentiated by the transportation mode of the fuel: pipeline, train, truck, and ship.

### 4.4 Transportation Network Classes

The hierarchy chart of the transportation network classes defines an *arc* and a *generic node* class. The generic node is further specialized into two classes called *node* and *centroid*, as shown in Figure 7.

For transportation networks, a first conceptual separation between urban and interurban networks must be made [15]. A strategic planning study with a national coverage must include an interurban traffic representation. Therefore, in the context of the proposed model, a *centroid* is associated with a conurbation or a vast urban area around and including a large city. The transportation activity of a *conurbation* is stored in attributes,

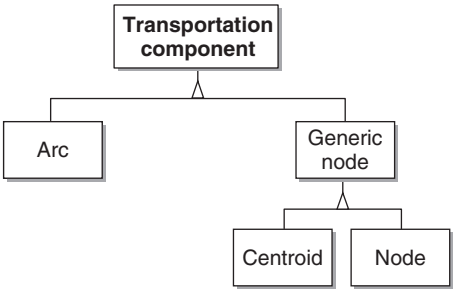



**FIGURE 7** Hierarchy chart of transportation network classes.

which register the number of attracted and generated travels, the rate of growth, and other relevant parameters.

The *node* component intends to represent only bifurcation and convergence points of transportation ways (with or without population). A *node* either generates or attracts travels. The transportation ways are modeled through a generic class called *Arc*, considering only one-way travels. *Arcs* define capacity, flow, length and speed for each of the following transportation modes: train, electric train, light vehicle, bus, heavy duty vehicle, ship, and plane.

### 4.5 Objects Relationship

One of the main objectives of the proposed modeling is to capture the interdependencies among different sectors. This is accomplished easily by using the classes of each OOP database (power, fuel, and transportation). In fact, a direct relationship between objects, from different databases, occurs through references to objects in the OOP. These references, as shown in Figure 8, are given as attributes, of the individual classes. Let us see some examples:

- A combined cycle generating plant is represented as a NG customer in the fuel network.
- Electricity consumption of arcs, centroids, injections, and links of the transportation network are represented by loads in the electric power network.
- Fuel consumption, resulting from the activity of centroids and arcs in transportation networks, is represented by customers in the fuel network.

In the case of HDB, hydro units processed water is electrically generated by generators and/or network feeders from NDB.

These references define information that is directly available to objects. Thus, the fuel customer "knows" the electrical behavior of a generator, the electrical load "*knows*" the energy consumption of an oil refinery, and so on.

## 5 INFORMATION PLATFORM

On the basis of the preceding models, the PIET (an acronym in Spanish for Transportation and Energy Information Platform) software was developed using Java technology

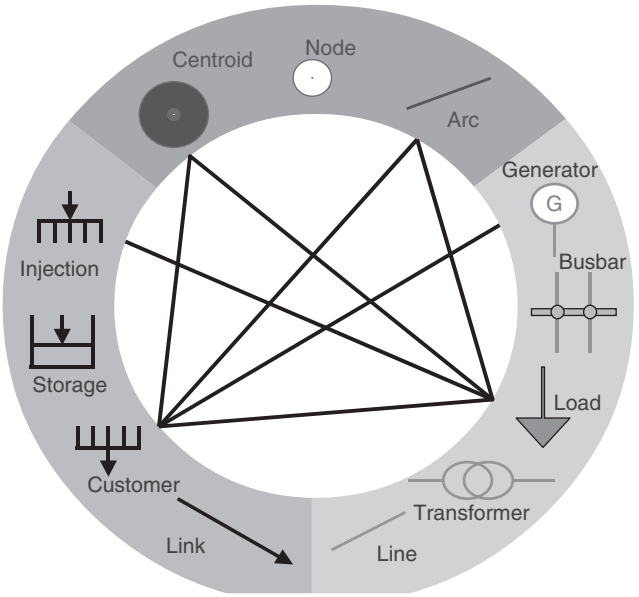



**FIGURE 8** Physical relationship between objects.

(Fig. 9) [10].[1] The OO database (server), which is required by the rest of the platform components, constitutes the core of the application. Source-file and specific power, fuel, and transportation editors allow user interaction with the system information and options.

The gray arrows represent the transmission of required services from clients to their respective servers and the black arrows represent data exchange flows. The design deals with critical aspects of the data management requirements for commercial software and energy companies by building a bridge to existing databases in different source/data file formats.

## 6 SCENARIO DESCRIPTION

The proposed model has the ability to generate, simulate, and analyze global potential scenarios. In this work, we define scenario as a "case study", expressed in words and numbers, about the way future events and the alternatives can develop. Although uncertainties dominate what really will happen, it is possible to write interesting and believable histories regarding the future.

The generation of a scenario usually involves the following steps:

- Defining the limit of space analysis (global, regional, etc.), thematic (sectors to cover, etc.), and temporal (time horizon).
- Describe the current economic, demographic, environmental, and institutional situation.
- Incorporating the driving and conditioning forces of the system and sectors.

[1]The final code (around 400 classes) runs efficiently on a Pentium IV computer with 512 MB RAM.

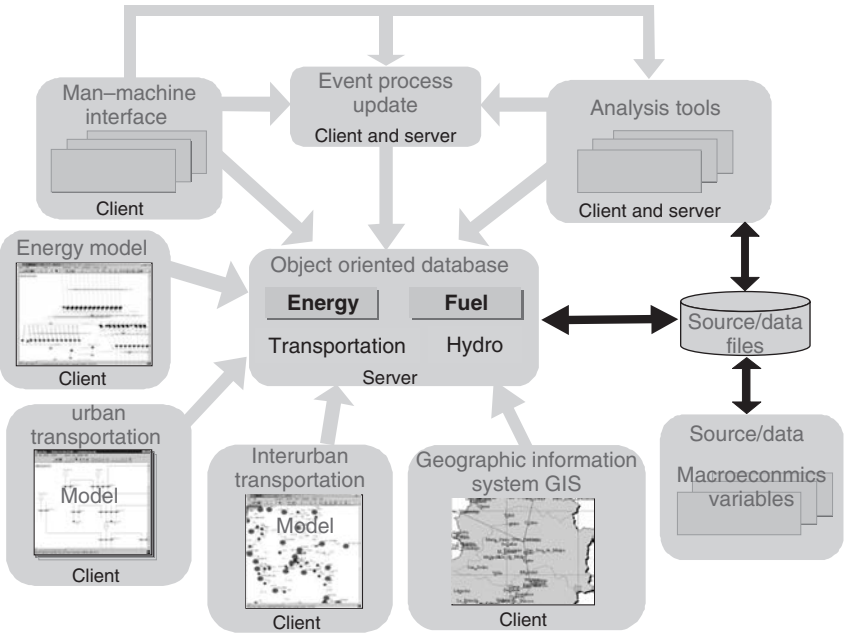



**FIGURE 9** PIET client-server architecture.

- Setting up a narrative that gives the context to the scenario. Often quantitative indicators are used to point out certain aspects.
- Drawing an image of the future. This involves specifying conditions and constraints for one or more points in the time horizon.

The outcome of this procedure is the definition of the following variables: demography, economy, social variables, culture, technology, environment, structures of administration (governance), and infrastructure. These variables work as the entry parameters defining a scenario in PIET. In practical terms, the OO design of PIET allows the following four ways to configure scenarios:

1. Through a direct linking with a *support model*. Support models, refers to those tools (computational programs, rules, databases, etc.) that allow the definition of a scenario. This can be a specific model usually used in the sector (i.e. transportation, energy, or environment) that can provide directly the information for the operation of the PIET.
2. A second alternative is through the use of *activity models* to obtain specific values for variables or entrance parameters to PIET. An example of an activity model is the calculation of fuel price profiles and deviations for a given scenario.
3. By using directly PIET dialogs and frames, that is, objects, system, and tools attributes.
4. Finally, structural changes in networks (for example, the expected generation expansion plan) can be incorporated in PIET by using the respective Editor. Typically it consists of drawing new objects in the networks.

Once the scenario has been incorporated into PIET, specific activity models for each network are run in order to obtain the quantification of interdependencies and the emissions of the scenario. The following studies can be carried out with PIET:

- fuel price variation effects;
- new technology impact;
- effects on energy sector produced by an efficient use of the transportation network;
- identification of network capacity constraints (critical expansion sectors);
- map with possible locations for power plants.

## 7 CASE STUDY EXAMPLE

For a validation of the proposed model, PIET was applied to Chile including the whole national territory. In this case, the hydro network was not considered.

### 7.1 Physical Chilean Networks

The Chilean mainland territory covers an area of 750,000 $km^2$ with a population of nearly 16 million. Chile has a market-oriented economy characterized by a high level of foreign trade. As a consequence, the electric, fuel, and transportation infrastructure come mainly from private investors. The electricity production was 39.577 billion kWh in 2000, which comprised fossil fuel (51.17%), hydro (46.36%), and others (2.47%). The transmission system, conformed by two main interconnected systems, includes voltage levels up to 500 kV.

NG is imported from neighbor countries using a pipeline system, while fuel and coal arrive in ships from different countries. In summary, the fuel network encompasses a pipeline system of crude oil (755 km), petroleum products (785 km), and NG (320 km).

In the transportation sector, all transport services are privately owned and/or operated with the exceptions of the interurban passenger trains and the urban railroad (Metro). Overall, the railroad system has 6702 km of railways, including 2831 km of broad gauge (1317 km electrified), 117 km narrow gauge (28 km electrified), and 3,754 km of meter gauge (37 km electrified). The highway system covers 79,800 km.

Because of data availability and geographical features of the country, the territory information is described at a province level by 51 zones. Nevertheless, major projects in any network, for example, a new mining site or a new combined cycle unit, are modeled explicitly in the networks (new objects).

In summary, as shown in Table 1, the modeling into PIET of the previous described networks (power system, transportation, and fuel network) can be translated in a collection of 1927 objects: 1127 objects are defined for representing the transportation sector, 492 for the electric sector, and 308 for the fuel network.

### 7.2 Network Dependencies

Network dependencies can be classified into two main categories: activity and physical dependencies.

On the one hand, the activity of each network—annual flow (vehicle·km/year) in transportation, annual energy (MWh/year) in electricity sector, and annual consumption

**TABLE 1 Objects in the Chilean Case**

| | |
|---|---|
| **Power system network** | |
| Number of nodes | 103 |
| Number of lines | 106 |
| Number of transformers | 39 |
| Number of generators | 42 |
| Number of loads | 202 |
| Total | 492 |
| **Transportation network** | |
| Number of centroids | 272 |
| Number of nodes | 183 |
| Number of arcs | 672 |
| Total | 1127 |
| **Fuel network** | |
| Number of fuel injections | 20 |
| Number of fuel storages Centers | 0 |
| Number of fuel links | 257 |
| Number of fuel customers centers | 31 |
| Total | 308 |

(barrel/year or ton/year) in fuel and NG—in the case of Chile can be related with a common set of economic indices. These indices are as follows: gross domestic product (GDP)/year for each province, international and domestic fuel prices, fuel taxes, population (inhabitants/province), and average income. These indices simultaneously shape the behavior of each network.

On the other hand, several physical interactions among the different networks are detected. A diagram with the main physical interdependencies among the networks in the Chilean territory is shown in Figure 10.

Figure 10 shows that in the whole Chilean territory, there are 133 links among electric, fuel, and transportation networks. As these links are geographically referenced, this information is useful for many purposes such as mapping of pollution in zones, energy consumption, available transfer capabilities of lines, pipelines, and so on.

The national power network is further divided into two main interconnected systems covering the north (Spanish the Northern Interconnected System (SING) with 800 km length) and the central part of the territory (Spanish the Central Interconnected System (SIC) with 2000 km length). As stated before, a major advantage of this representation is that it can be used for planning studies. For example, a new power plant may be drawn in the editor and the impact of this new project is seen inside the power grid and in the fuel network that will provide oil or NG for that plant. In addition, the pollution that this new project will produce will be displayed accordingly.

### 7.3 Specific Activity Models

On the basis of the studies carried out by the government and independent institutions, activity indices and physical dependencies are estimated for each year in the time horizon. A specific activity model is developed for each network.

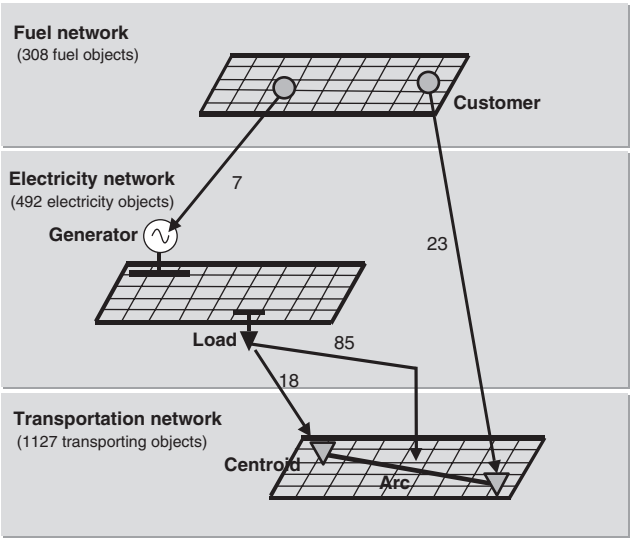



**FIGURE 10** Diagram with links among sectors.

***7.3.1 Power Systems.*** A multinodal, multireservoir dynamic stochastic model, with monthly stages and a time horizon of 10 years is used. Energy production and fuel consumption of each generating unit and their related emissions are obtained. The active power flow pattern for peak demand is computed [10].

***7.3.2 Transportation.*** It consists of two interrelated models. The first model encompasses urban transportation, that is, it renders the annual flow (vehicle·km/year) for each transportation mode (train, electric train, light vehicle, bus, and heavy duty vehicle) in any centroid (conurbation in a province).

Most methodologies of calculating urban transportation emissions are based on emissions factors and operational parameters that represent real-world traffic conditions [15–18]. The emissions factors represent emissions of each pollutant as a function of vehicle speed under normal traffic conditions. These factors are obtained experimentally with transient tests conducted on chassis dynamometers with a representative sample of technologies, vehicle types, and driving patterns [19–20]. Operational parameters are a function of link flow densities, average speed, and activity levels measured in kilometer per year per vehicle. These operational parameters are normally obtained from strategic transportation models, traffic surveys, and vehicle fleet databases [20]. However, for long-term and large-scale strategic studies, the data collection and parameter calibration components of these emission estimation methodologies are highly time consuming.

The second model represents the interurban transportation, which estimates the total flow between centroids for each transportation mode. This is a synthetic model that combines generation, distribution, and modal partition in one single stage. Mathematically, it corresponds to an econometric polynomial model.

The total vehicular activity associated with passengers is estimated through a two-stage sequential model that should reach a system-wide equilibrium: generation-attraction (G-A: stage 1) and joint distribution-modal split (D-M: stage 2). Separately, the freight movement is modeled with a direct demand model that simultaneously calculates the trip

generation, distribution, and mode choice. The assignment stage in both cases is carried out by a shortest path algorithm on the interurban network.

Because data from Chile is available at the province level, the models are specified at the province level. A province is a subdivision of a larger area called a *region*, and Chile is made up of 15 regions

***7.3.3 Fuel Network.*** Fuel consumption is determined by using existing historical data, which is used to adjust a logarithmic model to the activity indices.

## 7.4 Results

A scenario with an electric growth rate of 7%, for years 2003 and 2004, and 8% from year 2005 to 2011, considering hydro and thermal technologies in generation is presented in Figure 11. The scenario of Figure 11 is built under the assumption that no new hydro projects are carried out. Accordingly, the increase in demand is satisfied mainly by NG generating units.

Simultaneously, the fuel network activity model detects the expected capacity requirements for the pipeline infrastructure. As a consequence of this development, expected emissions increase in the system as shown for the NO$x$ case in Figure 12.

A summary of the urban transportation activity for the main provinces of the Chilean territory in the year 2002 is shown in Figure 13 to show the geographical capability of the model.

The corresponding emissions (ton/year) of the transportation activity for MP, NO$x$, HC, and CO are shown in Figure 14.

From Figure 14 it can be seen that Cachapoal, Iquique, and San Antonio provinces have high degrees of CO emissions, which can be related with public transportation (Fig. 13). This suggests that CO and NO$x$ mitigation could be achieved by converting the public transportation technology, for instance, to electric vehicles for the whole public

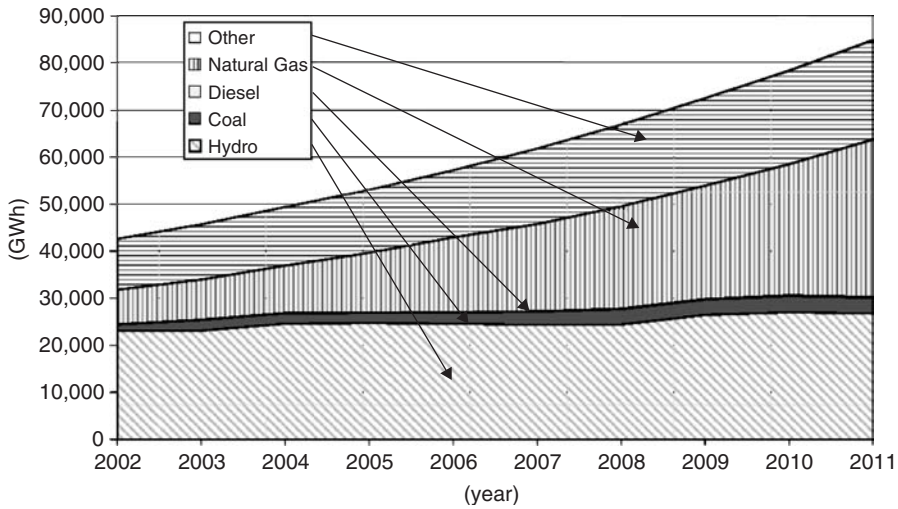



**FIGURE 11** Annual energy by technology [GWh].

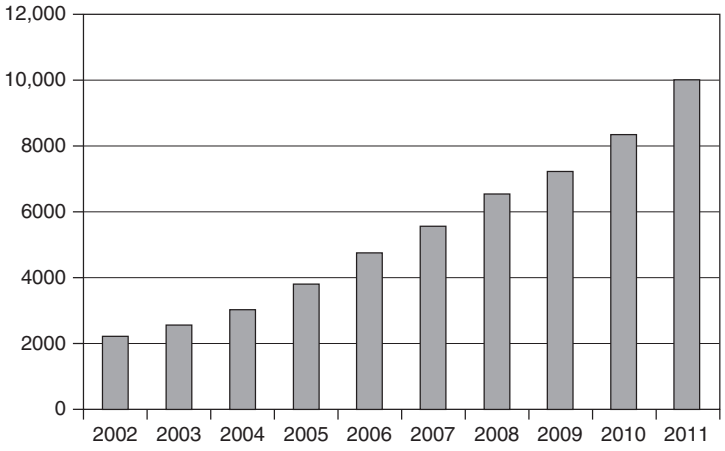



**FIGURE 12** Annual NO*x* emission in power network [ton/year].

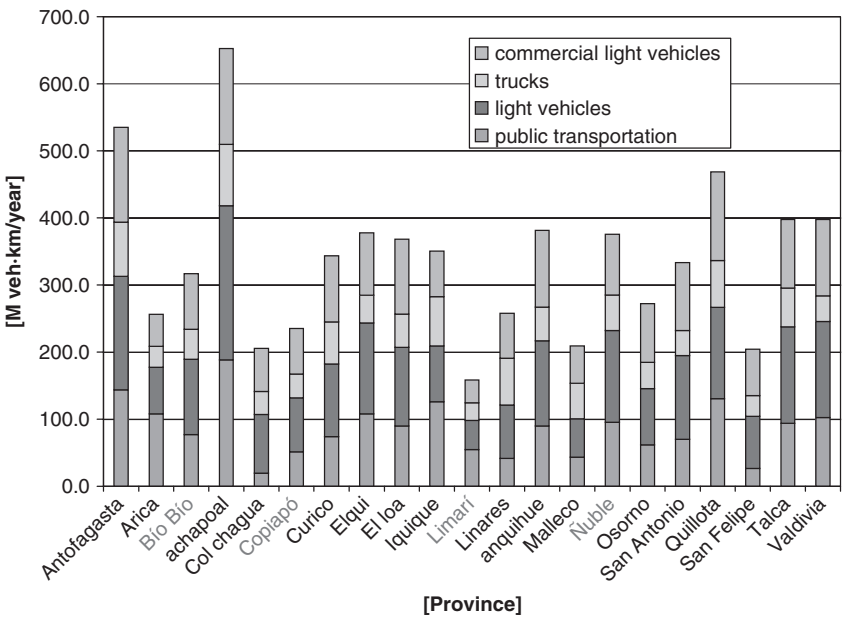



**FIGURE 13** Transportation activity in year 2002 by technology [M vehicle·km/year].

transportation system. The impact of these changes in the electric and fuel networks is summarized in Table 2.

Rows 1–3 of Table 2 show the base case information for provinces Cachapoal, Iquique, and San Antonio in year 2002. In these provinces, the public transportation activity is entirely diesel based (39 $\times$ 106 ga/year). After the proposed change, diesel consumption is replaced by electric energy, which means an important increase in NG consumption in combined cycle units. In fact, a new combined cycle unit is necessary (400 MW). The conversion scenario achieved a dramatic reduction in CO emission of 89%. In addition,

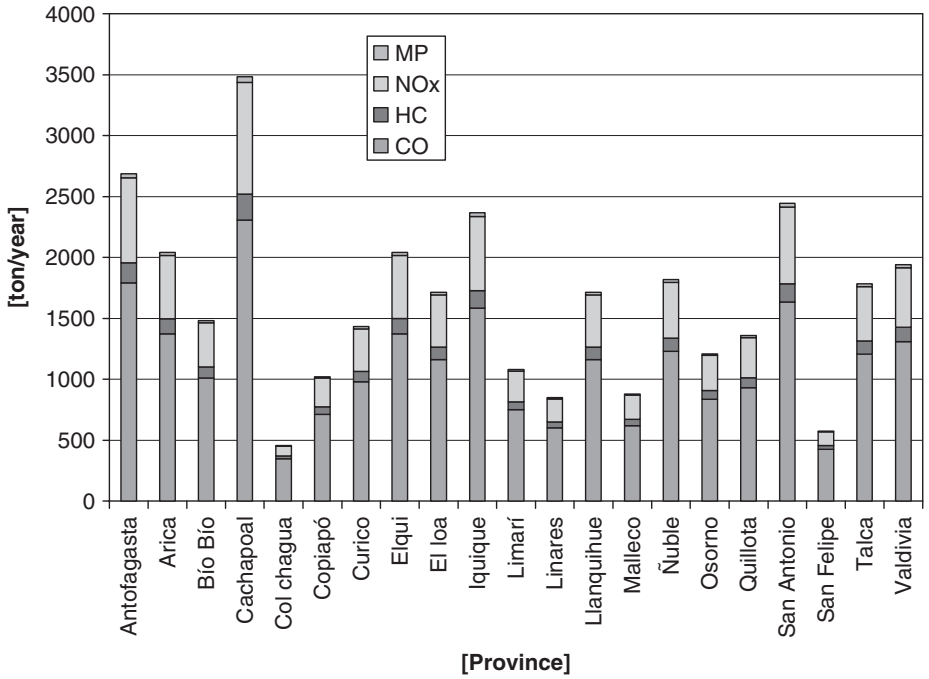



**FIGURE 14** Transportation emissions in year 2002 [ton/year].

**TABLE 2 Public Transportation Technology Conversion**

| | |
|---|---|
| **Provinces information (base case 2002)** | |
| Public transportation activity | $446 \times 10^6$ vehicle km/year |
| Diesel consumption | $39 \times 10^6$ ga/year |
| **Energy balance after conversion** | |
| Natural gas consumption | $+1716 \times 10^6$ $m^3$/year |
| Electric energy generation | +6460 GWh/year |
| **CO and NO*x* balance after conversion** | |
| CO emissions | −4529 ton/year (−89%) |
| NO*x* emissions | −107 ton/year (−5%) |

PIET shows that existing NG pipeline system supports the new requirements without new investments.

## 8 CONCLUSION

The OOP approach is useful to perform analysis of energy and transportation networks in the context of strategic planning. OOP and Java technology allow both flexible scenario definitions and a friendly GUI. Thus, a platform like PIET is flexibly adapted as a server

structure for the development of several analysis tools. Ongoing research is focused on identifying critical requirements for the energy and transportation infrastructure, and the improvement on activity models for each network and their relationships.

## REFERENCES


1. Cole, M. A., and Neumayer, E. (2004). Examining de impact of demographic factors on air pollution. *Popul. Environ.* **26**(1), 5–21.
2. Alson, J., DeCicco, J., Delucchi, M., Greene, D., Johnson, L., McNutt, B., Patterson, P., Santini, D., Sperling, D., and Turrentine, T. (1999). Transportation energy and environmental policy for the 21st century, Asilomar Conference Center, Monterrey, California, pp. 24–27.
3. Delucchi, M. A. (1991). *Emissions of Greenhouse Gases from the Use of Transportation Fuels and Electricity 1*, Center for Transportation Research, Argonne National Laboratory, Argonne, IL. ANL/ESD/TM-22.
4. EIA (2007). Annual energy outlook 2008 with projections to 2030 (Early Release), Report #:DOE/EIA-0383(2008), December 2007.
5. Zografos, K. G., Madas, M. (2003). Optimizing intermodal trip planning decisions in interurban networks, *Proceedings of the 82nd Annual Transportation Research Board Meeting*, January 12–16, 2003, Washington, DC.
6. Handschin, E., Heine, M., König, D., Nikodem, T., Seibt, T., and Palma, R., (1998). Object-oriented software engineering for transmission planning in open access schemes. *IEEE T. Power Syst.* **13**(1), 94–100.
7. Palma R., Moya, O., and Vargas, L. (2001). Object-oriented simulation software for a competitive environment—application to transmission expansion planning, *The First EPRI Latin American Conference & Exhibition: Toward a Mature Electricity Market Through Technology, R&D, and Business Vision*, *Rio de Janeiro*, Brasil, 28–30 November, 2001.
8. Department of Energy—DOE , White House Office of Science and Technology Policy-OSTP (2000). Workshop on Infrastructure Interdependencies Research and Development Workshop, McLean, IL, June, 2000.
9. York, R., Rosa, E. A., and Dietz, T. (2003). STIRPAT, IPAT and ImPACT: analytical tools for unpacking the driving forces of environmental impacts. *Ecol. Econ.* **46**(3), 351–365.
10. Palma, R., Vargas, L., Flatow, F., and Oyarce, N. (2003). Object oriented platform for an integrated analysis of energy and transportation networks. *IEEE T. Power Syst.* **18**, 1062–1069.
11. Rumbaugh, J., Jacobson, I., and Booch, G. (2004). *The Unified Modeling Language reference manual*, 2nd Ed. Addison-Wesley Professional, Boston, Massachusetts, ISBN: 0321245628.
12. UML Resource Page of the Object Management Group (2008). *Resources that Include the Latest Version of the UML Specification*. Available at http://www.uml.org/.
13. Foley, M., Bose, A., Mitchell, W., and Faustini, A. (1993). An object based graphical user interface for power systems. *IEEE T. Power Syst.*, **8**(1), 97–104.
14. Palma-Behnke, R., Vargas, L. S., Pérez, J. R., Núñez, J., and Torres, R. A. (2004). OPF with SVC and UPFC modeling for longitudinal systems. *IEEE T. Power Syst.* **19**(4), 1742–1753.
15. Lyons, T. J., Kenworthy, J. R., Moy, C., and Dos Santos, F. (2003). An international urban air pollution model for the transportation sector. *Transport. Res. D-Tr. E.* **8**, 159–167.
16. Sharma, P., and Khare, M. (2001). Modelling of vehicular exhaust—a review. *Transport. Res. D-Tr. E.* **6**, 179–198.
17. Zachariadis, T., and Zamaras, Z. (1999). An integrated modeling system for estimation of motor vehicle emissions. *J. Air Waste Manage. Assoc.* **49**, 1010–1026.

18. Corvalán, R. M., Osses, M., Urrutia, C. M., and Gonzalez, P. A. (2005). Estimating traffic emissions using demographic and socio-economic variables in 18 chilean urban areas. *Popul. Environ.* **27**(1), 63–87.

19. Ntziachristos, L., Samaras Z., Eggleston, S., Goriben, N., Hasse, l. D. Hickman, J., Joumard, R., Rijkeboer, R., and Zierock, H. (1999). *Computer Programme to Calculate Emissions from Road Transport, COPERT III. Methodology and Emission Factors*. European Environmental Agency. European Topic Centre on Air Emission, Thessaloniki.

20. De Cea, J., Fernández, E., Dekock, V., Soto, A., and Friez, T. (2003). ESTRAUS: a computer package for solving suplí-demand equilibrium problems on multimodal urban transportation networks with multiple user classes, *Proceedings of Transportation Research Board Annual Meeting*, Washington, DC, January 2003 (CD-ROM).

## FURTHER READING

Bakkes, J. (2000). Global Dynamics and Sustainable Development Programme, RIVM Report no. 402001018, October 2000.

# GEOSPATIAL DATA SUPPORT FOR INFRASTRUCTURE INTERDEPENDENCIES ANALYSIS

ANTHONY F. ADDUCI, SCOTT D. BAILEY, AND RONALD E. FISHER
*Argonne National Laboratory, Argonne, Illinois*

## 1 INTRODUCTION

Geospatial data provide a unique and rich source of information on the distribution of both environmental and man-made assets and reveal specific themes of the earth's surface. Such data are an element in almost all public decision-making processes [1]. Nonspatial data provide key attributes, such as the facility owner, size, and operational information, that augment geospatial data and provide additional insight for analysts. Geographic information system (GIS) and other visualization technologies are optimal solutions for displaying geospatial and nonspatial data. By providing a user-friendly, yet powerful, framework to quickly display data in varying layers at a variety of zoom levels, GIS presents a wide range of unique capabilities, such as thematic mapping, data overlay and synthesis, network analysis, geospatial modeling, and visual data exploration. Thus,

the use of geospatial data and GIS are essential to the analysis of the many components that make up critical infrastructures and key resources (CIKR).

## 2 TECHNOLOGY OVERVIEW

Infrastructure interdependencies are complex to identify and analyze because of the vast infrastructure components that are involved and the complex interactions among them. (GISs) and other visualization technologies provide innovative ways to identify and analyze infrastructure interdependencies because they give analysts the ability to overlay, zoom, pan, query, and manipulate geospatial and nonspatial data sets. These techniques also allow analysts to view infrastructure for any selected area, to determine its criticality to other infrastructures, and to identify and quantify interdependencies, such as proximity, connectivity, common corridor sharing, etc.

Computer and software advancements have greatly enhanced the area of geospatial visualization technology used in infrastructure interdependency analysis. Several types of tools are available to analysts, including stand-alone GIS, shared GIS, Web-based GIS, open source GIS, three-dimensional (3D) visualization, aerial imagery, and aerial flyover. Each of these tools offers unique advantages in the analysis of infrastructure interdependencies. They are described below.

- *Stand-alone GIS.* Although GIS capabilities have been available for many years, it has been only since the mid-1990s that GIS has been part of the mainstream. In the past, GISs were predominantly housed on Unix workstations, and data were limiting and expensive. However, rapid advancements have made GIS available on the personal computer (PC). As software capabilities have increased, data sets have become more readily available and less expensive. Furthermore, GIS has become much more user-friendly. Once, only trained geographers were able to apply GIS technologies, but now, nontechnical users can use GIS software. Today's GIS market includes several vendors, such as Environmental Systems Research Institute (ESRI), MapInfo, Intergraph, and Autodesk. Additionally, Microsoft has a GIS product called *Microsoft Streets and Trips*, and several global positioning system (GPS) units come with GIS software (i.e. DeLorme).
- *Shared GIS.* As the quantity of GIS data has increased so has its user base. Shared GIS applications became available that allowed for shared licensing among users and shared systems to house software and data. This development opened the door to an expanded group of users, especially those who do not use GIS enough to acquire their own licenses or who do not have the PC requirements to support these systems. Subsequently, this development led to the expansion of Web-based GIS, which will be addressed in the next section. Information about three examples of shared GIS products is provided in the following paragraphs.

  ArcIMS is a server-based GIS developed by ESRI that allows users to create, publish, and share maps over the Internet or within an organization. This product provides GIS access to users that do not have stand-alone GIS. Once the final product is published, it is available on the Internet and is accessible to numerous users. With ArcIMS, the end user can interactively view a map and have the ability to zoom, pan, identify layer attributes, and find and turn layers on and off. ArcIMS can be useful, particularly for infrastructure analysts who are knowledgeable in a

particular field, but do not have an extensive background in GIS that is required to operate most GIS software.

ArcGIS server is a more advanced server-based ESRI product. Like ArcIMS, the primary function of this tool is to deliver GIS data and maps to customers or clients using a browser-based environment. ArcGIS server is more advanced than ArcIMS because it provides users with not only the ability to publish interactive maps, but also the ability to publish more functionality, such as advanced geoprocessing, 3D visualization, and more enhanced analysis options. Users do not need to have expensive stand-alone GIS to perform analysis or previous experience with GIS to use this product. With ArcGIS server, users can create user-friendly and self-explanatory maps and tools, which are especially useful in the field of infrastructure analysis because they allow infrastructure analysts to have access to GIS functionality without possessing the software or extensive GIS knowledge.

GeoPDF by TerraGo is another example of a shared GIS product. GeoPDF provides GIS capabilities to anyone with access to Adobe Reader. Users can view GIS-produced maps and coordinates, pan, zoom, identify features, obtain attribute information, measure distances, and turn data layers on and off. The functionality of this product is not as advanced as ArcGIS server, but it is the easiest to use of the three examples of shared GIS products. The GeoPDF file is originally created in a GIS environment and there is a fee for the software license, but viewing a GeoPDF document is of no cost to the end user. The main advantage of this tool is that users can create interactive maps for other infrastructure analysts who do not have access to costly GIS software but can readily access widely used Adobe products.

- *Web-based GIS.* As web site capabilities expanded, GIS became a mainstream application for web site developers. Many sites, such as Geography Network, GeoComm, iMAP, Mapserver, United States Geological Survey (USGS) seamless site, and Google Earth, now offer key services that use Web-based GIS technologies as their backbone. Google Earth, for example, is a free service that offers a limited but useful range of GIS capabilities that are not as powerful as stand-alone GIS end products, but are still powerful and highly useful. The capabilities of Web-based GIS are combining various infrastructure layers with high resolution aerial imagery, terrain, 3D buildings, the ability to search for locations using GPS coordinates or keywords, and Keyhole Markup Language (KML) capabilities. KML is an XML language that allows users to view geographic data on Google Earth and web browsers. Other sites also include GIS capabilities that have become commonplace. For instance, numerous web sites, such as Mapquest, Google Maps, and Yahoo! Maps, use geocoding to allow users to find site locations or to obtain driving directions to specific locations. Such Web-based GIS tools have greatly increased the number of developers and users of GIS technologies. The main advantages to these tools are the same as those listed above for stand-alone and shared GIS: infrastructure analysts do not have to purchase expensive GIS software to analyze geospatial data. Instead, interactive GIS web sites and applications allow users to perform limited GIS analysis and data manipulation at a lower cost.
- *Open source GIS.* In addition to the proliferation of GIS technology as a whole, there has been recent growth in the development and use of open source GIS tools, libraries, and standards. Many common GIS tasks can now be accomplished with free or open source software. The biggest advantage of open source GIS is that these tools are typically free to users and provide a source code that can be customized

and integrated with other tools. Additionally, nonproprietary and open data formats, such as the shapefile format for vector data and the GeoTIFF format for raster data, have been widely adopted. The Open Geospatial Consortium (OGC) protocols, such as web mapping service (WMS) and web feature service (WFS), provide protocols that further encourage the continued development of open source software, especially for Web and Web service oriented applications. Examples of open source GIS tools are BASINS, Demeter, Geocoder, GRASS, ImageMagick, libGRASS, MP2KML, and VGMap. These products contain various GIS capabilities, including image processing, 3D analysis, interpolation, and access to geospatial libraries. As open source GIS technology continues to mature, users will be afforded greater flexibility in analyzing infrastructure interdependencies and in linking GIS tools to other crucial analysis capabilities, such as modeling and simulation, visualization, and data mining.

- *3D visualization.* In the past, geographers were bound by the limits of technology and confined to two-dimensional (2D) views for analyzing geographic data. Three-dimensional modeling enables a real-world representation of geospatial data to interact with physical land feature data in terms of terrain and surrounding environment. A leading product in this area is ArcGIS 3D Analyst developed by ESRI [2]. Three-dimensional applications change the way analysts view geospatial data and allow users to view and analyze data in new dimensions, which greatly benefits the infrastructure interdependency analysis. Traditionally, users have been limited to static maps and forced to use their imaginations to visualize what a landscape, city, or terrain look like. With 3D tools users can view elevation, depth, buildings, terrain, and bathymetry, which are not easily discernible on static maps. Three-dimensional applications are powerful tools for interdependency analysis because they allow users to portray enhanced depictions of how relationships exist between various infrastructure assets.
- *Aerial imagery.* Aerial imagery is a key data source to GIS applications and visualization. Integrating relevant imagery with GIS technologies allows for additional visualization options previously available through only high-resolution maps, photographs, or site visits. Infrastructure analysts commonly use aerial imagery to validate and verify facility locations in relation to other infrastructure assets. Aerial imagery also increases the reliability of GIS data by allowing users to verify geospatial and nonspatial data.
- *Aerial flyover.* Aerial flyover, which provides users a bird's-eye view of the region of analysis, is available in applications, such as ArcGIS 3D Analyst and ArcView 3D Analyst. Such tools are useful in the presentation and representation of geospatial analysis as viewed from a perspective that was previously unavailable to analysts. Prior to the availability of aerial flyover, photographers were limited to using 2D maps and were forced to use their imaginations to visualize GIS work. Aerial flyover technology combines 3D capabilities with an aerial perspective similar to that from an airplane or helicopter. Recent advancements in the GIS field have brought this new tool to the forefront.

From an interdependencies perspective, the wide array of GIS tools available provides methods to

1. accurately locate facilities within a geographic region;

2. identify the critical infrastructure within that region;
3. visualize and quantify relationships between critical infrastructures; and
4. support infrastructure interdependencies analysis.

Table 1 summarizes the GIS tool types identified in this section; identifies the strengths and weaknesses associated with each tool type; and addresses the applications of each tool type to interdependency analysis.

## 3 GEOSPATIAL AND NONSPATIAL GAPS

As noted in the preceding section, many modeling and visualization tools are available to analysts, but without complete and accurate data, these tools are limited in their application. This problem became evident within the US Department of Energy's Visualization Working Group, which discovered the limiting factor to the visualization of the energy infrastructure was the lack of available geospatial and nonspatial data [3]. Although much geospatial data currently is available (e.g. highways, streets, waterways, rail lines), limited geospatial data exists on the energy infrastructure (e.g. oil and gas pipelines, electric substations). In some cases, geospatial data exists but lacks attributes, completeness, or sufficient accuracy for interdependency analysts.

Infrastructure interdependency analysis requires vast amounts of data across CIKR, as well as a high level of data fidelity. Data accuracy and precision are critical to problem solving and decision making in this field. Limitations include lack of required data (data gaps) and erroneous data, which include existing but misleading data. Geospatial data used for interdependency analysis often contain errors that are not always obvious to users, and some examples of geospatial data pitfalls are provided below.

Erroneous data are more difficult to identify than data gaps. Such data are not always misleading upon examination, because the specific limitations to the data set may not be clear. For example, a map reader may not be aware that newer streets are not included on a map and that some of the streets may be slightly off in their placement. The producer of the map may be aware of the flaws, but they are not obvious to the map reader. Errors in geospatial data are well documented in the geospatial community but are not well known to external users of the data. Goodchild states, "The process by which a geospatial database is created from a source map is complex, and error of various types is introduced at each step [4]." The larger the area involved, the more important the mapping errors due to projection become [5]. Many of the sources of error are due to the method and process of geocoding, which is the key component in processing geospatial data.

Many researchers have stressed the need to deal with issues of geospatial data quality, as the risk of misuse of geospatial data has greatly increased [6]. Significant causes of the enhanced risk of misuse include the increased availability of geospatial data, the greater possibility that the data have been manipulated, and a growing group of inexperienced users [7]. Furthermore, producers of geospatial data sets provide little information regarding the quality of their data [8]. Understanding errors and their propagation during data manipulation and processing is becoming one of the major issues in geospatial analysis [9]. If uncorrected, these errors can lead to erroneous interdependency analyses. For example, an infrastructure analyst studying shared right-of-way corridors may not correctly identify collocated infrastructures if the geospatial layers display infrastructure

**TABLE 1 GIS Tool Types for Interdependency Analysis**

| GIS Tool Type | Strengths | Weaknesses | Interdependency Applications |
|---|---|---|---|
| Stand-alone | Full GIS functionality | Software cost | Offers robust GIS capabilities for interdependencies analysis by GIS trained staff |
| | | Learning curve (GIS/data) | |
| | Extensive analytical geospatial tools and extensions | | |
| | | Requires significant digital storage space and high-performance computers | |
| Shared | Low cost | Limited functionality for end user | Provides basic GIS capabilities for use in interdependencies analysis with little or no background in GIS |
| | Ability to control end user functionality | | |
| | | Limited integration with other programs | |
| | Published products | | |
| Web-based | Ease of use | Limited geoprocessing functionality | Quickly provides data for critical facilities and surrounding areas for interdependencies analysis |
| | Low cost | | |
| | Readily available | | |
| | | Lack of metadata | |
| | Interactive | | |
| Open source | Low cost | Steep learning curve | Provides a solution for extending legacy interdependencies tools to include GIS capabilities |
| | Ease of customizing and integrating | | |
| | | Programming skills required | |
| 3D visualization | Specialized functionality | Increased computational requirements | Allows for correlating interdependencies attributes and gives users an improved perspective of infrastructure interdependencies |
| | Improved visual perspective | | |
| | | Access and ability to create 3D data | |
| Aerial imagery | Provides excellent insights and reference points | Large files and datasets | Allows users to quickly zoom to areas of interest and determine first-order interpretation |
| | | Availability and cost | |
| | Real-world perspective | Quality/resolution | |
| Aerial flyover | Interactive | Limited data coverage | Offers an excellent tool for viewing infrastructure dependencies and interdependencies |
| | Combines raster and vector data in a virtual environment | Increased computational requirements | |

assets miles apart due to data errors. The same can be true if infrastructure assets on a map show they are collocated when in reality they are miles apart. Thus, accuracy is critical to GIS interdependency applications.

Table 2 provides a list of five common errors made in geospatial data processing, including a description of each error and potential corrections. A sample map of each of the five errors is provided to illustrate its significance.

Figure 1 shows a typical error caused by the difference in the number of decimal places used in representing a facility's absolute location. An accurate absolute location (latitude/longitude) should include four to eight decimal places. Figure 1 shows two different locations for what should be the same site. One shapefile is built by using five decimal places and accurately represents the location of the Advanced Photon Source building at Argonne National Laboratory. Although the other point is supposed to represent the same facility, it is actually located one-half mile southeast of the correct location because the latitude/longitude fields were truncated from five decimal places to two. This type of error is quite common to GIS users because of either manipulation or lack of knowledge in the construction of the database.

GIS data inherently contain errors due to the wide range of variables involved in the data collection process. Infrastructure analysts should be knowledgeable about the source of the data they use and about how the data were obtained. A commonly used practice in the creation of geospatial data is the use of geocoding or address matching. This method assigns geographic coordinates to a data table based on nonspatial information, such as addresses or ZIP codes. In the GIS field, this is a quick, primitive, and simple method of designating a geographic point to a data set. This method is useful because a user can take a large amount of nonspatial information, for example, a Microsoft Office Excel spreadsheet, and produce a geospatially registered dataset. The GIS tool will quickly assign geographic coordinates $(x,y)$ to a data set based solely on the relationship between the address and the street or reference layer. Rather than placing a feature point directly on the actual facility, the GIS tool will place the feature point on the point of reference, which is, in most cases, a street segment. Thus, the geographic coordinates will always be located on a street adjacent to a facility or site if the reference data is a street layer, rather than on the site of interest. Although this method of site location is adequate for some purposes (e.g. driving directions), it could produce misleading results for infrastructure analysts.

For example, Figure 2 displays the Argonne complex and a red star produced by using street-referenced geocoding. The address provided by Argonne is the business office, which is typically used by large facilities. In this case, the business address is beyond the physical parcel boundary of Argonne's property and does not provide the most accurate location of the facility. A more useful absolute location for an infrastructure analyst would be the centroid of the facility, which is represented in Figure 2 by a green star. Furthermore, since the complex is comprised of many facilities located across several acres, the complex would be better represented by a polygon rather than a point. The yellow lines demonstrate the best way to represent the complex, that is, by outlining the boundaries. This process consumes more time because the boundary of the site needs to be determined, but for positional purposes, it is a superior method for representing location. However, geocoding points is easier than creating polygons; while geocoding provides an effective way to initiate the process of representing absolute location, it should not be the final method of site location if user of the data.

**TABLE 2 Five Common Errors Made in Spatial Data Processing**

| Figure | Common Error | Description | Correction |
|---|---|---|---|
| 1 | Numerical spatial data decimal places truncated | Original created data contained latitude and longitude values with a higher number of decimal places than the data used in map production. In this example, the original spatial information (latitude/longitude values) contained five decimal places, which were reduced to two. | Use the number of original decimal values derived from the original data collection to obtain the most accurate location of facility. |
| 2 | Exact site location identified with geocoding method | Street addresses are used to locate facility in geocoding. However, this method does not provide accurate site location due to its emphasis on address ranges rather than physical locations. | Use methods such as GPS, which use satellites for coordinate accuracy. Other methods include verification using imagery and Web-based programs. |
| 3 | Outdated imagery used in cartographic production | Outdated imagery is used to represent current geographic features within an area. In this example, a 1999 aerial photograph of the Millennium Park area in Chicago is used. In Figure 3a notice the evidence of construction taking place within the boundary of the site. | Use updated imagery, as shown in Figure 3b in cartographic production. In this imagery produced in 2005, signs of construction are no longer visible. Updated imagery allows for a better representation of the area under analysis. |
| 4 | Incorrect map projection applied to data for display | The incorrect map projection that renders a geographic region into its true shape was applied to the data in Figure 4. Using a projection that was not used in creating the data causes location inaccuracies that can be either severe or more locally distorted, depending on the spatial difference between the projections. | Investigate metadata associated with the dataset to verify and apply correct map projection. The green circle in Figure 4 represents data with correct map projection. |
| 5 | Data digitized at scale not optimal for region of analysis | A 1 : 50,000 scale of digitization was used to create road infrastructure in Fig. 5a. This scale produced inaccurate and distorted results, because the scale of the area being drawn (1 : 5,000, large scale) did not match the scale of digitization (1 : 50,000, small scale). | Match the scale of the area being analyzed with the scale of digitization to produce more accurate and precise results, as shown in Figure 5b. |

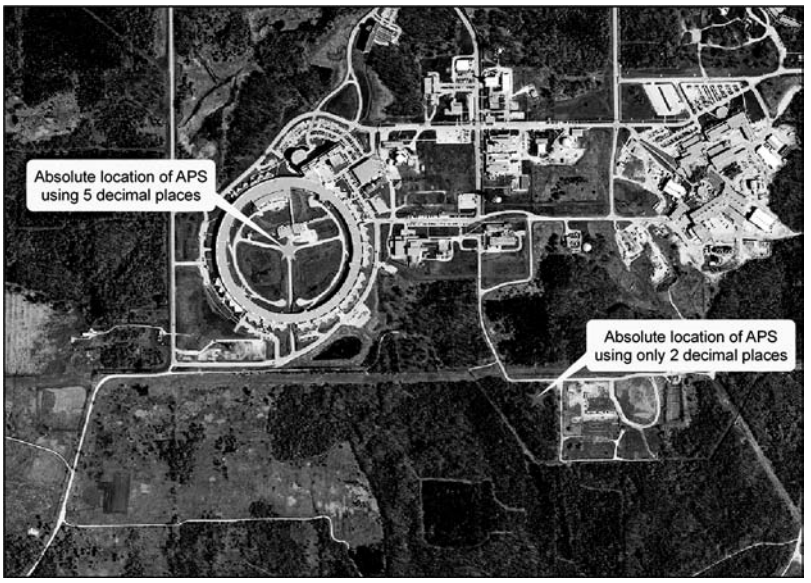



**FIGURE 1** Map example of error from truncating decimal places from five places to two places.

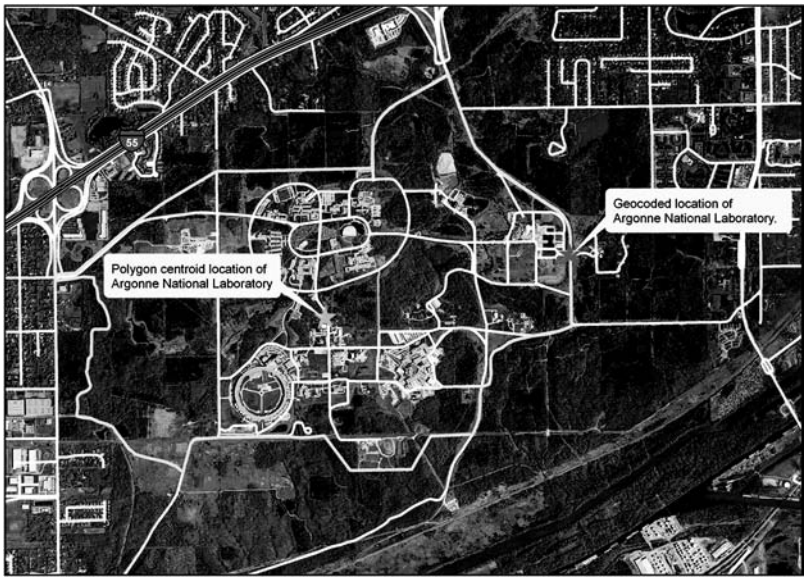
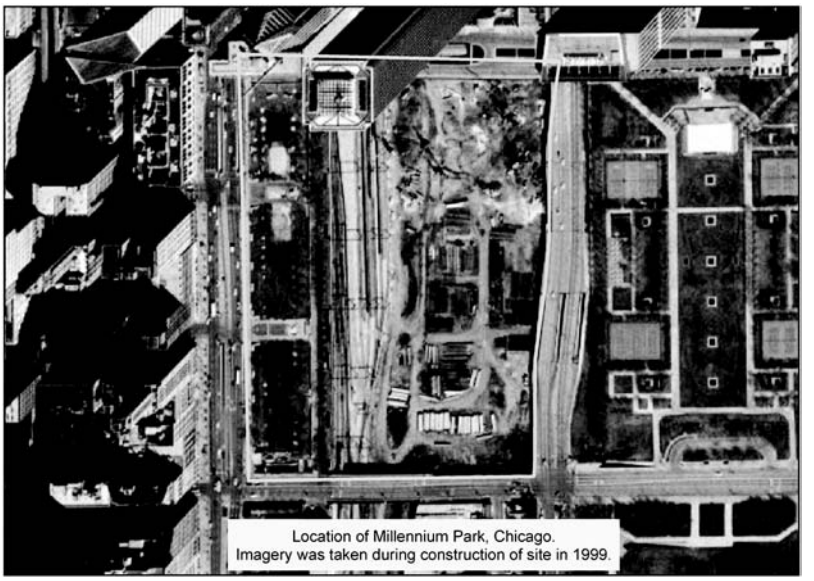
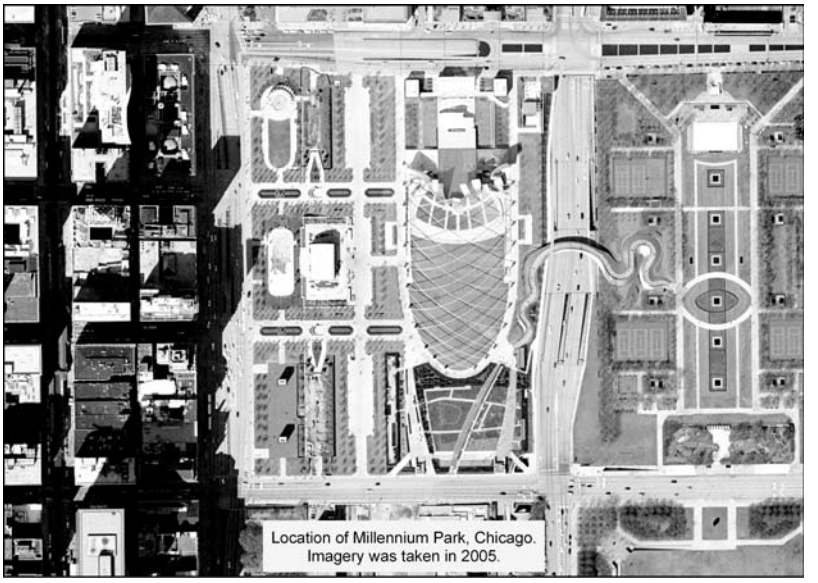



**FIGURE 2** Map example of error from geocoding.

Figure 3 represents a third pitfall shared by GIS users. Knowledge of the most recent available data is of utmost importance when it comes to visually displaying the location of a facility by using aerial imagery. Figure 3 shows two aerial photographs taken 6 years apart. Figure 3a represents the location from aerial photography taken in 1999, whereas Figure 3b represents the same location taken in 2005. The location is Millennium Park




(a)




(b)

**FIGURE 3** Map example of error from using outdated imagery.

in Chicago, IL, which was completed in 2004. The 1999 imagery does not accurately represent the current land use. Figure 3b, which is from the USGS seamless site, is a more appropriate choice of imagery for GIS purposes. This imagery allows for a more accurate site portrayal that will aid in a higher quality GIS analysis and cartographic production.

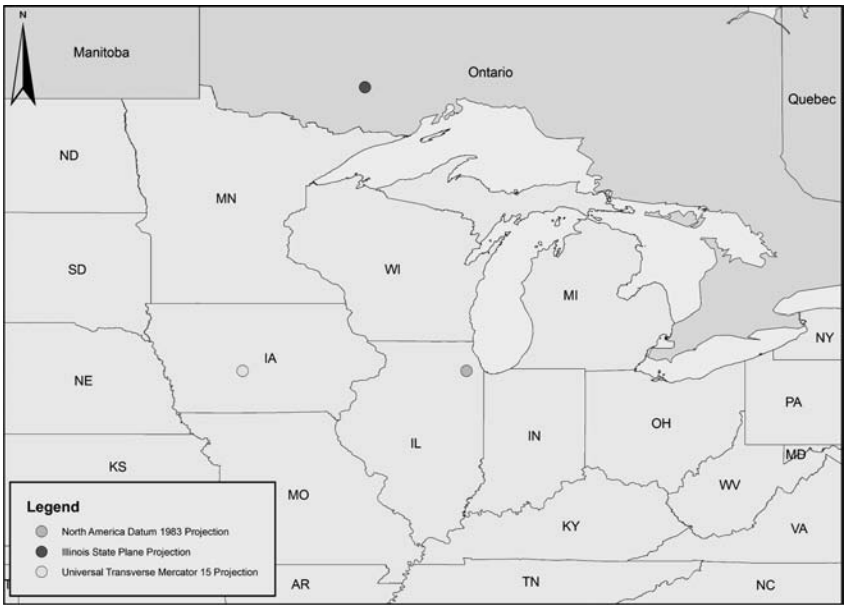


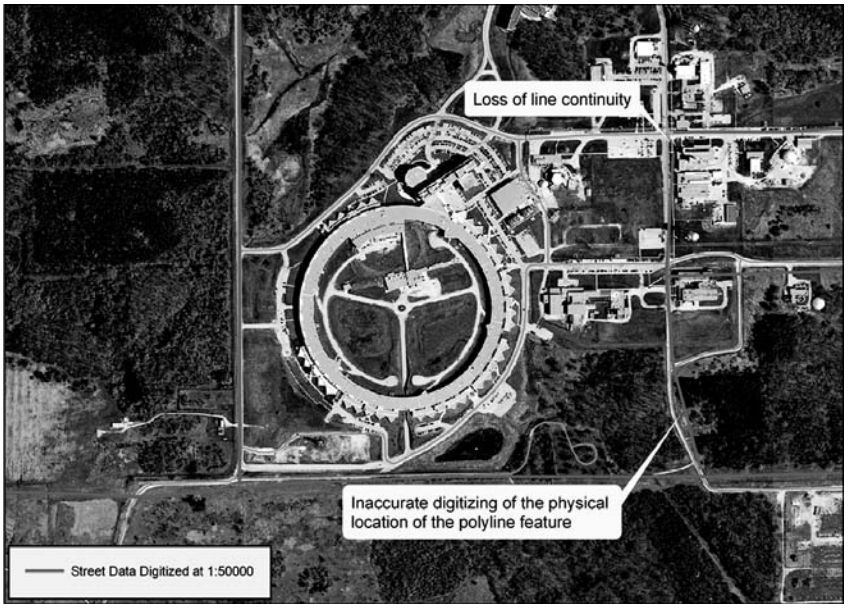

**FIGURE 4** Map example of error from incorrect map projection usage.

As previously discussed, differing map projections can lead to geospatial data errors. Figure 4 shows the same point represented by three different projections: the North American Datum 1983 projection, the Illinois State Plane Projection, and the Universal Transverse Mercator 15 Projection. If the projections are not converted to a common map projection, the same point and address place the point in Illinois, Iowa, and Canada. In this case, the inaccuracy results in a point hundreds of miles away, due to map projection error. As illustrated, differing projections, if not corrected, can lead to errors in facility identification and GIS analysis.

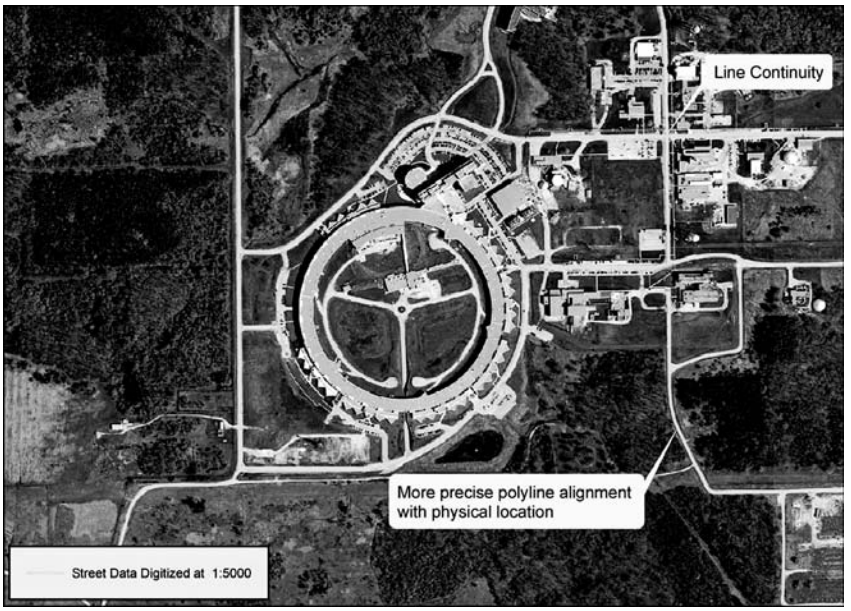
Figure 5 represents the final common error term—differing data scales. Figure 5a shows imagery at a 1 : 24,000 scale; the streets (represented in red) were digitized at a higher scale (1 : 500,000). The result is that the red lines do not correctly match the actual road locations. The red lines are coarse and do not capture all the curves in the road; and they are not continuous. Figure 5b shows imagery at a 1 : 24,000 scale; the streets (represented in yellow) were digitized at the same scale. The result is accurately placed and continuous lines. Thus, it is important to use consistently scaled data for the level of analysis being conducted.

## 4 METADATA GAPS

A major issue in GIS data consideration is the lack of or completeness of metadata. The term "metadata record" is defined by the Federal Geographic Data Committee (FGDC) as "a file of information, usually presented as an XML document, which captures the basic characteristics of a data or information resource [10]." The FGDC has developed a set of standards and guidelines for metadata, but these tools are often neglected during the production of GIS data. The objective of these standards is to provide users with a




(a)




(b)

**FIGURE 5** Map example of error from using differing levels of scale.

general set of terms and definitions for the documentation of digital geospatial data [10]. They were developed to be used by all levels of government and the private sector.

Data containing proper FGDC metadata are more legitimate in infrastructure interdependencies analyses than data that contain limited or no metadata at all, but having access to FGDC metadata does not guarantee that infrastructure GIS analysis is going to be of high quality. All GIS data have some type of error. The goal of the GIS or infrastructure analyst should be to use data with a minimized room for error and maximized accuracy. Available metadata give users the ability to assess data based on imperative information such as source, date, resolution, and method of collection. Properly created metadata guide the analysts in choosing data that will produce quality results and in turn, could lead to more effective decision making. Missing metadata may include the following:

- unknown organization/source/author of data;
- unknown method of data collection;
- unknown scale of data creation;
- unknown date of production;
- unknown projection and geospatial extent of data;
- unknown supporting data or web sites affiliated with data;
- unknown copyright and distribution restrictions;
- absence of definitions describing attribute table associated with data;
- unknown data classification; or
- unknown contact information for questions pertaining to data.

Other metadata initiatives have been developed by the USGS, ESRI, National Oceanic & Atmospheric Administration, US Department of Agriculture Forest Service North Central Research Station, and countless other agencies [10]. Two of the more common tools used for creating metadata are ESRI's ArcCatalog and Tkme or Tk metadata editor [11]. ESRI's ArcCatalog is a commercial data management tool that performs a number of functions, one of which is the creation and editing of metadata [10]. Although ArcCatalog is a highly useful and effective tool in metadata creation and editing, it is not a free software. However, most of the software is available at no cost, and one such is Tkme. This common, user-friendly tool is used to create metadata in a Windows-based environment and follows the guidelines set forth by the FGDC [11]. Numerous metadata tools are available to GIS users, and the choice of the tool depends on available resources, as well as on the nature of the data and the purpose of the project.

The essential objective of metadata is to provide GIS users with information that legitimizes the quality of the data being used and assures users that their data are sound. The use and creation of metadata are imperative entities of GIS data management, but the lack of its creation and misuse have resulted in data inaccuracies. Thus, interdependency analysts should convey their need for proper metadata to geospatial vendors and give preference to those geospatial datasets with complete metadata.

## 5 NEXT STEPS

Three recommendations are offered to increase the usefulness and accuracy of geospatial and nonspatial data to interdependency analysis: data investment, data documentation,

and data validation. Continued geospatial and nonspatial data investments are needed to alleviate data gaps by both public and private stakeholders. Some infrastructure layers such as roadways have sizable investments, regular updates, and high levels of accessibility. Other infrastructure layers, such as agriculture, energy, and telecommunications, lack investment and data stewardship.

Data investments lead to more accurate and updated geospatial data. As the geospatial features of the world change rapidly because of population growth, advancements in technology, and evolving political and cultural boundaries, the geospatial data attributed with these features must also change rapidly. Proper data investment ensures reliable, up-to-date data that create optimal standardization and awareness when distributed to the proper agencies.

Data documentation helps to inform the user of data limitations. The absence of GIS metadata creates risks that could influence decision makers in making poor choices that depend on potentially inaccurate data [12]. Analysts may use inaccurate data if they misunderstand the data limitations. Data uncertainty leads to erroneous assumptions that data are correct. Key documentation factors, such as data collection methods, date of creation, and attribute definitions, are crucial to the usage and accuracy of the data. For example, knowledge of the type of data collection used provides insights into the potential accuracy of the data. If a GPS receiver has been used in the data collection process, the user can expect a high degree of data accuracy because the data were collected by using highly accurate satellite systems. However, if the method of data collection has been geocoding, the user can expect a greater variance in the range of errors.

The lack of proper data documentation erodes users' confidence in the data implemented in their research. Data documentation includes widespread adoption of metadata standards. All data providers, public and private, should be required to include appropriate metadata. Geospatial data users, in particular, should require GIS data vendors to provide sufficient documentation. A strong front by GIS users will send a message to vendors that documentation is mandatory to conducting business. When none or limited documentation exists, users cannot be sure of the completeness and accuracy of their data.

Data validation involves understanding common errors, identifying them, and fixing them. Data validation may require a great deal of time and significant cost; it may also require manipulating the data to fix errors. When sufficient metadata are not available, users can take several steps to better understand the quality of the data they are using and to validate these data. These steps include the following actions:

- overlay high-resolution imagery to verify that geospatial data matches the accessible imagery. Public software is available from web sites such as Google Earth;
- use Web-based GIS applications that display land/parcel information to verify geospatial data. City and county web sites may provide such information;
- use GPS equipment to verify specific site locations. Low-cost GPS units are available for less than $500;
- verify sample data by visits or phone calls to facility owners;
- overlay duplicate geospatial data layers and analyze differences when duplicate sources are available; and
- geocode addresses and compare the addresses to provided geospatial data. Most GIS software includes user-friendly geocoding capabilities for nontechnical GIS users.

GIS tools (stand-alone, shared, Web-based, open source, 3D visualization, aerial imagery, and aerial flyover) provide infrastructure analysts with tremendous capabilities for interdependencies analyses. As discussed in this article, data investment, documentation, and validation are crucial to the quality of geospatial and nonspatial data. A high level of data fidelity is required to support the GIS and visualization tools needed for analyzing infrastructure interdependencies. Improvements in data investment, documentation, and validation will increase the value of GIS and visualization tools to infrastructure interdependencies analyses.

Several GIS forums continue to support data development and maintenance. An example of such a forum is Homeland Infrastructure Foundation-Level Data Working Group. This group is "a coalition of federal, state, and local government organizations, federally funded research and development centers (FFRDC), and supporting private industry partners who are involved with geospatial issues related to Homeland Security (HLS), Homeland Defense (HD), Civil Support (CS), and Emergency Preparedness and Response (EP&R)" [13]. This working group meets on a bimonthly basis and has a primary focus on geospatial information and its standards and presentation, as well as its accuracy. Such working groups promote a better understanding of data development and maintenance. They also create data uniformity among government agencies due to extensive collaboration, data sharing, and cooperative agreements on how to more accurately create and standardize data. Other GIS forums include vendor- specific, industry-specific, and state-level GIS forums. These forums are useful to all users of GIS tools and geospatial data.

## REFERENCES

1. Burrough, P. A., and McDonnell, R. A. (1998). *Principles of Geographical Information Systems*, Oxford University Press, Oxford, p. 333.
2. ArcGIS 3D Analyst. Dec. 13 2006. Accessed Feb. 2 (2007). http://www.esri.com/software/arcgis/extensions/3danalyst/index.html.
3. U.S. Department of Energy. (2004). *Data Subgroup Recommendations for Improving Energy Emergency Visualization Capabilities*, April 2004.
4. Goodchild, M. (1989). Modeling error in objects and fields. In *Accuracy of Spatial Databases*, M. Goodchild, and S. Gopal, Eds. Taylor and Francis, London, pp. 107–113.
5. Clarke, K. C. (2001). *Getting Started with Geographic Information Systems*, Santa Prentice Hall, Santa Barbara, CA.
6. Heuvelink, G. B. M., and Lemmens, M. J. P. M. (2000). *Proceedings of the 4th International Symposium Spatial Accuracy Assessment in Natural Resources and Environmental Sciences*, University Press, Delft, Netherlands, p. 772.
7. Morrison, J. L.. (1995). Spatial data quality. In *Elements of Spatial Data Quality. International Cartographic Association*, S. C. Guptill, and J. L. Morrison, Eds. Elsevier Science, Tokyo.
8. Jakobsson, A., and Vauglin, F. (2001). Status of data quality in European national mapping agencies. *Proceeding of the 20th International Cartographic Conference*, Beijing, Vol. 4, pp. 2875–2883.
9. Siska, P. P., and Hung, I. K.. (2000). Data quality on applied spatial analysis. In *Papers and Proceedings of the Applied Geography Conferences*, F. A. Schoolmaster, Ed. Kent State University, Ohio, Vol. 23, pp 199–205.
10. FGDC.gov. 7 Nov. 2006. Federal Geographic Data Committee. 29 Dec (2006). http://www.fgdc.gov/metadata.

11. USGS.gov. 29 Aug 2006. United States Geological Survey. 29 Dec. (2006). http://geology.usgs.gov/tools/metadata.
12. Van Oort, P. A. J., and Bregt, A. K. (2005). Do users ignore spatial data quality? A decision-theoretic perspective. *Risk Anal.* **25**(6), 1599–1609.
13. HIFLDWG.org. Homeland Infrastructure Foundation-Level Data Working Group. 16 Jan. 2007.

## FURTHER READING

Carmel, Y., Dean, D. (2004). Performance of a spatio-temporal error model for raster datasets under complex error patterns. *Int. J. Remote Sens.* **25**(23), 5283–5296.

Chrisman, N. R. (1991). *The Error Component in Spatial Data. Geographic Information Systems*, 1st ed., John Wiley & Sons, New York.

Cressie, N., Kornak, J. (2003). Spatial statistics in the presence of location error with an application to remote sensing of the environment. *Stat. Sci.* **18**(4), 436–456.

Foote, K. E., and Huebner, D. (1995). *The Geographer's Craft Project*, Department of Geography, University of Texas, Austin. (Available at http://www.forestry.umt.edu/academics/courses/for503/GIS_Errors.htm#Content).

Harrower, M. (2003). *Representing Uncertainty: Does it help People m Better Decisions?*, University of Wisconsin-Madison, (Available at http://www.cs.princeton.edu/courses/archive/spr04/cos598B/bib/Harrower.pdf).

Jakobsson, A., Vauglin, F. (2001). Status of data quality in European national mapping agencies. *Proceeding of the 20th International Cartographic Conference*, Beijing, Vol. 4, pp. 2875–2883.

Jinfeng, Ni, Ravishankar, Chinya V., and Bhanu, Bir. (2003). Probabilistic spatial database operations. *Advances in Spatial and Temporal Databases: Lecture Notes in Computer Science*, Springer-Verlag, New York, Vol. 2750, pp. 140–159.

Quon, S. (2006). Moving towards a more accurate parcel base. Presented at the *26th Environmental Systems Research Institute International User Conference*. San Diego, CA, 7–11 Aug. 2006.

Rapp, J., Wang, D., Capen, D., Thompson, E., and Lautzenheiser, T. (2005). Evaluating error in using the national vegetation classification system for ecological community mapping in Northern New England, USA. *Nat. Areas J.* **25**, 46–54.

Steiner, R., Bejleri, I., Yang, X., and Kim, D. (2003). Improving geocoding of traffic crashes using a custom ArcGIS address matching application. Presented at the *22nd Environmental Systems Research Institute International User Conference*. San Diego, CA, 7–11, July 2003.

Ubeda, T., Egenhofer, M. (1997). Topological error correcting in GIS. *Lect Notes in Computer Science*, Springer-Verlag, New York, Vol. 1262, pp. 283–297.

Wang, S., Shi, W., Yuan, H., and Chen, G. (2005). Attribute uncertainty in GIS data. *Fuzzy Syst. Knowl. Discov.* **3614**, 614–623.

Witschey, W. R. T., and Brown, C. (2002). The electronic atlas of ancient Maya sites. Presented at the *Symposium on Current Applications of Remote Sensing and GIS in North America and Mesoamerican Archaeology, 67th Annual Meeting of the Society for American Archaeology*. Denver, CO, 22 March, 2002.

Yeh, A. G., and Li, X. (2003). *Error Propagation and Model Uncertainties of Cellular Automata in Urban Simulation with GIS*. (Available at http://www.geocomputation.org/2003/Papers/Yeh_And_Li_Paper.pdf)

# THE MILITARY ROOTS OF CRITICAL INFRASTRUCTURE ANALYSIS AND ATTACK

STEVEN M. RINALDI
*Sandia National Laboratories, Albuquerque, New Mexico*

## 1 INTRODUCTION

Critical infrastructures underpin the political, military, economic, and social fabrics of societies. In recent years, it has become widely recognized that infrastructure disruptions could disproportionately affect the normal functioning of a nation. Disruptions from natural disasters, major strikes, attacks, and other mechanisms have amply demonstrated that critical infrastructures are highly interdependent, complex adaptive systems. Of import is the intricate, highly interdependent character of today's infrastructures. A disruption in one infrastructure, such as the electric power grid, can spread to other infrastructures such as communications networks and the Internet, thereby creating cascading disturbances and magnifying the effects far beyond those of the original disruption [1].

Since the mid-1990s, the US government has placed increasing emphasis on protecting the nation's critical infrastructures and associated key resources as matters of national and economic security. In 1996, President William J. Clinton issued Executive Order 13010, *Critical Infrastructure Protection* [2].[1] This order recognized that "(c)ertain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." The order directed the establishment of the President's Commission on Critical Infrastructure Protection (PCCIP), with the mission of examining vulnerabilities of and threats to critical infrastructures, determining legal and policy issues associated with protecting critical infrastructures, recommending a comprehensive national policy and implementation strategy to protect critical infrastructures, and proposing statutory or regulatory changes required to enable its recommendations. The PCCIP submitted its report [3] to the President in October 1997. In particular, the PCCIP stated that infrastructures are interdependent, that the destruction of key nodes and linkages in one infrastructure could ripple over and affect other infrastructures, and that coordinated attacks upon critical infrastructures could severely impact national and economic security [4].

[1]Executive Order 13010, *Critical Infrastructure Protection*, The White House, 15 July 1996. This executive order recognized eight critical infrastructures: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Today, the Department of Homeland Security recognizes 17 critical infrastructures and key resources (agriculture, food, defense industrial base, energy, public health and healthcare, national monuments and icons, banking and finance, drinking water and water treatment systems, chemical facilities, commercial facilities, dams, emergency services, commercial nuclear reactors, information technology, telecommunications, postal and shipping, transportation systems, and government facilities).

Yet the understanding that the destruction of certain key nodes and linkages could disproportionately affect national and economic security is not new. In fact, the roots of this insight can be traced to the early 1900s. As early as 1911, the French Lieutenant Poutrin wrote in the *Revue Générale de l'Aéronautique Militaire* that German aerial attacks on key ministries, transportation networks, and communication centers in Paris would shut down essential public services, thereby preventing France from mobilizing [5]. During World War I, British, French, and American air planners clearly recognized that attacks upon certain sectors of the German war industry could disrupt the manufacture and flow of war materiel to the Front, thereby affecting the ability of the German military to operate. American air warfare doctrine developed in the 1920s and 1930s by the Air Corps Tactical School (ACTS) significantly extended this line of thinking with the development of the "industrial web" theory of economic attack. This doctrine was put to test in World War II in the Allied bomber offensives against the Axis powers. Fifty years later, the air war waged against Iraq during Operation Desert Storm demonstrated refinements of the theory and the understanding and employment of critical infrastructure attack. Subsequent detailed academic studies of critical infrastructures and their interdependencies at the US Air Force's Air University in the 1990s indicate the emphasis placed by that Service on infrastructure attack to obtain specific strategic and operational effects and objectives.

This article traces the development of the theory and application of infrastructure attack in the 1900s. By and large, this development has occurred in air forces. Freed of the necessity to penetrate opposing surface forces, airmen realized early on that aircraft could range far beyond the terrestrial, tactical battle lines and directly attack strategic targets, including critical infrastructure. The objective of war was no longer engaging and destroying the enemy surface forces; rather, the air forces had an independent strategic mission of carrying the war to the enemy nation itself. The ability of airmen to identify, target, attack, and destroy key nodes and linkages is largely a story of the complex interplay of military doctrine and theory, wartime experience, and technological advancement. Initially, the ability to attack key nodes and linkages was limited by crude bombsights and small, dumb bombs. Operational considerations, such as the inability to bomb in adverse weather, decreased nighttime bombing precision, and primitive navigation capabilities, severely hampered and limited the effectiveness of counter-infrastructure operations in World War I. These issues were overcome by the end of the century with precision-guided weapons and all-weather, day–night attack capabilities. Furthermore, engineering and mathematical advancements, such as modeling, simulation, and analysis of critical infrastructures and operations research, enabled planners to better identify key nodes and linkages, all while driving the need for precision intelligence on adversary systems.

The sections below do not examine nuclear targeting doctrine and issues. Further, the analysis will focus predominantly on the development of American theory and doctrine of critical infrastructure attack.

## 2 INITIAL DEVELOPMENTS: WORLD WAR I

With the advent of military aviation in the first decades of the 1900s, nations at war had the ability to directly attack targets throughout their adversaries' homelands. World War I saw the first major operational analysis and application of this capability. Although the initial application of airpower during World War I was primarily limited to tactical

reconnaissance for the land forces, by the end of the conflict, strategic bombardment and targeting theories were coming into being.

British, French, and American airmen believed that airpower could be employed against both moral and material objectives. With respect to moral objectives, the British Admiralty theorized that bombing targets in Germany would force the recall of German aircraft from the front to defend the homeland. Further, the Admiralty hoped that bombardment would undermine the will of the German populace, and "optimistically attributed" an immense moral effect to every bomb that fell on Germany [6]. For General Hugh M. Trenchard, the first Chief of Staff of the British Air Ministry, the moral effect of bombing was critical. In a 26 November 1917 memo to the War Cabinet, he noted that bombardment had both a direct (material) and indirect (moral) effect:

> That purpose is to weaken the power of the enemy both directly and indirectly—directly by interrupting his production, transport and organization through infliction of damage to his industrial, railway and military centres, and by compelling him to draw back his fighting machines to deal with the menace—indirectly by producing discontent and alarm amongst the industrial population. In other words, it aims at achieving both a material and a moral effect [7].

The French had a different view of the moral effect of bombardment. Official policy held that the French would bomb German towns as reprisals for German bombardment of French towns. In one specific case of a reprisal, the French raided Freiberg on 14 April 1917 in retaliation for German submarine attacks on the hospital ships *Asturias* and *Gloucester Castle* the previous month. Interestingly, the French dropped leaflets upon Freiberg explaining the purpose of the raid [8].

With respect to the material effects of bombardment, the three allied nations sought to disrupt the ability of the German war industries to supply that nation's military forces. The British and French target sets can roughly be categorized as economic/industrial, infrastructural, and military:

- *Economic/industrial.* These targets would be termed the *defense industrial base* in today's parlance. They included iron and steel works, blast furnaces, gasworks, chemical works, benzene stores, and munitions factories. At the most fundamental level, these targets represent two primary commodities supporting the military—iron and explosives [9].
- *Infrastructural.* The primary targets in this set were rail assets, including rail yards, stations, lines, and rolling stock. These targets affected not only the ability of the German economy to produce war materiel but also that nation's ability to move finished goods to the front. In the last year of the war, the British also attacked at least three German electrical power grid targets [10].[2]
- *Military.* Targets included not only the lines of communication to the front but also aerodromes, fielded forces, and the German naval bases along the Belgian coast.

Beyond reprisals, the French developed bombardment plans that solely focused upon material objectives, primarily the factories and stations of the Saar Valley [11]. The

[2]The appendix of this source provides a detailed listing of raids by the British long-range bombing units (41st Wing, Eighth Brigade, Independent Forces) from 17 October 1917 to 11 November 1918. Information includes raid dates, target locations and descriptions, and bomb loads dropped. The target descriptions provide excellent insight into the types of targets considered important to crippling the German war industry.

French aimed at isolating the raw material producing regions, particularly iron ore, from the German factories. In a detailed analysis in January 1918, French planners determined that the Germans had altered rail traffic patterns for two primary reasons: "(1) to strip the area without using and consequently without burdening the main arteries of supply to the front and (2) to use the shortest possible route, in view of the shortage of rolling stock (locomotives and wagons), and in order to economize pit coal" [12]. The analysts concluding that attacking only four rail targets would isolate the iron ore regions, a significant aid to French operational planning.

American thinking was similar. A key goal of the US Air Service was to develop a bomber force capable of striking strategic targets in Germany. Targeting efforts concentrated on determining those assets without which Germany could not carry on its war effort [13]. Then-Major William "Billy" Mitchell believed that aviation could be divided into two types: tactical (observation for friendly artillery fire and control) and strategic (attacks on enemy materiel of all types behind the lines). He believed that the strategic attacks, if properly applied, would have the greatest effect upon the war effort [14].[3] Major Frank Parker, the US Liaison Officer to the French General Headquarters, reported to the US Board of Officers in July 1917 that the Air Service had a strategic function, acting independently of the ground forces to attack sources supplying the German military. This function included a military component (destroying aircraft, air depots, and the defensive air organization) and an economic component (destroying enemy depots, factories, lines of communications, and personnel) [15]. Major Edgar S. Gorrell, Chief of the Technical Section, Air Service, American Expeditionary Forces, developed a bombardment plan for the Air Service, dated 28 November 1917 [16]. He noted,

> The object of strategical bombing is to drop aerial bombs upon the commercial centers and the lines of communications in such quantities as will wreck the points aimed at and cut off the necessary supplies without which the armies in the field cannot exist... When we come to analyze the targets, we find that there are a few certain indispensable targets without which Germany cannot carry on the war.

Gorrell stated that a few "specific, well-known factories" were crucial to the manufacture of munitions. He noted that the destruction of the Mercedes engine and Bosch magneto plants in Stuttgart would cause the output of aircraft to drop in proportion to the damage done. He also called out rail, ammunition, and steel works for attack in the plan.

Following the end of the war, British and American intelligence services assessed the effects of bombardment from German records and interviews [17]. The Germans kept detailed records of the raids, including the resultant physical damages and estimates of their costs. Allied aircrew reports after raids were generally optimistic and overstated. One survey, which entailed extensive interviews with German plant directors, noted that the directors did not consider the bombardments effective, having created insignificant material damage and not affecting the war outcome. The effects of bombing munitions and chemical works did not meet the British expectations. The attacks upon the rail system were more of an annoyance, without ever producing a long-term isolation of rail stations or major dislocation of traffic.

[3]Memorandum for the Chief of Staff, US Expeditionary Forces, from Major Wm Mitchell, Aviation Section, Signal Corps.

A number of factors, driven in large part by the state of technology, contributed to the limited strategic results of bombardment. These factors included the following:

- limited bomb loads per aircraft;
- the generally small sizes of the bombs (anything under 112 pounds was ineffective, according to Germans interviewed after the war);
- failures of the bombs to detonate (e.g. 25% of the bombs dropped on the Saarbrücken region did not explode);
- poor radial blast effects of the bombs;
- limited combat radius of the aircraft;
- open cockpits, which exposed the pilots to environmental conditions;
- primitive bombsights and the inability to bomb accurately, particularly during night raids;
- navigation difficulties, particularly at night;
- mechanical difficulties and maintenance issues with the aircraft; and
- inexperienced and insufficiently trained aircrews [18].

Nevertheless, the stage had been set for strategic bombardment of the sources of war materiel, including supporting critical infrastructures such as transportation networks. Air planners clearly recognized the importance of attacking the adversary's defense industrial base. And, importantly, the first steps were taken toward analyzing that industry to determine chokepoints, bottlenecks, and key nodes for attack.

## 3 THE INTERWAR YEARS: THEORY AND DOCTRINE

The interwar period saw an intensive development of strategic bombardment theory and doctrine. Two early pioneers of airpower theory and vocal advocates for independent air forces with decisive strategic missions were the Italian General Giulio Douhet and the American Brigadier General William Mitchell. Both officers wrote extensively following World War I, arguing for independent air forces with their own respective strategic missions. Each discussed strategic target sets for bombardment, given that aircraft could fly over armies and navies and directly attack the interiors of adversarial nations.

Douhet argued that obtaining "command of the air"—essentially air supremacy—was a prerequisite and vital to victory. Once an air force had command of the air, it was free to range over the adversary and attack military, economic, and civil targets as well as the population itself at will:

> To have command of the air means to be in a position to wield offensive power so great it defies human imagination. It means to be able to cut an enemy's army and navy off from their bases of operation and nullify their chances of winning the war. It means complete protection of one's own country, the efficient operation of one's army and navy, and peace of mind to live and work in safety. In short, it means to be in a position *to win. To be defeated* in the air, on the other hand, is finally to be defeated and to be at the mercy of the enemy, with no chance at all of defending oneself, compelled to accept whatever terms he sees fit to dictate [19].

Douhet believed that the moral and material effects of bombardment would be tremendous, once command of the air was established. Receiving a relentless "pounding from the air", a nation's social structure would break down. The populace would rise up and demand an end to war, potentially even before the army and navy could mobilize [20].

Douhet clearly saw military utility in attacking critical infrastructure, both for its material and moral value. He wrote,

> In general, aerial offensives will be directed against such targets as peacetime industrial and commercial establishments; important buildings, private and public; transportation arteries and centers; and certain designated areas of civilian population as well. To destroy these targets three kinds of bombs are needed—explosive, incendiary, and poison gas—apportioned as the situation may require. The explosives will demolish the target, the incendiaries set fire to it, and the poison-gas bombs prevent fire fighters from extinguishing the fires [21].

Targeting civil infrastructure would spread confusion and panic among the populace. Douhet called for the rapid and complete destruction of rail, communications (including telegraph, telephone and radio), banks, public services, and government targets [22]. To hamper the ability of the army to mobilize, the air force should attack "railroad junctions and depots, population centers at road junctions, military depots, and other vital objectives". Naval operations would be degraded by "bombing naval bases, arsenals, oil stores, battleships at anchor, and mercantile ports " [23]. To Douhet, critical infrastructure was tightly intertwined with the ability of a nation to mobilize for and prosecute a war, and airpower provided the means to directly attack it.

Nonetheless, Douhet recognized that determining the specific targets to attack was not an easy task. He noted,

> The choice of enemy targets, as I have already pointed out, is the most delicate operation of aerial warfare, especially when both sides are armed with Independent Air Forces. . .The truth of the matter is that no hard and fast rules can be laid down on this aspect of aerial warfare. It is impossible even to outline general standards, because the choice of enemy targets will depend upon a number of circumstances, material, moral, and psychological, the importance of which, though real, is not easily estimated [24].

To Douhet, the selection of enemy targets would show the true abilities of the future air commanders.

From his experience in World War I, Mitchell was convinced that an air force should have an independent mission that would carry the war directly to the heartland of the enemy [25]. In his 1925 book *Winged Defense*, he argued that airpower should destroy the ability and will of the adversary to make war:

> To gain a lasting victory in war, the hostile nation's power to make war must be destroyed—this means the manufactories, the means of communication, the food products, even the farms, the fuel and oil and the places where people live and carry on their daily lives. Not only must these things be rendered incapable of supplying armed forces but the people's desire to renew the combat at a later date must be discouraged [26].

Sites manufacturing war material would be particularly inviting targets, as they took "months" to build and "if destroyed, cannot be replaced in the usual length of a modern war" [27]. While acknowledging that air forces would attack centers of production, he

did not believe that they should target the personnel *per se*. However, bombing could so terrorize a population that "the mere threat of bombing a town by an air force will cause it to be evacuated, and all work in munitions and supply factories to be stopped." In short, Mitchell proposed that war industries—and supporting systems such as the food and rail infrastructures—could be shut down by direct bombardment as well as worker absenteeism due to the threat of attack [28]. In contrast to Douhet, Mitchell almost always came out against directly attacking civilians, preferring to break the morale of the adversary indirectly by destruction of its vital centers [29].

Mitchell argued against the traditional view that destroying the enemy military forces constituted the main objective of war. "Vital centers" within the adversary nation were the true objective of a conflict:

> The advent of air power which can go to the vital centers and entirely neutralize or destroy them has put a completely new complexion on the old system of war. It is now realized that the hostile main army in the field is a false objective and the real objectives are the vital centers. The old theory that victory meant the destruction of the hostile main army, is untenable. Armies themselves can be disregarded by air power if a rapid strike is made against the opposing centers [30].

Mitchell believed that with airpower, it was no longer necessary to destroy an enemy's army in order to render the enemy incapable of waging war and induce him to sue for peace. Rather, by eliminating a nation's ability to manufacture and supply its forces with materiel, the nation would be unable to sustain a war—particularly a protracted conflict. Mitchell's views would strongly influence the next generation of air strategists and planners at the US Army's ACTS.

Economic attack and the concomitant destruction of critical infrastructures rose to an entirely new level at ACTS in the 1930s. Established as the Air Service Tactical School at Langley Field, VA, in November 1922, the school originally covered the tactics and techniques of the Air Service and other branches of the army and navy. In 1926, the school was renamed the Air Corps Tactical School. During the summer of 1931, the school relocated to Maxwell Field, AL, where it became the center of development of American airpower doctrine [31].

The doctrine of economic attack, along with a detailed methodology for target selection, developed at ACTS in the 1920s and 1930s. The fundamental precept of economic attack was that modern nations relied upon their economic and industrial systems for military weapons and supplies as well as the products and services required by a highly industrialized society. Destruction or paralysis of the economic and industrial systems would lead to a collapse of the enemy's military capability to fight and its social and political will to resist [32].

The 1926 ACTS text *Employment of Combined Air Force* argued that airpower could strike directly at vital centers in an enemy nation, thereby avoiding exhaustive wars of attrition and obtaining military victory at the minimum cost. If the enemy morale could not be destroyed, at least the enemy's military strength could be. The most suitable objectives for this purpose were the hostile air force; troops, supplies, and lines of communications in the combat zone; and industrial and transportation centers in the interior zone of the adversary [33].

By 1933, bombardment was firmly established as the primary means of employment of airpower at ACTS. At this junction, however, suitable surface targets were still vaguely designated. Instructor Major Donald Wilson undertook a more detailed approach to target

selection. Targets should be selected such that they would disrupt the adversary's *entire* economic fabric (supporting both the military and civilian sectors), thereby affecting normal civilian life to the point where faith in the military was lost and public outrage would force the government to sue for peace. The key was to locate those targets whose destruction could unravel this fabric—in other words, those key nodes or links that were vital to the functioning of the economy. That such targets existed was not doubted by the instructors: a prime example was a highly specialized spring used in controlled-pitch propellers. The spring was manufactured by only one firm, whose destruction would have meant the loss of the majority of production of aircraft in the United States. Determination and selection of such targets became central to ACTS theory [12].

During the period 1934–1940, the ACTS faculty refined its theory of economic warfare and target selection, known as the *industrial web theory*. As they were strictly forbidden to analyze foreign nations, the faculty surveyed American industry to locate those bottlenecks or nodes that would cause the destruction of the social, economic, political, and military fabric—or web—of a modern nation [34]. The 1934–1935 ACTS lecture *Air Force Objectives* stated that the ultimate objective in warfare was the destruction of national courage or morale [35]. Although the military arms of the nation might lose morale, the lecture noted that "loss of morale in the civil population is decisive. . .Morale is the pivotal factor. Its disintegration is the ultimate objective of all war." The resources to wage war were locked up in social, economic, political, and military spheres of a nation, so that pressure against these systems would lead to the destruction of morale and the defeat of the nation. Furthermore, the lecture noted that these spheres obtained an absolute interdependence during war, so disturbances in one sphere would affect all others. Those elements of an economy that supported the production of military goods were intricately intertwined with those elements supporting civilian life; pressure on one would affect the other.

The lecture then laid out in detail target sets in each of the spheres. The course provided a sophisticated analysis of the target sets including the interdependencies among them.

- *The social sphere.* Noting that "(t)he object here is the dislocation of normal life to the extent that the people are willing to surrender in the hope that they can at least regain a normal mode of living," the lecture discussed attacks against:
  - food supplies (which in turn relied upon lines of communication, transportation, and storage);
  - public utilities, including water-supply systems (linked to sanitation, public health, and firefighting), electric power (linked to modern conveniences and electric transportation modes), illuminating gas, and gasoline refining (linked to transportation); and
  - industry and transportation, which in turn would affect finances through loss of income, increase psychological pressure though worker idleness, and disrupt lines of communications.
- *The economic sphere.* The lecture stated that modern warfare placed an enormous load on an economy, which if it were to break down would "seriously influence the conduct of war by that nation, and greatly interfere with the social welfare of its nationals". The lecture examined in detail six primary target sets:
  - bottlenecks of specific commodities that entered into the production of many goods;

  - energy, including electricity (linked to manufacturing) [36], petroleum (linked to civil and military transportation and lubricants needed by industry), and coal (required for steel production and electric power generation);
  - raw materials, such as food, steel, fuel, nitrates, sulfuric acid, rubber, nonferrous metals, and cotton;
  - transportation, including rail, highways, and inland waterways;
  - manufacturing facilities; and
  - financial systems underpinning the economy.
- *The political sphere.* The lecture described government departments as the nervous system of the adversary, which if attacked would add confusion to the war effort. The lecture called for balance in attacking this sphere, as the political establishment would need to sense and react to the sentiments of the population.
- *The military sphere.* The lecture considered bombing military targets as strategically defensive, other than direct attacks against enemy airpower. Attacks against armies should be designed to prevent mobilization or strategic concentration; naval objectives included aircraft carriers, battleships, naval bases, docks, dry docks, shops, naval stores, and fuel oil reserves.

Other lectures that year amplified the themes of paralyzing the interdependent economic structures of a nation.[4] Bottlenecks received particular emphasis; the instructors sought those points that could unravel multiple sectors supporting both the war effort and civilian society. One lecture on the principles of war as applied to airpower postulated that the results of bombardment were sufficiently permanent that they would accumulate. It stressed that missions should have sufficient rapidity that the enemy could not repair and recover between attacks. Finally, and critically, the theory assumed that during a war, an economy would be stressed to its maximum point as it supported both civil and military needs. Without slack, the economy would be highly vulnerable to attack.

Although the destruction of morale was considered crucial, the faculty was opposed to direct attacks on civilians [37]. This presented a problem in that population centers frequently held industrial concentrations. The faculty believed that if certain systems supporting civil society were destroyed, then the cities would be rendered untenable and have to be evacuated. This could force the unraveling of the social sphere and morale of the nation, without the need to directly attack civilians. To this end, a 1939 lecture provided a detailed analysis of New York City, with specific target systems including the financial markets, transportation system, water supply, foodstuffs, and electric power [38].

In conjunction with its detailed analysis of targets, timing, mechanisms and objectives, the ACTS faculty also spent considerable effort considering the operational aspects of bombardment. By 1935, the preferred method of attack was high altitude, daylight precision bombardment of pinpoint targets. To carry out such missions, several technological innovations were required. Most notable were the development of long-range bombers with sufficiently heavy payload capacities. The B-17 bomber, successfully tested in 1935, provided this capability and profoundly affected the thinking of the ACTS faculty. Bombsights required marked improvements from the primitive devices of World War I. An

[4]These ACTS lectures included *Lecture—Air Force, General*, Lecture AF-2; *General Air Force Principles*, Lecture AF-6; *Lecture—Principles of War Applied to Air Force Action*, Lecture AF-7. These lectures were part of the 1934-35 *Air Force* course and were likely written by either Lieutenant Colonel Harold L. George or Captain Robert M. Webster.

improved Sperry bombsight appeared in 1933 and was followed by the more advanced Norden Mark XV bombsight. The Air Corps now had the ability to range widely over an enemy and attack individual targets [39].

ACTS came to its end in the summer of 1941. By this time, the faculty had developed a detailed airpower and targeting theory that focused on attacking the social, economic, political, and military spheres of an adversary, in which critical infrastructure attack played the central role. Locating and attacking bottlenecks would lead to an unraveling of this highly interconnected and stressed web, with an attendant loss of morale. The dislocation of civilian life under wartime conditions would be sufficient to cause the enemy to sue for peace. Although highly developed, the doctrine was theoretical with little basis in actual warfare. It awaited its test in the cauldron of World War II.

## 4 TRIAL BY FIRE: WORLD WAR II AND ECONOMIC TARGET SELECTION

In the years immediately before World War II, the British government began serious war planning, including collecting data on and analyzing the German economy. The Air Ministry developed a series of war plans, called the *Western Air Plans*, that focused on specific elements of the Germany economy [40]. WA-4 called for the destruction of the German railroad system, which by 1939 was deemed too dense for the existing British forces to make much of an impact. WA-5 planned the destruction of the Ruhr industrial region by primarily attacking power plants and coking plants. Subsequent analyses showed that it would be perhaps easier to shut down the Ruhr region by bombing the Möhne and Sorpe dams, which supplied water to industry. Unfortunately, the British did not possess sufficiently large bombs to destroy the dams. WA-6 focused on the German fuel supply, with 28 synthetic oil plants and refineries comprising the target list.

Some target systems such as the German fuel supply contained too many targets to be practical for the available British forces. Consequently, the British Ministry of Economic Warfare (MEW) sought out bottlenecks, particularly those critical items that were made only in a few isolated plants. Two such targets identified in 1941 were ball bearings and synthetic rubber. By late November 1942, the MEW identified other bottlenecks included alkalis, fuel injection pumps and electrical equipment for aircraft, and optical and laboratory glasses and instruments [41].

However, the British were hampered by several problems. Bomber range and payloads limited those targets that could be attacked. British bombers were not sufficiently armed and armored for daylight bombing of precision targets; the force had difficulty penetrating German fighters. The British switched to night bombing, which presented its own difficulties with navigation and accurate target identification. As a result, the British focused on area bombing as opposed to the destruction of precision targets until late in the war [42].

In 1940, the US Army Air Corps' Strategic Air Intelligence Section was also analyzing the industrial-economic structure of Germany. The Section initially focused on the following:

- electric power, including sources of fuel and the distribution system;
- steel, including raw materials;
- petroleum products, including the synthetic processes;

- the aircraft industry, including aluminum production and engine plants; and
- transportation networks, including railways, canals, and highways.

The section also examined the nonferrous metals supplies, machine tool production, and food processing and distribution [22].

In July 1941, then-Major Haywood Hansell visited the British as an observer. The express purpose of his visit was to explore British intelligence and bring home what material he could. Hansell, a former instructor at ACTS and member of the Strategic Air Intelligence Service, was impressed with the similarity of British and American targeting philosophies. Like the Americans, the British sought the collapse of German industry by destroying carefully selected targets. Hansell brought with him digests of American intelligence and found that he had much to offer. He noted that the Americans were better informed on the German electric power system and petroleum and synthetic products; the British had better information on the German aircraft industry including engine production, transportation, and the German Air Force. The British shared a considerable amount of information with Hansell, and he returned to the United States "loaded down" with targeting information [43].

In July 1941, the US Army Air Corps established its Air War Plans Division (AWPD). Lieutenant Colonel Harold L. George led the small staff, comprised of Lieutenant Colonel Kenneth N. Walker, Major Laurence S. Kuter, and Major Hansell. Each of these officers had been an ACTS faculty member. On 9 July 1941, President Franklin D. Roosevelt tasked the Secretaries of War and Navy to provide an estimate of "the overall production requirements required to defeat our potential enemies" [44]. In turn, General Henry H. "Hap" Arnold, Chief of the Army Air Force, tasked AWPD to develop the Air Annex for the requirements estimate. The guidance for the plan was quite broad and included four principal tasks:

> (1) (T)he provision of air forces in the defense of the Western Hemisphere; (2) the prosecution of an unremitting air offensive against Germany and lands occupied by German forces, including air preparation for a final invasion of the continent if that should be necessary; (3) the provision of strategic and close support air operations for such a land invasion; and (4) the provision of air defense and air support for strategic defensive operations elsewhere [45].

George's approach to developing the Air Annex was to plan a strategic offensive to debilitate the German war industry, defeat Germany if possible, and if necessary support an eventual invasion of the continent and Germany itself. Further, the planning effort assumed that the main burden for the strategic defensive in the Pacific region would lie on the Navy and that there would be no strategic offensive against Japan until Germany was defeated. Using the methods developed at ACTS, the officers examined in detail the German economy and military for vital links. As Hansell later recounted, several questions formed the basis of their analysis:

- What were the vital links?
- Among those links, which were the most vulnerable to air attack?
- Among those vulnerable to air attack, which would be the most difficult to replace or harden by dispersal or by going underground? [46].

The German economy was assumed to be highly stressed and drawn taut by the war effort. In the end, the plan focused on electric power, transportation (railways, canals, and highway networks), and the petroleum system (particularly synthetic oil production processes and the oil sources in Ploesti, Romania). An "intermediate objective" of overcoming the German fighter aircraft forces was established in order to permit the optimum effectiveness of the strategic attack against the German homeland. This could be accomplished by destroying the aircraft and engine manufacturing facilities, by elimination or curtailment of fuel supplies, or by attrition in air-to-air combat. The Germans were resourceful and their responses to the attacks would need to be anticipated. Further, the Germans would repair damaged targets so that revisiting targets would be necessary. The plan designated 154 targets in several systems, listed in Table 1 [47].

The resultant plan, AWPD-1, was accepted by the Combined Chiefs of Staff at the Acadia Conference in December 1941–January 1942. Of critical note is that AWPD-1 was essentially an aircraft production requirements plan and schedule, based upon a strategic campaign against Germany and Japan. The acceptance of the plan by the Combined Chiefs of Staff was interpreted as an acceptance of the strategic air campaign as well: Major General Carl Spaatz, Commanding General of Eighth Air Force, and Brigadier General Ira Eaker, Commanding General of VIIIth Bomber Command, accepted AWPD-1 (and its successor plan, AWPD-42) as the authoritative strategic guidance for the air campaign in the European theater [48].

A year after its delivery, AWPD-1 underwent the first of two modifications. In August 1942, the American air planning group modified it based on changes in the strategic situation and lessons learned to date. The new plan, AWPD-42, was delivered to the President on 24 August 1942. Like its predecessor, it was a requirements plan for aircraft

**TABLE 1 Targeting Priorities in World War II**

| AWPD-1 | AWPD-42 | Combined Bomber Offensive |
|---|---|---|
| 1. German Air Force<br>• Aircraft factories<br>• Aluminum plants<br>• Magnesium plants<br>• Engine factories | 1. German Air Force<br>• Aircraft factories<br>• Aircraft engine plants<br>• Aluminum plants | 1. German Air Force<br>• Fighter aircraft factories<br>• Aircraft engine plants<br>• Combat attrition |
| 2. Electric power<br>• Power plants<br>• Switching stations | 2. Submarine building yards | 2. Submarine building yards and bases |
| 3. Transportation<br>• Rail<br>• Water | 3. Transportation<br>• Rail<br>• Water | 3. Ball bearings |
| 4. Petroleum<br>• Refineries<br>• Synthetic plants | 4. Electric Power<br>• Power plants<br>• Switching stations | 4. Petroleum<br>• Refineries<br>• Synthetic plants |
| 5. Morale | 5. Petroleum<br>• Refineries<br>• Synthetic plants | 5. Rubber<br>• Synthetic plants |
| | 6. Rubber<br>• Synthetic plants | 6. Military transportation<br>• Armored vehicle factories<br>• Motor vehicle factories |

production. Its fundamental strategic philosophy called for a strategic offensive against Germany and a strategic defensive against Japan. As with AWPD-1, the primary strategic purpose was to undermine and destroy the capability and will of Germany to prosecute the war by destroying those industries supporting the war effort and associated structures that supported both the war industries and the civilian economy. The secondary purpose of the plan was to provide air support to forces operating in Mediterranean and the Pacific. It was a combined US–British air plan, with the US Army Air Forces focused on daylight bombing of precision targets, and the Royal Air Force taking on nighttime bombing of area objectives associated with munitions manufacturing. The targeting systems were similar to those of AWPD-1 and are detailed in Table 1 [49].

In December 1942, General Arnold issued a directive establishing the Committee of Operations Analysts (COA), an organization of respected American businessmen, economists, and military air planners. Unfortunately, the memo did not make clear the purpose of the COA and the objective of the air campaign. Subsequently, the Casablanca Directive clarified the COA's mission by calling for an air offensive against Germany to "bring about the progressive destruction and dislocation of the German military, industrial and economic system and the undermining of the morale of the German people to a point where their capacity for armed resistance is fatally weakened" [50].[5] The COA analyzed potential target sets, applying available intelligence information. It submitted its initial report in March 1943. The report, endorsed and slightly modified by MEW, contained the following list of priority target sets:

- German aircraft industry, with first priority on fighter aircraft, including assembly plants and engine factories;
- ball bearings;
- petroleum;
- grinding wheels and crude abrasives;
- nonferrous metals—copper, aluminum, zinc;
- synthetic rubber and tires;
- submarine construction yards and bases;
- military motor transport vehicles;
- transportation systems in general;
- coking plants;
- steel;
- machines tools;
- electric power;
- electrical equipment;
- optical precision instruments;
- chemicals;
- food production;
- nitrogen and the chemical industry; and
- antitank machinery and antiaircraft machinery.

[5]This directive was amended in late April/early May 1943 to include a final sentence that read, "This is construed as meaning so weakened as to permit initiation of final combined operations on the Continent."

This list was similar in target selection and philosophy to the targeting lists compiled for AWPD-1 and AWPD-42 [51].

The inputs of the COA were used by an American–British joint planning team headed by Brigadier General Hansell in VIII Bomber Command. This team developed its final list of targets based upon operational considerations that it believed would create the most damage to Germany given the existing and planned bomber force. This plan, which formed the basis of the US–British Combined Bomber Offensive (CBO), differed from AWPD-1 and AWPD-42, in that it was primarily a capabilities plan based on existing aircraft and those in the production pipeline as opposed to an aircraft requirements plan. The target sets of the CBO Plan are listed in Table 1. This plan was briefed to and accepted by the Eighth Air Force Commander, the European Theater Commander, and the Joint Chiefs of Staff, as well as their British counterparts [52]. The CBO, code-named POINTBLANK, got underway in May 1943.

The strategic concept for the air war against Japan paralleled the approach with Germany: defeat the Japanese air force and so weaken Japan's capability and will to fight that it would either capitulate or permit occupation against disorganized resistance, or, failing this, would enable an invasion at minimal cost [53]. The experiences in Europe heavily influenced the selection of target systems in Japan. In late 1943, General Arnold asked the COA for its recommended list of targets for a final offensive in Japan. The COA recommended seven target systems, although not in priority order:

- merchant shipping in harbors and at sea;
- iron and steel production, via the coke ovens;
- urban industrial areas vulnerable to incendiary attack;
- aircraft plants;
- antifriction bearing plants;
- the electronics industry; and
- the petroleum industry [54].

The following year, the Air Staff and ultimately the Joint Chiefs of Staff gave the overriding priority to the destruction or neutralization of the Japanese air force. Aircraft and engine plants were designated as the top priority targets for the newly formed XXI Bomber Command, led by Hansell.

Targets in Japan fell into two broad categories: select targets to be attacked with precision bombardment and urban area targets slated for incendiary attack. Hansell preferred precision attack. However, much of the Japanese industry was dispersed in small shops in the highly flammable urban areas, which made incendiary attacks attractive. In fact, in late 1944, the COA raised urban attacks to a higher priority than economic and industrial systems [55]. Given the critical importance of shipping, the XXI Bomber Command also executed aerial mining operations [56].

The selection of targets for attack in the two theaters followed a rigorous, scientific approach. Colonel Guido R. Perera, a member of the COA, described the process followed by that group in selecting targets in a 1943 memorandum to General Arnold:

> The Committee has arrived at certain conclusions in regard to target selection. It is better to cause a high degree of destruction in a few really essential industries or services than to cause a small degree of destruction in many industries. Results are cumulative and the plan once

> adopted should be adhered to with relentless determination. In the determination of target priorities, there should be considered (a) the indispensability of the product to the enemy war economy; (b) the enemy position as to current production, capacity for production and stocks on hand; (c) the enemy requirements for the product for various degrees of activity; (d) the possibilities of substitution for the product; (e) the number, distribution and vulnerability of vital installations; (f) the recuperative possibilities of the industry; (g) the time lag between the destruction of installations and the desired effect upon the enemy war effort [57].

Similarly, a RAND memorandum written shortly after the war provides insights into the analyses behind the selection of military and economic targets for bombardment by the Enemy Objectives Unit (EOU). The London-based EOU was comprised of US Army Air Corps officers and members of several intelligence units, including the Office of Special Studies and the Board of Economic Warfare. It assisted the 8th and 15th Air Forces with target selection and target intelligence. For each item or service considered for targeting, the EOU examined the following:

- the military importance of the item (e.g. frictionless bearings were essential for military vehicles);
- the percentage of direct military usage of the item;
- the depth, defined as the time elapsed between the end of production of an item and the occurrence of its shortage in tactical units;
- the economic vulnerability of an item or service, including the following:
  - the ratio of capacity to output (excess capacity, slack in the system, etc.);
  - substitutability for processes and equipment;
  - substitutability for the product (or service);
  - vulnerability of process and plant layout to attack; and
  - recuperability following attack;
- the physical vulnerability of the targets; and
- the location and size of the target sets.

The EOU gave preference to those targets with relatively small depth, that is, those items whose effects would show up rapidly. The relative size of the target set to the capabilities of the available air forces also influenced target selection [58]. Clearly, such analyses required insights from military planners, industrialists, and economists, all supported by the most detailed intelligence available.

How effective was the economic targeting of Germany and Japan? In November 1944, the Secretary of War established the United States Strategic Bombing Survey (USSBS), based on a directive from President Roosevelt. The Survey comprised civilians, officers, and enlisted personnel. The Survey was tasked to enter Germany and Japan as soon as possible and to assess the effectiveness of bombardment and its contribution to the victory over the Axis powers. Teams made close inspections of plants, cities, and areas; amassed statistical data and documentation; and interviewed and interrogated thousands of persons, including political, military, and industrial leaders in Germany and Japan. The Survey wrote several hundred highly detailed reports on the effectiveness of the bombardment campaigns [58].

In the conclusion section of its summary report on the war against Germany, the USSBS made a number of key observations about the effectiveness of bombing. In the words of the Survey,

- "A first-class military power—rugged and resilient as Germany was—cannot live long under full-scale and free exploitation of air weapons over the heart of its territory."
- "As the air offensive gained in tempo, the Germans were unable to prevent the decline and eventual collapse of their economy. Nevertheless the recuperative and defensive powers of Germany were immense; the speed and ingenuity with which they rebuilt and maintained essential war industries in operation clearly surpassed Allied expectations. . ." The German economy was undermobilized throughout much of the war, allowing it to recover and rebuild facilities to some levels of pre-attack production between raids, particularly in the early days of the war. The Germans employed numerous means to support their industrial operations, including camouflage, smoke screens, shadow plants, dispersal, and underground factories. The Germans were also able to make strategic substitutions for critical products [59], and employed means to increase industrial efficiencies. Dispersal, however, increased the importance of transportation networks, and thus multiplied the problems created by Allied air attacks against those networks.
- "The importance of careful selection of targets for air attack is emphasized by the German experience. The Germans were far more concerned over attacks on one or more of their basic industries and services—their oil, chemical, or steel industries or their power or transportation networks—than they were over attacks on their armament industry or the city areas. The most serious attacks were those which destroyed the industry or service which most indispensably served other industries."
- "The Germany experience showed that, whatever the target system, no indispensable industry was permanently put out of commission by a single attack. Persistent re-attack was necessary." Between attacks, the Germans worked to recover those destroyed facilities. For example, following the attacks on the ball bearing facilities at Schweinfurt, the Germans dispersed facilities, redesigned equipment where possible, and drew down existing stocks of frictionless bearings. An important lesson was that frequent reattack to ensure destruction of the industry was necessary.
- "In the field of strategic intelligence, there was an important need for further and more accurate information, especially before and during the early phases of the war." Much critical intelligence and analytic capability came from civilian experts not associated with the military before the war [60].

The USSBS examined the impacts of bombardment on specific target systems. With respect to the German transportation networks, the railroad system was unable to meet its transportation requirements after October 1944. This disorganized the flows of raw materials, components, and finished goods. Dispersal of industry only complicated the situation [61]. Coal was a particularly crucial commodity, as it was used for the manufacture of steel, electric power generation, and by the locomotives of rail system itself. One detailed analysis of the collapse of the German war economy concluded that the coal-rail nexus was the foundation of all economic activity in Germany, and its destruction created dire short-term effects on the economy, led to the disintegration of Germany's division of labor, created serious declines in armaments production, and caused a major decrease in supplies to the Wehrmacht [62].

Grinding wheels and abrasives were critical commodities in the German economy. During interrogations after the war, Albert Speer, the German Minister of Armaments

Production, stated that the entire armaments industry would have come to a standstill in 6 months if the production of abrasives had been destroyed. Furthermore, the complete loss of the ball bearing industry would have halted armaments production in 4 months [63].[6]

Speer was likewise concerned about the potential loss of electricity. Noting that "electricity alone could not be stockpiled," Speer stated that the destruction of the electric power grid would have been "the most radical measure, as it would at once lead to a breakdown of all industry and support of public life". The chief engineer in charge of the electric power grid observed that "the war would have been finished two years sooner if you concentrated on the bombing of our power plants" [64].

The destruction of the petroleum infrastructure had critical implications for the German economy and war effort. Significant declines in 1945 of petroleum stocks affected the ability of German ground and air forces to operate. From an infrastructure interdependencies perspective, loss of the synthetic petroleum industry killed nitrogen production, which itself was required for synthetic rubber and ammunition production [65].

In the Pacific theater, the Japanese economy was strangled by the destruction of its shipping industry by submarine and air attack as well as mining operations. Shipping logistically supported the fielded Japanese military forces and was vital to Japanese industry. Japan was critically dependent upon imports, which were cut off by the antishipping campaign. Steel production, for example, was directly affected by the destruction of shipping. Oil imports began declining in mid-1943 and were eliminated by April 1945. The USSBS report stated that even without air attacks on industry, the overall level of Japanese production in August 1945 would have been 40–50% below the peak levels of 1944 [66].

To paraphrase the USSBS, the air campaign against Japan destroyed its economy a second time over. The precision attacks against the aircraft and engine plants forced dispersal of those industries, including moving some manufacturing underground. The dispersal coupled with the destruction wrought by the bombing campaign crippled the Japanese aircraft industry. The electric power distribution system, though not explicitly targeted, and its associated load were largely destroyed by the urban incendiary attacks. The urban incendiary attacks severely damaged smaller urban industrial plants. Attacks against the rail system were beginning at the end of the war; consequently, the rail system was in reasonably good condition at the war's end. The labor force declined inefficiency due to malnutrition, fatigue, destruction of urban housing areas, and local transportation problems. Approximately 30% of the entire urban population of Japan lost their homes and possessions. The targeting of industry, both through area bombing and precision attacks, reduced prewar production by the following amounts:

- oil refineries: 83%;
- aircraft engine plants: 75%;
- airframe plants: 60%;
- electronics and communications equipment: 70%;
- army ordnance plants: 30%;
- naval ordnance plants: 28%;

[6]Some have questioned Speer's motivation behind his statements—was he stating what he honestly believed, or was he providing inputs that the USSBS and airpower advocates wanted to hear?

- merchant and naval shipyards: 15%;
- light metals: 35%;
- ingot steel: 15%; and
- chemicals: 10%. [67].

The Survey concluded that "heavy, sustained and accurate attack against carefully selected targets is required to produce decisive results when attacking an enemy's sustaining resources. . .no nation can long survive the free exploitation of air weapons over its homeland. For the future it is important fully to grasp the fact that enemy planes enjoying control of the sky over one's head can be as disastrous to one's country as its occupation by physical invasion" [68].

Technology was a major enabling factor in air campaigns of World War II. Long-range bombers able to deliver heavy bomb loads, the turbosupercharger, the Norden bombsight, radar bombing, and improved navigation all contributed to the ability to attack and destroy precision targets. Nonetheless, "precision" was limited during the war: the average miss distance for a 2000-lb bomb in the European campaign was 3300 feet. An Eighth Air Force assessment concluded that only 7% of the bombs dropped from September through December of 1944 fell within 1000 feet of their aimpoints. Numerous factors contributed to bombing problems, including inherent limitations in the bombsights, poor weather, dispersion of bomber formations when attacked by fighters, training, and poor aerodynamic designs of the bombs themselves [69]. By the end of the century, however, advanced technologies would largely resolve these issues, enabling truly precision attack.

## 5 MODERN THEORY AND PRACTICE

By the late 1980s to early 1990s, the confluence of technical developments, theory, and the Iraqi invasion of Kuwait drove a new test of critical infrastructure attack. The first driver, technology, had advanced to the point where the early promise of attacking precision targets on a global scale could finally be achieved. Bombing accuracies for unguided weapons had significantly improved, due to improved navigation, better aerodynamic designs of the bombs, improved weapons-release technologies, and better cockpit displays. Table 2 illustrates the improvement in bombing accuracy, for the case of hitting with a 90% probability a 60 $\times$ 100 feet target with an unguided 2000-lb bomb from medium altitude. CEP is the circular error probable, defined as the radius of a circle inscribed around a target inside of which 50% of the bombs fall [70]. Precision-guided weapons, introduced during the Vietnam War, completely redefined the military principle of mass. At the end of the century, laser- and global positioning system (GPS) guided weapons had advanced to the point where CEPs were measured in feet [71].[7] With this level of precision, the size of the weapon required to destroy a target could potentially be smaller. Reduced weapon sizes in principle meant that a single aircraft could carry more weapons, accurately attack multiple targets per sortie, and potentially reduce collateral damage. In fact, by the Gulf War of 1991, planners talked of "targets per sortie"

[7]As an example, F-117 fighters dropped 2041 tons of bombs during Operation DESERT STORM in 1991. One thousand six hundred and sixteen tons, or 79%, hit their targets, implying that they landed within 10 feet of the desired aimpoints. One well-publicized video showed a smart bomb flying down the ventilation shaft of the Iraqi Air Force headquarters building near Al Muthenna airfield.

**TABLE 2 Bombing Accuracy in the 1900s**

| War | Number of Bombs | Number of Aircraft | CEP (feet) |
|---|---|---|---|
| World War II | 9070 | 3024 | 3300 |
| Korean War | 1100 | 550 | 1000 |
| Vietnam War | 176 | 44 | 400 |
| Fall 1990 | 30 | 8 | 200 |

rather than "sorties per target" [72]. With aerial refueling, aircraft such as the B-1 and B-52 bombers had by this time achieved truly global range. Technologies such as GPS eliminated the navigation problems that had plagued bomber crews during the two world wars. The combination of accurate navigation and precision weaponry opened the night to precision attack operations, which during World War II had been used primarily for area attacks. Stealth technology enabled attacks against heavily defended targets. Finally, computer modeling of critical infrastructures and sophisticated engineering and operations research techniques opened the door to understanding the effects of destroying individual elements in a critical infrastructure—as well as potentially planning attacks to create very specific operational or strategic level effects [73].[8]

Airpower doctrine and theory had likewise advanced by the end of the 1900s, in large part due to the significant contributions of US Air Force Colonels John Boyd and John A. Warden III. Both men shared a common theme of defeating an adversary through strategic paralysis, or the incapacitation of the enemy, although from distinctly different perspectives and approaches. Further, both colonels emphasized a shift from the economic warfare of ACTS and World War II to forms of control warfare. Boyd emphasized the mental, moral, and temporal aspects of war, arguing that one could induce strategic paralysis in an adversary by operating inside the adversary's observe-orient-decide-act (OODA) loop. Warden developed a detailed airpower theory that focused on the physical aspects of warfare and considered in detail the question of targeting. His "Five Rings" model included critical infrastructure attacks and their influence upon the overarching objective of forcing strategic paralysis [74]. As Boyd did not consider in depth critical infrastructure targeting, we do not explore his theories below.

While a student at the National Defense University, Warden published his theories of air warfare at the strategic and operational levels in his book *The Air Campaign: Planning for Combat* [75]. In the 1990s, he published a series of articles that concisely described his theories [76]. Warden argued that the ultimate aim of all military operations was to control the civil and military command structures of the adversary. This could be accomplished by causing changes in one or more parts of the enemy's physical systems in such a manner as to force the adversary to adopt one's objectives as his own or by making it physically impossible for the adversary to offer opposition. To Warden,

[8]At the end of the century, Sandia National Laboratories and Los Alamos National Laboratory jointly established the National Infrastructure Simulation and Analysis Center (NISAC), with the mission of modeling, simulating, and analyzing critical infrastructures, key assets, and infrastructure interdependencies. NISAC employs highly sophisticated engineering and computer models to simulate infrastructures and the effects of disturbances, including high-order and cascading effects. In 2003, NISAC became a formal program of the Department of Homeland Security. NISAC has a homeland security mission focused on critical infrastructure protection and defense, as opposed to offensive military mission. See http://www.sandia.gov/mission/homeland/programs/critical/nisac.html.

making the adversary incapable of offering opposition was the essence of imposing strategic paralysis. Warden recognized that warfare had both a physical and morale side and suggested that war could be visualized in terms of the equation:

$$(\text{Physical}) \times (\text{Morale}) = \text{Outcome}$$

The physical side of war was, in principle, completely knowable and predictable, whereas the morale side involved humans and their reactions and therefore was not predictable. Consequently, Warden argued that one's efforts in war should be directed at the physical side.

Warden viewed an adversary from a systems engineering perspective with his "Five Rings" model. This model postulated that any strategic entity—whether a state, business, or terrorist organization—could be represented by five concentric rings (Fig. 1). The rings, from the innermost outward, and in order of importance, are as follows:

- Leadership, containing the enemy command structure and command communications.
- Organic essentials (or key production), comprised of more than just war-related industry. The electric power and petroleum industries are organic essentials; Warden noted that these systems had relatively few targets and were generally fragile.
- Infrastructure, with a focus on the adversary's transportation networks, including key nodes, railroads, and bridges. He noted that the targets in these systems were more numerous and redundant than the organic essentials and would likely take more effort to effectively damage.
- Population, including its food sources. Warden did not advocate directly targeting people, given that there were too many to effectively target, moral objections notwithstanding. However, he believed that indirectly attacking populations, such as the North Vietnamese did to the American populace during the Vietnam War, could be effective under certain circumstances.
- Field military forces. Warden emphasized that the fielded military forces were just means to an end and not the proper objective in war. He noted that fielded forces were often the "hardest" of all targets, given that they were designed for combat.

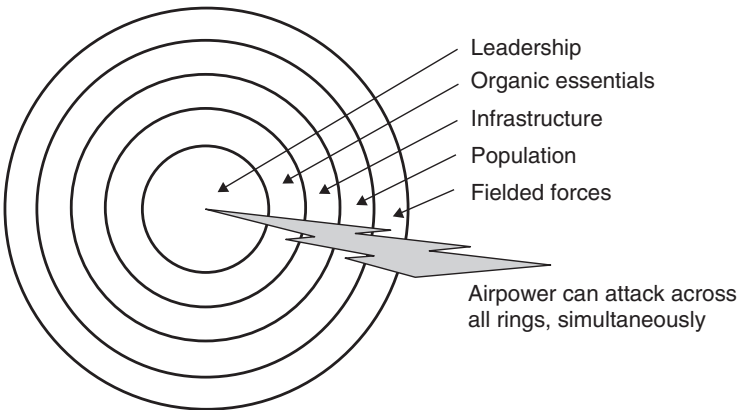



**FIGURE 1** Warden's Five Rings model.

Warden noted that the rings are not independent entities; rather, they are interdependent with one another. Like his predecessors, Warden was clear that an air force could attack targets within and throughout any of the rings. Nonetheless, he stressed that all actions must be aimed at the mind of the enemy command and that the essence of war was to apply pressure to the central ring—the enemy's command structure. Targeting this ring alone would generally not be sufficient, but all actions against targets in other rings must be focused on affecting the command structure. To Warden, this was "inside-out warfare", in that the traditional concept of attacking fielding forces was replaced with an emphasis on directly affecting and influencing the innermost leadership ring.

Warden also maintained that attacks should be compressed in time. Given that an air force could attack across an entire strategic entity, parallel attacks against many target sets were preferred to a serial attack stepping sequentially through target sets. He likened this to "death by a thousand cuts", which would only hasten strategic paralysis (and in the sense of Boyd, would enable one to get inside the adversary's OODA loop). With stealth and precision weaponry, many targets could be attacked simultaneously, thus enabling parallel warfare throughout the entire depth of an adversary. Given the time-compressed nature of parallel war and his experience in the Gulf War of 1991, Warden termed this form of conflict *hyperwar*.

The Gulf War put Warden's theories to the test. In August 1990, as Iraq invaded Kuwait, Colonel Warden led CHECKMATE, an office under the Air Force Deputy Chief of Staff for Plans and Operations. CHECKMATE was primarily tasked with long-range planning. Following the invasion, General Norman Schwarzkopf, the Commander in Chief (CINC) of Central Command, sent Lieutenant General Charles Horner, Commander of Ninth Air Force, to the theater as the onsight commander and the Joint Force Air Component Commander (JFACC). The JFACC was responsible for developing and executing the air campaign. However, in the days immediately following the Iraqi invasion, General Horner's staff was consumed with logistics and aircraft deployment and beddown issues. On August 8th, General Schwarzkopf consequently called upon the Air Force Chief of Staff for assistance in developing the air campaign. This tasking flowed down to Colonel Warden and his CHECKMATE staff. The staff developed the concept for a strategic air war within 2 days and on August 10th, briefed the plan to General Schwarzkopf at MacDill AFB in Florida. The air campaign, named INSTANT THUNDER, was accepted with some changes by US officials, General Horner, and General Schwarzkopf. In the theater, General Horner placed Brigadier General Buster C. Glosson in charge of planning and directed him to turn INSTANT THUNDER into an operational plan [77].

Warden's Five Rings provided the framework for the CHECKMATE planners. Their initial target breakout by ring is given in Table 3. The initial breakout, which changed little during the planning, provided a framework for determining individual targets. The planners considered interdependencies among target sets. Generally, they did not search for bottlenecks as did the World War II planners, as they were not constrained to serial attacks. Instead, the planners sought to attack simultaneously across the entirety of Iraq, aiming to impose strategic paralysis. For individual targets such as refineries, the planners took advantage of precision-guided weapons by seeking those specific aimpoints that would debilitate the target [78]. The objectives of the strategic campaign were to isolate

**TABLE 3 Breakout of the Five Rings in the Gulf War**

| Leadership | Organic Essentials | Infrastructure | Population | Fielded Forces |
|---|---|---|---|---|
| Communications | Electricity | Railroad bridges | Psychological operations | Strategic air defense system |
| Internal control mechanisms | Oil refining | Civilian airfields | | Strategic offensive forces |
| | Nuclear technology<br>Weapons production facilities | | | Republican Guard |

the Iraqi leadership, degrade key production, disrupt the infrastructure through transportation attacks, turn the population and the military forces against the Iraqi regime, and destroy Iraq's offense and defensive capabilities [79].

Airpower during the Gulf War had a decisive effect. By striking several dozen targets in the Baghdad area, the regime lost its ability to command and control its forces. In effect, the regime was rapidly rendered blind to the ongoing war. Air strikes against 27 selected electric power targets across the nation shut down the grid in the Baghdad area. Because electricity cannot be stockpiled, and given that other infrastructures depend upon electricity, the loss of power affected many Iraqi military facilities. The oil campaign reduced Iraq's production to near zero, with slightly more than 500 sorties against 28 targets. In 3 days of attacks against the oil infrastructure, Iraq's refined oil production was halved; after 13 days, production was reduced to zero. The transportation campaign reduced the flow of supplies to Basra, a major transshipment point, to a level well below that required to sustain Iraqi combat operations. The combination of stealth, precision, and parallel warfare reduced the Iraqi regime's ability to command its forces to near zero and rendered the Iraqi military ineffective before the commencement of ground operations [80].

Following the Gulf War, Colonel Warden was appointed as Commandant of Air Command and Staff College (ACSC) and the School of Advanced Airpower Studies (SAAS), the US Air Force's professional military schools for midgrade officers. His influence on the curriculum was profound; he oriented it toward the operational level of war with a heavy emphasis on air campaign planning. He instituted student research projects, again at the operational level of war [81]. A number of student papers and SAAS theses during his tenure examined critical infrastructure analysis and attack. These papers included analyses of telecommunications systems [82], the petroleum sector [83], electric power [84], and social networks [85]. One thesis provided a detailed examination of infrastructure interdependencies, postulating that modern economies are complex adaptive systems and must be targeted as such [86]. Chaos theory was applied to critical infrastructures, social systems, and campaign-level planning in an ACSC student research project [87]. Another detailed analysis of electric power grids included computer software that demonstrated effects-based targeting of that infrastructure [88]. Although these papers included detailed information on the functioning, structure, and architectures of their respective infrastructures, they were primarily studies of the strategic and operational utility of critical infrastructure attacks in the age of modern warfare.

By the end of the twentieth century, a new technology of warfare was emerging on the horizon: information or cyber warfare. Many have speculated in the open literature

about the possibility of cyber attacks against the computerized control systems that manage and operate the nation's critical infrastructures [89].[9] If disrupted, these supervisory control and data acquisition (SCADA) systems could directly affect the infrastructures they control. Adversarial control or attack of SCADA systems and the subsequent infrastructure disruptions could have important economic and national security ramifications. Today, the Departments of Homeland Security and Energy both have programs with the objectives of increasing the security of SCADA and other process control systems to reduce the risks and consequences of such attacks.

## 6 OBSERVATIONS

The above-mentioned historical survey demonstrates that airpower theory and practice in the 1900s leaned heavily upon critical infrastructure attacks to obtain national and military objectives. Analyzing the air campaigns and theories, we can make the following observations on military thought concerning specific critical infrastructures:

- *Defense industrial base.* Attacks against this infrastructure were employed primarily to deny an adversary the physical means to sustain a war. ACTS theorized that many industries were actual dual use; hence, their destruction would also undermine the social fabric of a nation.
- *Electricity.* Electric power is vital to the normal operation of a nation, including the functioning of its defense industrial base. Planners believed that disrupting electric power would affect the ability of the adversary government to carry out its essential functions and prosecute the war, degrade the military's ability to operate, and disrupt normal civilian life.
- *Petroleum.* Loss of refined petroleum products would preclude the operation of military vehicles, disrupt transportation networks, and deny raw materials used in many manufacturing processes vital to the production of war materiel.
- *Communications.* Disruption of communications would directly affect the ability of the national and military leadership to command and control military operations, add confusion to the war effort, and potentially panic and confuse the population.
- *Transportation.* Loss of transportation networks would hamper the ability to mobilize and concentrate forces, affect the ability to move raw materials to the defense industrial base, degrade the ability of dispersed industries to produce war materiel, and potentially affect the ability of the labor force to get to work.
- *Food.* Destruction of food supplies, including agricultural areas, would lead to malnutrition, with a particular target of the labor force of the defense industrial base.

Although this list is not exhaustive, particularly with respect to cascading and higher order effects, it is representative of the thought that went into targeting infrastructures throughout the 1900s.

[9]The massive cyber attacks on Estonia in April–May 2007 illustrate a means of attacking critical infrastructures that do not use SCADA systems yet rely upon the Internet to function. Targets included banks, newspapers, and the government—representative elements of several critical infrastructures. For example, the attacks forced Estonia's largest two financial institutes to severely restrict online access. Of note is that Estonia is one of the most wired European nations.

Despite the detailed development of economic and infrastructure attack theories and plans, the ability to carry out such attacks was tightly linked to the state of technology. Attacks in World War I were largely viewed by the Germans as ineffective; technology and operational considerations precluded the air services from obtaining their desired operational and strategic effects. Improvements in technology were a critical enabling factor for aerial bombardment in World War II; infrastructure attacks yielded decisive effects against the German and Japanese economies and warmaking abilities. Nevertheless, technological limitations were apparent in that war, such as the degree of precision that could be obtained by bombing. By the end of the century, these limitations had largely been overcome, thereby opening up new operational possibilities for infrastructure attack as demonstrated in the Gulf War.

## 7 CONCLUSIONS

While protection of critical infrastructures has risen to the level of a national priority only during the past 15 years, attacking critical infrastructures during conflicts is hardly new. With the advent of the airplane, air forces were able to fly over fielded surface forces and directly attack strategic objectives throughout an adversary's homeland. Target sets originally concentrated on the defense industrial base and transportation networks. By World War II, with improved aircraft, bombs, and bombsights, the Allied forces attacked "precision" targets throughout the Axis nations, including many critical infrastructures. By the end of the century, precision weapons had come to the forefront, enabling surgical attacks on critical infrastructure targets. Indeed, during the Gulf War of 1991, Coalition forces conducted rapid, parallel attacks against infrastructure targets throughout Iraq. Theory and technology contributed heavily to the use of critical infrastructure attack during conflicts in the twentieth century.

## REFERENCES

1. Rinaldi, S. M., J. P. Peerenboom, and Kelly, T. K. (2001). Complexities in identifying, understanding, and analyzing critical infrastructure interdependencies. Invited paper, *IEEE Control Syst. Mag.* **21**(6), 11–25.
2. Department of Homeland Security (2006). *National Infrastructure Protection Plan*. Department of Homeland Security, Washington, DC, p. 3.
3. PCCIP (1997). *Critical Foundations: Protecting America's Infrastructures*. The Report of the President's Committee on Critical Infrastructure Protection, October 1997.
4. Ibid, 15.
5. Kennett, Lee (1991). *The First Air War: 1914-1918*. The Free Press, New York, p. 44.
6. Williams, G. K. (1999). *Biplanes and Bombsights: British Bombing in World War I*. Air University Press, Maxwell Air Force Base, AL, p. 11.
7. Ibid., 53.
8. Ibid., 11.
9. Ibid., 44, 97, 102,
10. Ibid., 271–287.

11. Ibid., 15.
12. Ibid., 65.
13. Huston, J. W. (1978). Major General, USAF. Forward in *The U.S. Air Service in World War I*, Vol. II, M. Maurer, Ed. The Office of Air Force History, Headquarters USAF, Washington, DC.
14. Ibid., 108.
15. Parker, Frank. Major. (1917). *The Role and Tactical and Strategical Employment of Aeronautics in an Army*, Report to the Board of Officers, 2 July 1917. Ibid., 119–121.
16. Ibid., 141–157.
17. Williams, G. K. (1999). *Biplanes and Bombsights: British Bombing in World War I*. Air University Press, Maxwell Air Force Base, AL, pp. 111–118.
18. Ibid., 9, 17, 24, 102, 120, 121, 123.
19. Douhet, G. (1942). *The Command of the Air*. Coward-McCann, New York. Translation by Dino Ferrari. Ferrari's translation includes five separate works of Douhet, originally published between 1921 and 1930. The version cited in this article is the 1983 reprint of Ferrari's translation by the Office of Air Force History, Washington, DC. Page 23, emphasis in original.
20. Ibid., 58.
21. Ibid., 20.
22. Ibid., 51.
23. Ibid., 57.
24. Ibid., 59–60.
25. Maurer, M. (1917). *Memorandum for the Chief of Staff, U.S. Expeditionary Force, from Major Mitchell, Aviation Section, Signal Corps*, dated 13 June 1917, p. 111.
26. Mitchell, W. (1925). *Winged Defense: The Development and Possibilities of Modern Air Power Economic and Military*. Putnam's, New York, pp. 126–127. The version cited in this article is the 1988 Dover Publications, Inc., reprint.
27. Mitchell, W. (1925). *Winged Defense*, 17.
28. Ibid., 5–6.
29. Metz, D. R. (1998). *The Air Campaign: John Warden and the Classical Airpower Theorists*. Air University Press, Maxwell Air Force Base, AL, p. 35.
30. Mitchell, W. (1930). *Skyways*. J.B. Lippincott, Philadelphia, PA, p. 253.
31. Finney, R. T. (1992). *History of the Air Corps Tactical School 1920-1940*. Center for Air Force History, Washington, DC, pp. iii, 11, 25.
32. Hansell, H. S. Jr. (1986). *The Strategic Air War Against Germany and Japan*. United States Air Force Office of Air Force History, Washington, DC, pp. 9–11. Hansell was a member of the ACTS faculty from 1935-1938.
33. Finney, R. T. (1992). *History of the Air Corps Tactical School 1920-1940.* Center for Air Force History, Washington, DC, p. 63.
34. Hansell, H. S. (1986). The implicit assumption was that the economies of modern, industrialized nations would share many characteristics. *Strateg. Air War* **12**, 22.
35. Air Corps Tactical School (1934). *Air Force Objectives*. Lecture AF-5 from the 1934-35 course entitled *Air Force*. Air Corps Tactical School, Maxwell Field, AL.
36. Hansell, H. S. Jr. *The Strategic Air War Against Germany and Japan*. United States Air Force Office of Air Force History, Washington, DC, p. 12. Hansell was a member of the ACTS

faculty from 1935-1938. Hansell considered the electric power system to be the "very heart of our industrial system".

37. Hansell, H. S. Jr. *The Strategic Air War Against Germany and Japan*. United States Air Force Office of Air Force History, Washington, DC, p. 12. Hansell was a member of the ACTS faculty from 1935–1938.
38. Fairchild, M. S. (1939). *Lecture—New York Industrial Area*, Lecture AF-11-C from the 1939 course *Air Force*. This lecture was developed by Major Muir S. Fairchild.
39. Finney, R. T. (1992). *History of the Air Corps Tactical School 1920-1940.* Center for Air Force History, Washington, DC, p. 68.
40. Levine, A. J. (1992). *The Strategic Bombing of Germany, 1940-1945*. Praeger, Westport, CN, p. 9.
41. Ibid., 38.
42. Hansell, H. S. Jr. (1972). *The Air Plan that Defeated Hitler*. Higgins-McArthur/Longino & Porter, Inc., Atlanta, GA, p. 53.
43. Hansell, H. S. (1986). *Strategic Air War*, pp. 24–25.
44. Ibid., 30.
45. Hansell, H. S. (1972). *Air Plan*, p. 69.
46. Ibid., 79–80.
47. Ibid., 163.
48. Ibid., 144.
49. Ibid., 102.
50. Ibid., 147–153, 158.
51. Ibid., 158.
52. Ibid., 158–168.
53. Hansell, H. S. (1986). *Strategic Air War*, p. 141.
54. Ibid., 147, 167.
55. Ibid., 219.
56. Ibid., 177, 198.
57. Perera, G. R. (1944). *History of the Organization and Operations of the Committee of Operations Analysts, 16 November 1942–10 October 1944*, Air Force Historical Research Agency. Document 118.01, Volume II, Tab 22. This particular quotation was taken from the Memorandum to Lt Gen Arnold, 8 March 1943, Subject: Report of the Committee of Operations Analysts with Respect to Economic Targets Within the Western Axis.
58. (a) United States Strategic Bombing Survey. (1945). *The United States Strategic Bombing Survey Summary Report (European War)*. September 30, 1945, pp. 3–4; (b) United States Strategic Bombing Survey. (1946). *The United States Strategic Bombing Survey Summary Report (Pacific War)*. July 1, 1946, pp. 46–67. The versions of these reports cited in this paper are from the October 1987 reprint by Air University Press, Maxwell Air Force Base, AL.
59. Olson, M. Jr. (1962). The economics of target selection for the combined bomber offensive. *RUSI J.* **CVII**, 308–314.
60. USSBS, (1945). *Summary Report*, pp. 37–40.
61. Hansell, H. S. (1986). *Strategic Air War*, p. 125.
62. Mierzejewski, A. C. (1988). *The Collapse of the German War Economy, 1944-1945*. The University of North Carolina Press, Chapel Hill, NC, pp. 161–162.

63. Hansell, H. S. (1986). *Strategic Air War*, p. 130.
64. Ibid., 131–133.
65. Ibid., 122.
66. USSBS, (1946). *Summary Report*, pp. 77–82.
67. Ibid., 86–90.
68. Ibid., 110.
69. Hallion, R. P. (1992). *Storm Over Iraq: Air Power and the Gulf War*. Smithsonian Press, Washington, DC, pp. 9–10.
70. Ibid., 282–283. Table 2 is adapted from Hallion's Appendix Table 2, page 283.
71. Ibid., 174, 177.
72. Deptula, D. A. Brigadier General. (2001). Brigadier General, *Effects-Based Operations: Change in the Nature of Warfare*. Aerospace Education Foundation, Air Force Association, Arlington, VA, p. 7 (Figure 4).
73. For the military application of computer modeling to target selection, see Rinaldi, S. M. Major (1995). *Beyond the Industrial Web: Economic Synergies and Targeting Methodologies*, Masters Thesis, School of Advanced Airpower Studies. Air University Press, Maxwell AFB, AL.
74. A detailed examination and comparison of Boyd and Warden's theories can be found in Major Fadok, D. S. (1995). *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*, Masters Thesis, School of Advanced Airpower Studies. Air University Press, Maxwell AFB, AL.
75. Warden, J. A. III (1988). *The Air Campaign: Planning for Combat*. National Defense University Press, Washington, DC.
76. (a) Warden, J. A. III (1992). Employing air power in the twenty-first century. In *The Future of Air Power in the Aftermath of the Gulf War*, R. H. Shultz Jr., and R. L. Pfaltzgraff Jr., Eds. Air University Press, Maxwell AFB, AL, pp. 57–82; (b) Warden, J. A. III (1994). Air theory for the twenty-first century. In *Challenge and Response: Anticipating US Military Security Concerns*, K. P. Magyar Ed. Air University Press, Maxwell AFB, AL, pp. 311–332; (c) Warden, J. A. III (1995). The enemy as a system. *Airpower J.* **IX**(1), Spring, 40–55.
77. Metz, D. R. (1998). *The Air Campaign: John Warden and the Classical Airpower Theorists*. Air University Press, Maxwell Air Force Base, AL, pp. 142–143.
78. Author interview with Colonel Warden, J. A. III (1994). 28 March 1994, Maxwell AFB, AL.
79. Hallion, R. P. (1992). *Storm Over Iraq: Air Power and the Gulf War*. Smithsonian Press, Washington, DC, p. 151.
80. Ibid., 188–196.
81. Author recollection as an ACSC and SAAS student during the 1992-1994.
82. Hulst, G. R. Major (1993). *Taking Down Telecommunications*, Masters Thesis, School of Advanced Airpower Studies. Air University Press, Maxwell AFB, AL.
83. Wuesthoff, S. E. Major (1994). *The Utility of Targeting the Petroleum-Based Sector of a Nation's Economic Infrastructure*, Masters Thesis, School of Advanced Airpower Studies Air University Press, Maxwell AFB, AL.
84. Griffith, T. E. Major (1994). *Strategic Attack of National Electrical Systems*, Masters Thesis, School of Advanced Airpower Studies. Air University Press, Maxwell AFB, AL.
85. Tolbert, J. H. Major (2006). *Crony Attack: Strategic Attack's Silver Bullet?* Masters Thesis, School of Advanced Air and Space Studies. Air University Press, Maxwell AFB, AL.
86. Rinaldi, S. M. (1995). *Beyond the Industrial Web*.
87. Carpenter, M. P. Major et al. (1993). *Chaos Primer for the Campaign Planner*, unpublished student research paper. Air Command and Staff College, Maxwell AFB, AL.

88. DeBlois, B. M. Major, Reid, M. A. Major, Walsh, S. J. Major, Werner, S. J. Major and Combs, G. (1994). *Dropping the Electric Grid: An Option for the Military Planner*, student research paper, Air Command and Staff College. Air University Press, Maxwell AFB, AL.

89. Grant, R. (2007). *Victory in Cyberspace*. Air Force Association, Arlington, VA.

## FURTHER READING

Keysen, C. (1949). *Note on Some Historical Principles of Target Selection*, RAND Memorandum RM-189, July 15.

# NETWORK FLOW APPROACHES FOR ANALYZING AND MANAGING DISRUPTIONS TO INTERDEPENDENT INFRASTRUCTURE SYSTEMS

EARL E. LEE

*University of Delaware, Newark, Delaware*

JOHN E. MITCHELL AND WILLIAM A. WALLACE

*Rensselaer Polytechnic Institute, Troy, New York*

## 1 INTRODUCTION

The American way of life relies on the operations and interactions of a complex set of infrastructure networks. These networks include transportation, electric power, gas and liquid fuels, telecommunications, wastewater facilities, and water supplies. This set of civil infrastructures has also been included in the broader set of critical infrastructures defined by the USA Patriot Act of 2001 [1]. In the Patriot Act, critical infrastructures are those

> "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such would have a debilitating impact on security, national economic security, national public health or safety or any combination of these matters [1]."

Each of these infrastructure systems evolved independently. However as technology advanced, the systems became interconnected. The reliance of any of these systems

on electric power is obvious. Failures, by whatever cause, within the communications networks in one locale may have far-reaching effects across many systems.

Infrastructure management systems did not allow a manager of one system to "see" the operations and conditions of another system. Therefore, emergency managers would fail to recognize this "interconnectedness" or interdependence of infrastructures in responding to an incident, a fact recognized by *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* [2]. This research provides a model of this "system of systems." Each system is explicitly modeled and the manager could be provided with a familiar view of their system. Additionally, the model captures how these systems rely on each other. The model and its associated decision support system becomes a tool for emergency and system managers to improve post-disruption response and better understand vulnerability due to this interconnectedness. In the sections to follow, this article provides a brief discussion of the policy documents and past studies in system modeling; a description of the model and its associated decision support system; and an overview of how the model can be used for post-disruption system restoration and vulnerability analysis.

## 2 BACKGROUND/PAST STUDIES

This literature and past studies relevant to this research fall into one of the three categories. These are the policy documents, the past research on single system modeling, and the work involving modeling multiple systems or a system of systems. In the interest of brevity, a lengthy discussion of this past study is not being presented in this article. An extensive review of the literature relating to this study can be found in [3] and [4].

The policy documents [1, , 5–12] have framed the discussion, recognizing the need for models to aid in decision making and discussing how models can provide better understanding of the behavior of these complex, interconnected systems.

Single system research [13–25] has focused on mitigating disruptions due to willful act or natural events. In general, this work has not included detailed discussions on how these systems are vulnerable due to their reliance on other networks.

Past research [26–30] has also studied vulnerability and reliability as they relate to interconnected systems. Some of these have been at the macroscopic levels of detail that are suitable for analyses relating to system vulnerability, but would not easily translate to restoration activities following a disruptive event. Other work has focused on just two specific systems and are not easily extendable across the system of systems. Again, a more detailed discussion of this work is found in [4]. Models of national scale are being developed by the national laboratories and within Department of Homeland Security-sponsored research. These models are useful in assessing impacts to quality of life, the economy, and national security. They can also aid in developing national response strategies. However, they lack the detail to be useful in guiding system restoration or identifying system vulnerabilities within smaller regions, a gap which is filled by this research, which is discussed in the next section.

## 3 THE INTERDEPENDENT LAYERED NETWORK MODEL

This research has developed a formal, mathematical representation of the set of civil infrastructure systems that explicitly incorporates the interdependencies among them and

is called the *Interdependent Layered Network model* (ILN). The ILN is a mixed-integer, network-flow-based model, which is implemented in a software that enables the resulting model to be exercised. The detailed mathematical formulation of the model can be found in [3] and [4]. The ILN is embedded in a prototype decision support system, that is, Multi-Network Interdependent Critical Infrastructure Program for Analysis of Lifelines (MUNICIPAL). MUNICIPAL consists of a geographic information system (GIS) interface for the user, a database with the attributes of the set of infrastructures, the ILN module, and a vulnerability and system design module.

The model provides the capability to understand how a disruptive event affects the interdependent set of civil infrastructures. This capability improves a society's ability to withstand the impact of and respond to events that can disrupt the provision of services that are required for the health, safety, and economic well being of its citizens. Managers of infrastructure systems are able to assess the vulnerability of their own system due to its reliance on other systems. Organizations responsible for coordinating emergency response efforts will also be able to model different event scenarios and assess their impact across the full set of systems and the services they provide. With this broader perspective of impact, mitigation, and preparedness strategies can be formulated and evaluated for their ability to reduce their effects on society.

MUNICIPAL is not based upon a unique configuration of infrastructures, but is generic and therefore, applicable to more than one location. It is also not specific to a particular type of event, such as an earthquake or hurricane. The only requirements are that the event is of sudden onset and the event causes damage to the physical components of the infrastructure system.

The intended use of MUNICIPAL was for response and restoration efforts following a disruptive event and as a training tool for personnel who would be guiding response and restoration efforts. As the research progressed, MUNICIPAL was found to be useful in supporting system design, assessing the vulnerability of a system, measuring the benefits of pre-staging resources, or installing backup power systems, and even changing the physical design of the existing systems. This research has developed a network flow formulation of interdependent networks, which clearly identifies effects of a disruptive event across the set of infrastructure systems.

### 3.1 The General Construction of the Model

Interdependent infrastructures are viewed as networks, with movement of commodities (i.e. material) corresponding to flows and with services corresponding to a desired level of these flows. For ease of representation, each network, or infrastructure system, is defined as a collection of nodes and arcs with commodities flowing from node to node along paths in the network. Fundamentals of network flow problems are fairly uniform within the literature and texts on the subject [31].

For each commodity, each node is either a supply node which is a source for the commodity; a demand node which is a point that requires some amount of the commodity; or a transshipment node which is a point that neither produces nor requires the commodity but serve as a point through which the commodity passes. Arcs may, of course, have limited capacities. Infrastructure systems operate in an environment subject to disruptions. These disruptions could be caused by a natural phenomenon, human error or willful act. Based upon performance criteria, an infrastructure system can be designed to minimize possible service degradation following a disruption. In addition, once a disruption occurs,

alternative ways of restoring service can be determined. Included in the model are *flow conservation constraints* that (i) for supply nodes ensure that total flow out of the node is no greater than the available supply, (ii) for demand nodes ensure that demand is met, and (iii) for transshipment nodes ensure that flow into the node equals flow out of the node. The structural requirements are modeled by constraints on the capacities of arcs and transshipment nodes.

Network flow models can also be characterized as single-commodity or multi-commodity systems. Infrastructures such as water, power, gas, and sewer would be single-commodity systems, where material moves from one or more supply points, through a set of arcs and nodes, subject to constraints on capacity, and reaches one of more demand points in an optimal fashion. However, systems like transportation and telecommunications have additional requirements. In these cases, commodities moving across the system have specific origin and destination requirements. For example, passengers arriving at a subway station may each have unique destinations and the needs of each passenger must be met. However, these multiple commodities are not moving independently of each other. Associated with each origin–destination (O–D) pair is a market, the amount of a commodity which must flow between that O–D pair. Between each O–D pair is a set of possible paths. Each path is comprised of a subset of the arcs. The flows across all the paths for a particular O–D pair must equal the market. If the flow is less than the market, then there is an unmet demand for service. The flow on an arc is determined by summing the flows on all paths which contain the arc and is constrained by the arc's capacity.

One common formulation of a network flow model is the minimization of service delivery (minimum cost incurred to move the material across the arcs) while minimizing the unmet demands for service. Following a disruption, the flow into demand nodes may be insufficient. This unmet demand is commonly referred to as slack. At points of interdependency, this unmet demand occurs at the parent node. In the case of a pump and motor combination, the motor would be the parent node and the pump would be the child node (the node in the dependent system which is relying on the parent node in order to be able to deliver service). All demand nodes in every system would be provided a weighting factor, indicating their relative importance. These weights could be decided on well in advance of a disruptive event and would let system and emergency managers decide the relative importance of various demands for service. These weights would tend to push service toward those with higher importance. The weights would also guide restoration (discussed later in this article) by focusing priority on these high importance nodes. How managers would decide on the importance of one facility or area over another, considering social factors and critical service needs, is a topic for future study and is not included in this article.

### 3.2 Types of Interdependence

Rinaldi et al. [9] formalized the definitions of interdependence within this ongoing discussion of critical infrastructure and defined four classes of interdependency. Due to the number of different types of dependencies and interdependencies, these authors classified the entire family of interrelationships among systems as interdependencies, an approach retained in this article. This research identified five types of interrelationships between infrastructure systems—input, mutual, shared, exclusive-or, and co-located. A discussion of these is provided below. The mathematical details of each can be found in [3] and [4].

### 3.3 Input

An infrastructure is input interdependent when it requires as input one or more services from another infrastructure in order to provide some other service. In the case of a telephone switching station, the switching station itself is a transshipment node within the telecommunications network. However, this same switching station, from the perspective of the electrical network, is seen as a demand node since it needs an adequate source of electricity to operate. If insufficient power is available for the switching center, then it will be unable to operate and this change of capacity will affect the telecommunications system. The effect on any set of systems can be analyzed in a similar manner.

The existence of slack at a parent node of interdependent systems acts as a control switch for a connector variable. This binary connector variable works to turn the child node on or off, altering its capacity, depending on the conditions at the parent. When a parent node has unmet demand, the corresponding capacity of its child node in the dependent system is reduced. (Note that some interdependent infrastructure system failures may result in reducing the system's capacity to some value other than zero. For example, loss of supervisory control systems in a subway system may result in operators exercising greater care and slowing trains. So the post-disruption capacity may be lower than normal.)

### 3.4 Mutual

A collection of infrastructures is said to be mutually interdependent if at least one of the activities of one infrastructure system is dependent upon any other infrastructure system and at least one of the activities of this other infrastructure system is dependent upon the first infrastructure system. Consider a natural gas system compressor and a gas-fired electric power generator. From the perspective of the natural gas system, the compressor is a transshipment node and the generator is a demand node. From the perspective of the electrical network, the generator is a supply node and the compressor is a demand node. The generator needs gas to produce electricity; the compressor needs electric power to deliver gas through the system to the generator. If the compressor were to fail, supply of gas to the generator would be inadequate. If the capacity of the generator is set to zero, all flows on the arcs (i.e., the power lines) leaving the generator would be zero. Alternately, a lack of power at the compressor's demand node in the electrical generating network causes its capacity to be set to zero. To correct his situation, either an alternate source of gas must be found for the generator or an alternate source of power must be found for the compressor.

### 3.5 Shared

Shared interdependence occurs when some physical components and/or activities of the infrastructure used in providing the services are shared. Phone lines could be considered in the shared interdependence. Each phone line carries two types of calls, incoming and outgoing. Therefore, if a cable section contains 50 lines, they could be 50 incoming calls or 50 outgoing calls or some combination totaling 50. This type of interdependence is common in modeling of multicommodity systems. This is modeled mathematically by limiting the sum of the flows of the various commodities across the component to not exceed the total capacity.

### 3.6 Exclusive-Or

Exclusive-or interdependence occurs when multiple services share infrastructure component(s), but the component can only be used by one service at a time. In the first few days following the World Trade Center (WTC) attacks, streets (i.e., shared components) could not be used by both the emergency response personnel and financial district workers. This conflict had to be resolved prior to reopening the New York Stock Exchange [32]. Exclusive-or interdependencies are modeled by selecting additional constraints to restrict flow to one commodity or the other.

### 3.7 Co-Located

The co-located interdependency occurs when any of the physical components or activities of the civil infrastructure systems are situated within a prescribed geographical region. It was previously noted that managers of individual infrastructure systems would identify the components of their respective system at or near the site of the incident that may have been affected by the event. Based on further investigation, the status of these components will be adjusted. However, since only those emergency response agencies who are responsible for coordinating activities across multiple agencies maintain the complete view of all civil infrastructure systems, it is ultimately their responsibility to ensure that all co-located interdependencies have been considered and the models of the affected infrastructures revised as appropriate.

## 4 THE COMPONENTS OF MUNICIPAL

### 4.1 The User Interface and Database

A GIS was selected as the user interface as this seemed to be the most natural method of displaying systems and determining affected areas. The interface allows the operator to update the conditions of the modeled systems' components and to add temporary systems during restoration and when the display areas are affected by inabilities to meet demands.

The database contains the component attributes such as name, their capacity and their priority, as well as spatial attributes such as location and length. These spatial characteristics are generated automatically by the GIS software, ESRI's ArcGIS [33] in this case. The remaining attributes are added by the modeler. Changes to attributes, caused by disruption, can easily be made.

### 4.2 The Manhattan Dataset

In Manhattan, the goal was to develop highly detailed models in the area south of 60th Street of the power, telecommunications and subway systems, three major infrastructure systems impacted by the September 11 attacks. While unable to obtain details on specific components and their locations, Consolidated Edison, Verizon, and the Metropolitan Transit Authority were very open in discussing the general construction and operation of their respective systems and have provided a feedback during the model's construction. The subway system includes 115 stations and 338 local and express track sections. The phone system includes 18 switching centers and their associated service areas, 72 controlled environmental vaults where distribution cables are joined into larger feeder

cables and all the associated wiring. Below Canal St, approximately 500 blocks of phone service were modeled in detail. The power system as modeled includes 16 substations and 32 service areas. Each substation distributes power along 8–24 feeders to 18 phone switching centers, 178 AC/DC rectifiers for the subways, and service to all residences and businesses in the area.

## 5 USING MUNICIPAL DURING SYSTEM DISRUPTIONS

When an event occurs which disrupts any of the infrastructure systems included in MUNICIPAL, the operators would first use the GIS interface to identify components in and around the area of the disruption that may have been affected. Crews could then be dispatched to determine the actual condition of these possibly affected components. Outage reports from customers could also be entered in a separate database and linked to the GIS. On-scene reports would ascertain the actual condition of these components and the GIS would be used to update the component database. The operator would update the capacity of links and nodes based upon these reports.

With the direct impact of the disruption entered, MUNICIPAL can be run to determine where demands for service are not being met. In the case of the Manhattan data set, these unmet demands could include the number and location of electric power outages, number of telephone system calls that cannot be completed, and the number of subway system passengers who cannot reach their destinations. These outages would be due to failures of components in a system as well as outages caused by failure between interdependent systems.

With the full extent of the disruption modeled, the operators can use MUNICIPAL to begin restoration planning. Priorities can be set for each customer outage and plans can be developed in a collaborative environment. A complete example of the use of MUNICIPAL for a disruption is found in [3] and [4]. When a restoration plan is decided upon, MUNICIPAL can then develop work schedules based upon available resources, cost, and priorities.

## 6 USING MUNICIPAL FOR VULNERABILITY ANALYSIS

System managers are limited in their ability to evaluate the resilience of the systems they control because they cannot take into account the interdependencies of their systems with other infrastructures. In Lee et al. [34] and in [3], a procedure was introduced to evaluate the vulnerability of current or proposed designs of infrastructures that considers their interdependence to other systems. This procedure allows a system engineer to evaluate existing paths which are considered to provide redundancy for example, two existing paths in a telecommunications network between two important government or corporate offices. Since these two paths do not share any telecommunications components, they would appear to be redundant. However, using MUNICIPAL and its interconnected system model, the system engineer can conduct a backward trace into each system that telecommunications relies on. If these backward traces find single components in other systems whose failure causes both telecommunications paths to fail, then no redundancy has been provided. Examples could include single points in a power system that could lead to failure of redundant paths in telecommunications or single

components in a gas system that provide fuel to both the normal and backup generators for a facility or region.

MUNICIPAL can also aid in designing redundant paths. By conducting its backward trace along any path considered vital into all systems the path relies on, MUNICIPAL can be used to determine if a new, redundant path can be provided, utilizing the components not used by the current path and new connections or components, when appropriate.

## 7 CONCLUSIONS

This article has provided an overview of the ILN and MUNICIPAL and the capabilities of each. Our research continues and includes alternative formulations and solvers, extension of the study from the civil infrastructure systems to service systems such as supply chains and public safety. There is also an intent to improve the method by which priorities are established during system restoration, based upon methods found in the social sciences and economic impacts. Future research will also include the improvement of the decision support system and user interfaces.

## ACKNOWLEDGMENT

The authors wish to acknowledge the valuable assistance of the Manhattan offices of Consolidated Edison and Verizon, as well as the New York City Office of Emergency Management and the New York State Emergency Management Office. This study was supported by the National Science Foundation under Grant CMS 0139306, Impact of the World Trade Center Attack on Critical Infrastructure Interdependencies; Grant DMII 0228402, Disruptions in Interdependent Infrastructures: A Network Flows Approach; and Grant CMS 0301661, Decision Technologies for Managing Critical Infrastructure Interdependencies.

## REFERENCES

1. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001* , Public Law 107-56, October 26, (2001).
2. The White House. (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, Washington, DC.
3. Lee, E. E. (2006). *Assessing Vulnerability and Managing Disruptions to Interdependent Infrastructure Systems: A Network Flows Approach*, Doctoral Thesis, Department of Decision Sciences and Engineering Systems, Rensselaer Polytechnic Institute, Troy, NY.
4. Lee, E. E., Mitchell, J. E., and Wallace, W. A. (2007). Restoration of services in interdependent infrastructure systems: a network flows approach. *IEEE Trans. Syst. Man Cybern. C Appl. Rev.* **37**(6), 1303–1317.
5. Office of Homeland Security. (2002). *The National Strategy for Homeland Security*, Washington, DC.
6. President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations—Protecting America's Infrastructures*, October, 1997. Available from www.ciao.gov.
7. The White House. (1998). *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998, Washington, DC.

8. National Research Council. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. The National Academy Press, Washington, DC.
9. Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Contr. Syst. Mag.* **21**(6), 11–25.
10. Heller, M. (2001). Interdependencies in civil infrastructure systems. *The Bridge* **31**(4), 9–15.
11. Little, R. (2002). Controlling cascading failure: understanding the vulnerabilities of interconnected infrastructures. *J. Urban Technol.* **9**(1), 109–123.
12. Robinson, C. P., Woodard, J. B., and Varnado, S. G. (1998). Critical infrastructure: interlinked and vulnerable *issues*. *Sci. Technol.* **15**(1) 61–68.
13. Hasse, P. (2001). Of horseshoe nails and kingdoms. *EPRI J.* Spring, 1–10.
14. Amin, M. (2000). Toward self-healing infrastructure systems. *Computer* **33**(8) 44–53.
15. Amin, M. (2000). Modeling and control of Electric Power Systems and Markets. *IEEE Contr. Syst. Mag.*, **20**(4) 20–24.
16. Amin, M. (2001). Toward self-healing energy infrastructure systems. *IEEE Comput. Appl. Pow.* **14**(1), 20–28.
17. Amin, M. (2002). Toward secure and resilient interdependent infrastructures. *J. Infrastruct. Syst.* **8**(3) 67–75.
18. Amin, M. (2002). Modeling and control of complex interactive networks. *IEEE Contr. Syst. Mag.*, **22**(1) 22–27.
19. Salmeron, J., Wood, K., and Baldick, R. (2004). Analysis of electric grid security under terrorist threat. *IEEE Trans. Power Syst.* **19**(2), 905–912.
20. Haimes, Y. Y., Matalas, N. C., Lambert, J. H., Jackson, B. A., Fellows, J., (1998). Reducing vulnerability of water supply systems to attack. *J. Infrastruct. Syst.* **4**(4), 164–177.
21. National Petroleum Council Committee on Critical Infrastructure Protection. (2001). *Securing Oil and Natural Gas Infrastructures in the New Economy*, Washington, DC.
22. Kuhn, D. R. (1997). Sources of failure in the public switched telephone network. *Computer* 31–36.
23. Klincewicz, J. G. (1998). Hub Location in backbone/tributary network design: a review. *Location Science* **6**(1), 307–355.
24. Chamberland, S. and Sanso, B. (2001). On the design of multitechnology networks. *INFORMS J. Comput.* **13**(3), 245–256.
25. Cremer, J., Rey, P., and Tirole, J. (2000). Connectivity in the commercial internet. *J. Ind. Econ.* **48**(4), 433–472.
26. Haimes, Y., and Jiang, P. (2001). Leontief-based model of risk in complex interconnected infrastructures. *J Infrastruct. Syst.* **7**(1), 1–12.
27. Haimes, Y. Y., Horowitz, B. M., Lambert, J. H., Santos, J. R., Lian, C., and Crownther, K. G., (2005). Inoperability input-output model for interdependent infrastructure sectors. *J. Infrastruct. Syst.* **11**(2), 67–79.
28. Carullo, S. P., and Nwankpa, C. O. (2003). Experimental studies and modeling of an information embedded power system. In *36th Hawaii International Conference on System Sciences*. IEEE, Hawaii.
29. Holmgren, Å., Molin, S., and Thedéen, T. (2001). Vulnerability of complex infrastructure. *The 5th International Conference on Technology, Policy and Innovation*, Delft, The Netherlands.
30. Jha, S., and Wing, J. M. (2001). Survivability analysis of networked systems. *Proceedings - The 23rd International Conference on Software Engineering*, Toronto, Ontario, Canada, pp. 307–317.
31. Ahuja, R. K., Magnanti, T. L., and Orlin, J. B. (1993). *Network Flows: Theory, Algorithms and Applications*. Prentice Hall, Englewood Cliffs, NJ.

32. Lohr, S. (2001). Financial district vows to rise from the ashes. In *New York Times*, New York, NY, pp. A-6.

33. ESRI. (2004). *ArcGIS*. ESRI, Redlands, CA.

34. Lee, E. E., Mitchell, J. E., and Wallace, W. A. (2004). Assessing vulnerability of proposed designs for interdependent infrastructure systems. *37th Hawaii International Conference on System Science*, Hawaii.

# SOCIAL AND BEHAVIORAL RESEARCH

# SOCIAL AND PSYCHOLOGICAL ASPECTS OF TERRORISM

FATHALI M. MOGHADDAM AND NAOMI LEE
*Georgetown University, Washington, D.C.*

## 1 INTRODUCTION

Claims that "one person's terrorist is another person's freedom fighter" have made it notoriously difficult to define terrorism [1]. From a social psychological perspective, terrorism can be defined as *politically motivated violence, perpetrated by individuals, groups, or state-sponsored agents, intended to bring about feelings of terror and helplessness in a population in order to influence decision making and to change behavior* [Reference 2, p. 161]. Social and psychological processes are at the heart of terrorism, because it is through bringing about particular feelings and perceptions (terror and helplessness) that terrorists attempt to change actual behavior of victim individuals and societies.

## 2 SOCIAL ROOTS OF TERRORISM

In order to explain why people commit terrorist acts, a variety of socio-psychological explanations have been put forward [3, 4]. These include irrationalist explanations influenced by Freud, as well as rationalist, materialist explanations. An overlooked factor is functionality: terrorism is adopted as a tactic because it sometimes works effectively. For example, it is generally agreed that the March 11, 2004, terrorist attacks in Madrid, resulting in close to 200 deaths and over 1000 serious injuries, led to the ruling party in Spain being voted out of power because of their close alliance with the Iraq policies of the Bush administration. Of course, this kind of political impact tends to be short term and limited in scope.

In this discussion, our focus is on terrorism carried out by fanatical Muslims, particularly violent Salafists, because at the dawn of the twenty-first century this type of terrorism poses the greatest threat at the global level, as reflected by the focus of research [5–12]. On the other hand, other types of terrorism, such as by members of Euskadi ta Askatasuna, Basque Homeland and Freedom (ETA) in Spain or the Tamil Tigers in Sri

Lanka, have not ended, but tend to be confined to particular regions and separatist causes, and are a less serious threat globally.

We outline the social and psychological aspects of terrorism in two main parts. First, we examine the roots of terrorism; second, we explore the consequences of terrorism. In order to better understand the roots of terrorism, it is useful to adopt a staircase metaphor [3]: imagine a narrowing staircase winding up a multistory building. Everyone begins on the ground floor, and it may be that people are sufficiently satisfied with conditions to remain on the ground floor. However, under certain conditions, people will feel they are being treated unjustly and some individuals will start climbing up the staircase, searching for ways to change the social–economic–political situation.

The climb up the staircase to terrorism involves radicalization. The challenge is to transform the conditions, to facilitate deradicalization, so that people are not motivated to climb up, and those who have climbed up become motivated to climb back down.

The weight of evidence suggests that contextual rather than dispositional factors best explain movement up and down the staircase to terrorism (e.g. see 13–15). Terrorism is not explained by psychopathology, illiteracy, or poverty [3, 16, 17]. Under certain conditions, individuals with "normal" psychological profiles will do harm to others [18]. The staircase metaphor helps to highlight the role of context, as well as the psychological processes that characterize thought and action on each floor of the staircase to terrorism.

### 2.1 Radicalization: Moving Up the Staircase

Radicalization typically involves a step-by-step process, well documented in almost a century of research on conformity and obedience (see Reference 19, Articles 15 and 16). As individuals move up the staircase, step-by-step, they gradually adopt those attitudes, beliefs and morality that condone terrorism, and some of them eventually become recruited to carry out terrorist attacks. This process begins with the radicalization of entire communities on the ground floor.

*Ground floor*. The ground floor is occupied by about 1.2 billion Muslims. Psychological processes central to thought and action on this floor are relative deprivation and identity.

In the Near and Middle East, as well as in North Africa—including other important Islamic countries such as Egypt, Saudi Arabia, and Pakistan—Muslims are ruled by governments that cannot be voted out by popular will, yet they are supported by Western powers (e.g. United States). This support comes in the form of political and military interventions (as in the case of Kuwait and Saudi Arabia) and economic aid (as in the case of Egypt and Pakistan). Oil producing countries have suffered from an "oil paradox" [Reference 3, pp. 74–76): instead of improving the lives of the masses, oil revenue has allowed despotic ruling groups, such as the Saudis, to pay for a stronger security apparatus and to win the support of Western powers through enormous arms purchases and promises of reliable, cheaper oil supplies.

Two factors have helped to raise expectations and to create fraternal (collective) relative deprivation among the populations on the ground floor. First, the global mass media has presented the impoverished Islamic masses with images of an opulent life that is available to people in some countries. Secondly, Western politicians have promised

democratization and reform. Consequently, the expectation has been raised among the Islamic masses for great choice and greater participation.

In practice, most people in the Near and Middle East lack choices both in economic and political spheres. In the economic arena, wealth disparities are enormous and the standard of educational and social services have remained poor. In the political sphere, little actual progress has been made toward giving people a voice in government, although there has been considerable publicity about "democratic changes" in places such as Egypt and Saudi Arabia.

Globalization has also helped to create an identity crisis in Islamic communities [3]. In the midst of social–economic–technological global changes, one set of extremists in Islamic societies are urging the abandonment of traditional life-styles and the copying of the West; other extremists push for a return to "pure Islam" as it was (supposedly) practiced in its original form 1400 years ago. The "become copies of the West" strategy has led to the "good copy problem" [3] because following this option means Muslims will lack an authentic identity, and at best can only become "good copies" of a Western ideal. The "return to pure Islam" option is also associated with enormous problems because it is being used by fundamentalists to implement regressive interpretations of Islam.

An alternative, secular "middle ground" needs to be constructed, but for this to happen the governments of Islamic societies must allow greater political freedom. At present, procedures to allow people to participate in decision making about the cultural, social, economic, and political future of their societies are still not in place. Social psychological research suggests that procedural justice is vitally important, and influences how fair people believe a system is, independent of the actual outcome of decision making.

*First floor*. Individuals climb to the first floor particularly motivated to achieve individual mobility, and central to their experiences is procedural justice. The importance of openness and circulation has been emphasized by thinkers from Plato to modern theorists: closed systems lead to corruption, a sense of injustice, and eventual collapse [2]. Individuals who feel that paths for progress are not available, now move further up the staircase.

*Second floor*. Those who arrive on the second floor are experiencing tremendous frustration because the paths to change and improvement seem blocked to them. They become vulnerable to the influence of radical preachers as well as government propaganda, displacing aggression onto Westerns, the United States and Israel in particular, as the "cause of all problems". Research demonstrates that displacement of aggression is a powerful factor in redirecting frustrations onto external targets [20].

*Third floor*. Individuals who climb to the third floor already perceive their own societies to be unjust, and perceive external targets (particularly the United States) as the root cause of injustice. On the third floor, these individuals gradually "disengage" from moderate policies and morality, and engage with a morality supportive of terrorism, often seeing terrorist tactics as the only weapon at the disposal of Muslims fighting for justice.

*Fourth floor*. Recruitment takes place on the fourth floor, where individuals become integrated into the culture of small, secretive terrorist cells. The new recruits are trained to view the world in a rigidly categorical, us versus them, good versus evil manner, and to see the terrorist organization as legitimate. Unfortunately, the categorical thinking of extremist Islamic groups tends to mirror, and be reinforced by, the categorical "us versus them" thinking of extremists in the West.

*Fifth floor*. In the animal kingdom, intraspecies aggression is limited by inhibitory mechanisms brought on by one animal's display of submission to another. Inhibitory mechanisms prevent serious injury and death. In order to carry out terrorist acts, often resulting in multiple deaths and injuries, individuals must learn to sidestep the inhibitory mechanisms that function to prevent human aggression under normal circumstances. This "learning" takes place on the fifth floor, and in part involves further distancing and dehumanizing of targets. Having to live in isolation, separated from the rest of society by secrecy and fear, results in even tighter bonds within terrorist cells.

### 2.2 Deradicalization: Moving Down the Staircase

Using the staircase metaphor, as well as insights from earlier research on deradicalization [16, 21, 22], we arrive at important general guidelines for deradicalization programs.

First, research suggests that for any given individual, the path to deradicalization is not necessarily the opposite of the path that person took to radicalization; the path down is not always the same as the path up.

Secondly, deradicalization programs need to be designed for each set of individuals depending on the floor they have reached on the staircase to terrorism. For example, individuals on the top floor are ready to carry out terrorist attacks, and deradicalization can be most effective after the terrorist has been captured. However, individuals who reach the third floor are in the process of adopting terrorist morality, and they can be influenced by deradicalization programs without necessarily first being captured.

Thirdly, resources should be focused particularly on the ground floor, where the vast majority of people reside. International surveys reveal that the populations of many important Islamic societies have become radicalized on the ground floor [23]. This is associated with a rise in conspiratorial thinking. For example, in 2006 the percentages of people who believed that Arabs *did not* carry out the 9/11 attacks were: Indonesia 65%, Egypt 59%, Jordan 53%, and Pakistan 41%. In the traditionally "pro-Western" society of Turkey, the percentage of Muslims who expressed disbelief that Arabs carried out the 9/11 attacks went up from 43% in 2002 to 59% in 2006. In Egypt 28% and in Jordan 29% of Muslims believe that violence against civilian targets in order to defend Islam is sometimes justified [23]. These findings reflect a broad radicalization processes associated with some support for terrorism and generally higher anti-Western sentiment.

## 3 SOCIAL PSYCHOLOGICAL CONSEQUENCES OF TERRORISM

Research attention to the effects of terrorism on civil society and psychological well-being was ignited after the attacks of September 11, 2001. This research can be organized into three general topics: political attitudes, prejudice, and mental health.

### 3.1 Political Attitudes

Terrorism is associated with demonstrable changes in political attitudes, as both experimental studies and surveys have shown. Research linking terrorist attacks in support of more authoritarian political policies and abdication of civil liberties, is discussed.

Authoritarianism is a personality trait popularized by Adorno [24] and subsequently refined by Altemeyer [25] as consisting of submissiveness to authority, aggressiveness toward outgroups, and conventionalism. This personality trait appears to both predict people's responses to aggression and increase in response to aggression.

In a quasi-experimental study of the effects of Islamic terrorist attacks in Madrid (March 11, 2004), right-wing authoritarianism and conservatism were measured in Spanish citizens both before and after the attacks [26]. Right-wing authoritarianism increased, and Spanish citizens reported a stronger attachment to traditional conservative values. Since the study was quasi-experimental, a causal link between the attacks and changes in political beliefs could not be established. In a controlled laboratory experiment [27], the presence of a terrorist threat was manipulated. Results showed that the more authoritarian participants were prior to the threat, the less they supported democratic values, the more they supported military aggression. It was concluded that threats increase the activation of an authoritarian response.

Repeated attacks (whether terrorist or military) appear to elicit support for escalating retaliatory actions among young, voting-age US citizens in controlled experiments [28]. Retaliatory responses were stronger when the attacks were perpetrated by terrorists rather than a militia. The signing of a peace treaty prior to attacks led males to retaliate more than females, supporting the thesis that men act with vengeance after a transgression while women pursue conciliation. In all permutations of their experiment (terrorist vs. military attack, peace treaty vs. no peace treaty, democratic vs. nondemocratic adversary), repeated attacks corresponded with responses that eventually matched or surpassed the conflict level of the initial attack. These studies have important implications for policies designed to contain conflicts.

The issue of civil liberties in the context of the US "War on Terror" has received extensive media coverage. The scholarly literature on this topic, however, is limited to correlational analyses based on public polling. Although these analyses do not permit causal inferences, they are highly informative. In a review of all the major political polls conducted pre- and post-September 11th, 2001, US respondents expressed increased willingness to abdicate civil liberties, increased confidence in the government's ability to protect the United States from terrorist threats, and increased support for the use of ground troops in combating terrorism [29]. In the months following the attacks, however, perceived threat declined, as did support for surveillance of Americans' communications and respondents' confidence in the US government's ability to prevent future attacks.

### 3.2 Prejudice and Social Cohesion

Well-established social psychological research on intergroup relations demonstrates that people placed into groups will discriminate against outgroup members and favor ingroup members [30]. When placed into groups, people also exaggerate the homogeneity of their ingroup and its distinctiveness from outgroups. These effects are even present when groups are formed on the basis of such trivial dimensions as one's estimation of how many dots appear on a piece of paper. These well-established research findings provide a backdrop to reports of rising anti-Arab and anti-Muslim prejudice in the United States since September 11th, 2001.

Nearly all studies of prejudice in the United States concern White prejudice toward Blacks. This focus warrants broadening, particularly in the light of evidence suggesting that prejudice directed more toward Arabs than Blacks [31]. Both immediately after 9/11 and one year later, American college students reported higher levels of prejudice toward Arabs than Blacks. Those students with higher levels of media exposure displayed higher levels of overall minority prejudice, whether toward Arabs or Blacks. Anti-Arab prejudice was also higher among those who more strongly endorsed social hierarchies, more strongly identified as "American", and believed future terrorist attacks are likely [32].

Terrorism is also linked to increased social cohesion, as international research demonstrates. Akhahena [33] documented how the terrorist bombing in Kenya (August 1998) helped Kenyans forge a new national identity that united previously fractured social identities. A negative aspect of increased social cohesion, however, is decreased intergroup contact. Persistent violence between Catholics and Protestants in Northern Ireland over the past 30 years has led to segregation in the areas of education, residence, and personal life. This segregation limits contact between Catholic and Protestant communities and arguably plays a major role in maintaining intergroup conflict [34].

### 3.3 Mental Health

Mental health has been the most intensively researched aspect of terrorism's psychological consequences, with posttraumatic stress disorder (PTSD) comprising the majority of studies. The most common psychological effects of a traumatic event such as a terrorist attack are acute stress disorder (in the short term) and PTSD (in the longer term), with depression, anxiety disorders, and substance abuse as the next most frequent effects [35].

Which factors determine who will suffer psychologically after a terrorist attack? This matter has been disputed. Silver et al. [36] conducted a nationally representative longitudinal study of US residents' psychological response to the attacks of September 11th, 2001. They found that proximity or degree of exposure was not a necessary precondition for high levels of acute and posttraumatic stress symptoms at 2 weeks and 12 months post-9/11. These results indicate the need to study the effects of indirect exposure to terrorism. In contrast, Schlenger's [37] review of the major studies of psychological distress post-9/11 concluded that PTSD following the attack was concentrated in the New York City metropolitan area. Furthermore, PTSD prevalence was strongly associated with direct connection to the attacks. Though many adults across the United States were distressed by the attacks, Schlenger [37] concludes that much of this distress resolved over time without professional treatment.

It is important to recognize that the vast majority of mental health literature follows a Euro-American academic traditional and adopts a Western medical perspective. It follows that important cross-cultural differences in response to terrorism may exist that are not captured by predominant methods. De Jong [38], for instance, has asserted that the predominant diagnostic criteria (DSM-IV and ICD-10) are not always appropriate for non-Western cultures.

Research on the effects of terrorism is little, but growing. The more expansive literature on traumatic events such as war and natural disasters can complement and further enrich our understanding of terrorism's social psychological consequences.

## REFERENCES


1. Cooper, H. H. A. (2001). The problem of definition revisited. *Am. Behav. Sci.* **44**, 881–893.
2. Moghaddam, F. M. (2005a). The staircase to terrorism: A psychological exploration. *Am. Psychol.* **60**, 161–169.
3. Moghaddam, F. M. (2006). *From the Terrorists' Point of View: What They Experience and Why They Come to Destroy*, Praeger International Security, Westport, CT.
4. Pyszcznski, T., Solomon, S., and Greenberg, J. (2003). *In the Wake of 9/11: the Psychology of Terror*, American Psychological Association, Washington, DC.
5. Booth, K., and Dunne, T. Eds. (2002). *Worlds in Collision: Terror and the Future Global Order*. Palgrave Mamillan, New York.
6. Davis, J. (2003). *Martyrs: Innocence, Vengeance, and Despair in the Middle East*, Palgrove Macmillan, New York.
7. Kegley, C. W. Jr. Ed., *The New Global Terrorism: Characteristics, Causes, Controls*. Prentice Hall, Upper Saddle River, NJ.
8. Khosrokhavar, F. (2005). *Suicide Bombers: Allah's New Martyrs*, (Translator Macey, D. Ed). Pluto Press, London.
9. Pape, R. A. (2005). *Dying to Win: The Strategic Logic of Suicide Bombing*, Random House, New York.
10. Pedahzur, A. (2005). *Suicide Terrorism*, Polity Press, London.
11. Sageman, M. (2004). *Understanding Terror Networks*, University of Pennsylvania Press, Pennsylvania, PA.
12. Silke, A. Ed. (2003). *Terrorism, Victims, and Society: Psychological Perspectives on Terrorism and its Consequences*. Wiley, Hoboken, NJ.
13. Atran, S. (2003). Genesis of suicide terrorism. *Science* **299**, 1534–1539.
14. Bongor, B., Brown, L. M., Beutler, L. E., Breckenridge, J. N., and Zimbardo, P., Eds. (2006). *Psychology of Terrorism*. Oxford University Press, New York.
15. Stout, C. E. Ed. (2002). *The Psychology of Terrorism*, Vol. 4, Praeger Publishers, Westport, CT.
16. Horgan, J., and Taylor, M. (2003). *The Psychology of Terrorism*, Frank Cass & Co., London.
17. Ruby, C. L. (2002). Are terrorists mentally deranged? *Anal. Soc. Issues Public Policy* **2**, 15–26.
18. Zimbardo, P. (2007). *The Lucifer Effect: Understanding How Good People Turn Evil*, Random House, Inc., New York.
19. Moghaddam, F. M. (2005b). *Great Ideas in Psychology: A Cultural And Historical Introduction*, Oneworld, Oxford.
20. Miller, N., Pederson, W. C., Earlywine, M., and Pollock, V. E. (2003). A theoretical model of triggered displaced aggression. *Pers. Soc. Psychol. Rev.* **7**, 75–97.
21. Bernard, C. Ed. (2005). *A Future for the Young: Options for Helping Middle Eastern Youth Escape the Trap of Radicalization*. Rand Corporation, Santa Monica, CA.
22. Crenshaw, M. (1991). How terrorism declines. *Terrorism Polit. Violence* **3**, 69–87.
23. Pew Research Center. (2006). *Conflicting views in a divided world*. Retrieved at http://pewglobal.org/.
24. Adorno, T. W., Frenkel-Brunswik, E., Levinson, D. J., and Sanford, R. N. (1952/1982). *The Authoritarian Personality*, W.W. Norton & Company, Inc, New York.
25. Altemeyer, B. (1996). *The Authoritarian Spectre*, Harvard University Press, Cambridge, MA.

26. Echebarria-Echabe, A., and Fernández-Guede, E. (2006). Effects of terrorism on attitudes and ideological orientation. *Eur. J. Soc. Psychol.* **26**, 259–265.
27. Hastings, B. M., and Schaffer, B. A. (2005). Authoritarianism and sociopolitical attitudes in response to threats of terror. *Psychol. Rep.* **92**, 623–630.
28. Bourne, L. E., Helay, A. F., and Beer, F. A. (2003). Military conflict and terrorism: General psychology informs international relations. *Rev. Gen. Psychol.* **7**, 189–202.
29. Huddy, K., Khatib, N., and Capelos, T. (2002). Reactions to the terrorist attacks of September 11, 2001. *Public Opin. Q.* **66**, 418–450.
30. Taylor, D. M., and Moghaddam, F. M. (1994). *Theories of Intergroup Relations: International Social Psychological Perspectives*, 2nd ed., Praeger Publishers, Westport, CN.
31. Persson, A. V., Musher, E., and Dara, R. (2006). College students' attitudes toward blacks and Arabs following a terrorist attack as a function of varying levels of media exposure. *J. Appl. Soc. Psychol.* **35**, 1879–1893.
32. Oswald, D. L. (2006). Understanding anti-Arab reactions post 9/11: The role of threats, social categories, and personal ideologies. *J. Appl. Soc. Psychol.* **35**, 1775–1799.
33. Akhahenda, E. F. (2002). *When Blood and Tears United a Country: The Bombing of the American Embassy in Kenya*, University Press of America, Lanham, MD.
34. Campbell, A., Cairns, E., and Mallet, J. (2005). Northern Ireland: the psychological impact of "the Troubles". In *The Trauma of Terrorism: Sharing Knowledge and Shared Care. An International Handbook*, Y. Danieli, D. Brom, and J. Sills, Eds. Haworth Press, New York, NY, pp. 175–184.
35. Danieli, Y., Engdahl, B., and Schlenger, W. E. (2004). The psychosocial aftermath of terrorism. In *Understanding terrorism: Psychosocial roots, consequences, and interventions*, F. M. Moghaddam, and A. J. Marsella, Eds. American Psychological Association, Washington, DC, pp. 223–246.
36. Silver, R. C., Poulin, M., Holeman, E. A., McIntosh, D. N., Gil-Rivas, V., and Pizarro, J. (2004). Exploring the myths of coping with a national trauma: A longitudinal study of responses to the September 11th Terrorist Attacks. *J. Aggress. Maltreat. Trauma* **9**, 129–141.
37. Schlenger, W. E. (2004). Psychological impact of the September 11, 2001 terrorist attacks: Summary of empirical findings in adults. *J. Aggress. Maltreat. Trauma* **9**, 97–108.
38. De Jong, J. T. V. M. (2002). Public mental health, traumatic stress and human rights violations in low-income countries. In *Trauma, war, and violence: Public mental health in socio-cultural context*, J. T. V. M. De Jong, Ed. New York, Luwer Academic/Plenum Publishers, pp. 1–92.

## FURTHER READING

Alexander, Y. (2002). *Combating terrorism: Strategies of ten countries*, University of Michigan Press, Ann Arbor, MI.

Bloom, M. (2005). *Dying to Kill: The Allure of Suicide Terror*, Columbia University Press, New York.

Crenshaw, M., Ed. (1995). *Terrorism in Context*. Pennsylvania University Press, University Park.

Horgan, J. (2005). *The Psychology of Terrorism*, Routledge (UK), London.

Hunter, S. T., and Malik, H., Eds. (2005). *Modernization, Democracy, and Islam*. Praeger Publishers, Westport, CT.

McDermott, T. (2005). *Perfect Soldiers: The Hijackers-Who They Were, Why They Did It.*, Harper Collins Publishers, New York.

Moghaddam, F. M. and Marsella, A. J., Eds. (2004). *Understanding Terrorism: Psychosocial Roots, Consequences, and Interventions*. American Psychological Association, Washington, DC.

# HUMAN SENSATION AND PERCEPTION

ROBERT W. PROCTOR
*Department of Psychological Sciences, Purdue University, West Lafayette, Indiana*
KIM-PHUONG L. VU
*Department of Psychology, California State University, Long Beach, California*

## 1 INTRODUCTION

Sträter begins his book *Cognition and Safety* with the statement "Human society has become an information processing society" [1, p. 3]. This statement is as true for homeland security tasks as for any other tasks that require people to interact with machines and other people in complex systems. Homeland security involves people interacting with information technology, and use of this technology to communicate effectively is an important aspect of security [2]. For communication to be effective, human–machine interactions must conform to users perceptual, cognitive, and motoric capabilities. In particular, because all information that a person processes enters by way of the senses, sensory and perceptual processes are going to be critical factors. These processes are relevant to detecting a weapon in luggage during screening, identifying vulnerable targets for which risk is high, and communicating warnings to individuals. Given the masses of data extracted from intelligence gathering activities of various types, these data need to be integrated and displayed to appropriate security personnel in an easy to perceive form at the proper time. These and other aspects of homeland security systems require an understanding of fundamental concepts of sensation and perception.

## 2 BACKGROUND

Much is known about the methods for studying perception, the structure and function of the sensory systems, and specific aspects of perception such as the role of attention [3]. Understanding how people sense, perceive, and act on the information they receive is essential for homeland security because many of the surveillance tasks involve monitoring, detecting, and reporting events.

This article provides an overview of sensation and perception, with emphasis on topics that seem relevant to homeland security. Five sensory modalities are typically distinguished: vision, hearing, touch, smell, and taste—all of which are relevant to certain aspects of homeland security. For the sake of brevity, we cover vision and hearing in most detail, describing the other senses only briefly. The reader is referred to longer and more specialized review chapters [4], as well as to textbooks on sensation and perception [3].

All sensory systems have receptors that convert physical stimulus energy into electrochemical energy in the nervous system. The sensory information is coded in the activity of neurons and travels to the brain via structured pathways consisting of interconnected

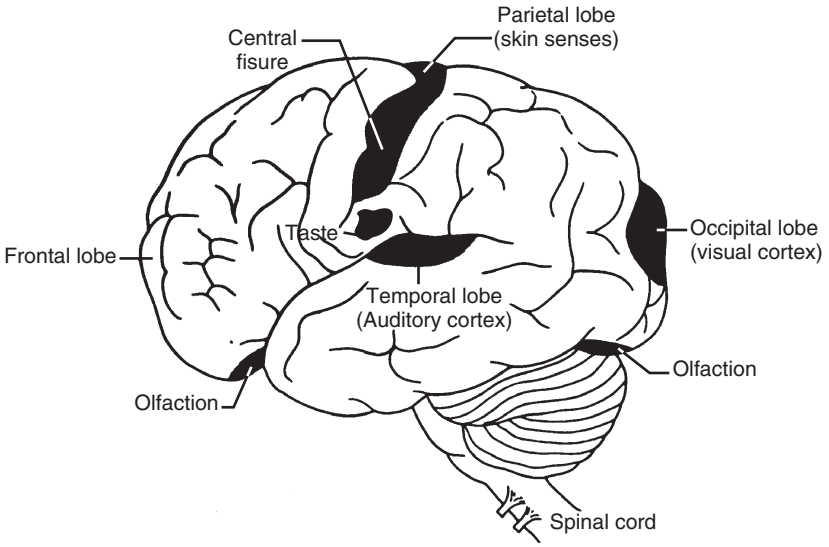



**FIGURE 1** Illustration of the primary sensory receiving areas in the cerebral cortex.

networks of neurons. For most senses, two or more pathways operate in parallel to analyze and convey different kinds of information from the sensory signal. The pathways project to primary receiving areas in the cerebral cortex (Fig. 1) and then to many other areas within the brain.

The study of sensation and perception involves not only the anatomy and physiology of the sensory systems, but also behavioral measures of perception. Psychophysical data obtained from tasks in which observers detect, discriminate, rate, or recognize stimuli provide information about how the properties of the sensory systems relate to what is perceived. They also provide information about the functions of higher-level brain processes that interpret the sensory input through mental representation, decision-making, and inference. Thus, perceptual experiments provide evidence about how the sensory input is organized into a coherent percept on which actions are based.

## 3 METHODS FOR INVESTIGATING SENSATION AND PERCEPTION

Many methods for studying sensation and perception exist. We emphasize behavioral and psychophysiological methods because of their relevance to homeland security.

### 3.1 Threshold Methods and Scaling

Classical psychophysical methods for measuring detectability and discriminability of stimuli are based on the concept of a threshold, the minimum amount of stimulation necessary for an observer to detect a stimulus (absolute threshold) or distinguish a stimulus from another one (difference threshold). Examining how thresholds change in different settings can tell us much about perception and whether specific stimuli such as alarms

may be effective. Many techniques have been developed for measuring thresholds in basic and applied settings [5].

Classical psychophysics also provides methods for building scales of perceived magnitude [6]. Indirect methods construct scales from an observer's accuracy at discriminating stimuli, whereas direct methods construct scales from an observer's magnitude estimates. Scaling methods can be used to quantify perceptual experience on any dimension that varies in magnitude, such as perception of risk. They can be used as design tools in development of new methods for displaying information, for example, data sonifications (representations of data by sound; [7]).

### 3.2 Signal Detection Methods

An observer's judgments, when stimuli are difficult to detect or discriminate, are influenced by the willingness to give one response or another. Signal detection methods allow measurement of this response criterion, or bias, separately from detectability or discriminatiblity [8]. Situations for which signal detection is applicable involve a "signal" (e.g. a weapon in luggage) that an observer must discriminate from "noise" (e.g. other items in luggage). If the observer is to respond "yes" when a signal is present and "no" when it is not, the outcome can be classified as a hit ("yes" to signal), false alarm ("yes" to noise), miss ("no" to signal), or correct rejection ("no" to noise). Measures of detectability (how accurately a weapon can be discriminated from other items) can be calculated based on the difference between hit and false alarm rates, and measures of response bias (the tendency to open the luggage regardless of whether a weapon is present) on overall rate of responding "yes" versus "no".

For a given level of detectability, the possible combinations of hit and false-alarm rates vary as a function of the observer's response criterion. For example, immediately after a terrorist attempt, screeners may adopt a liberal criterion and open any luggage that they think might possibly contain a weapon, yielding a high hit rate coupled with a high false alarm rate. Detectability can be improved by providing better screening equipment and operator training, whereas a desired response bias can be induced by an appropriate reward system. Signal detection methods and theory provide powerful tools for investigating and conceptualizing performance of other security-related tasks such as maintaining vigilance [9].

### 3.3 Psychophysiological Methods and Brain Imaging

Methods for measuring physiological reactions to stimuli are useful in studying perception [10]. Measures of electrical brain activity, electroencephalograms, can be recorded from the scalp. Event-related potentials, which measure brain activity locked to an event such as stimulus onset, provide detailed information about the timecourse of brain activation. Functional neuroimaging techniques, which measure brain activity indirectly through bloodflow, provide insight into the spatial organization of brain functions. These methods can be used to determine whether a particular behavioral phenomenon has its locus in processes associated with sensation and perception or with subsequent response-selection and execution. Their use for applied purposes is being explored in the areas of neuroergonomics [11] and augmented cognition [12], which have the goals of implementing

and adapting high-technology interfaces to facilitate communication of large amounts of information.

## 4 VISION

Vision is arguably the most vital sense for interacting with the world. It provides detailed information about objects in the surrounding environment, and their locations and movements. Complex information can be depicted in high fidelity displays that mimic the external environment, more abstract graphical formats that represent data or interactions among system components, and alphanumerically to convey verbal messages and numerical values.

### 4.1 Visual Sensory System

The stimulus for vision is light energy generated by, or reflected from, objects in the environment. Light travels in waves, with the wavelengths of the visual spectrum varying from 400 to 700 nm. Light enters the eye through the cornea and passes through the pupil and lens (Figure 2). The pupil adjusts between 8 and 2 mm diameter in dim and bright light, respectively, allowing a larger percentage of light to enter when it is scarce. The cornea and lens focus images on the photoreceptors, located on the retina at the back of the eye. The cornea provides a fixed focusing power, and the lens changes its shape through a process of accommodation to provide increased focusing power as the distance of a fixated object changes from far to near. The amount of rotation of the eyes inward, the vergence angle, also increases as the distance of a fixated object is reduced. Because accommodation and vergence require muscular activity, tasks that necessitate rapid and numerous changes in them will cause visual fatigue.

The retina contains two types of photoreceptors, rods and cones, which have photopigments that begin a process of converting light into neural signals. Rods are responsible for night vision and do not support color perception. Cones are responsible for daylight vision and for perception of color and detail. The image of a fixated object will fall on the fovea, a small retinal region containing only cones. The retina also contains another region, the blind spot, where the optic nerve leaves the eye and there are no photoreceptors.

The nerve fibers leaving the eye form two pathways. One is devoted to rapid transmission of global information across the retina. It carries high temporal frequency information

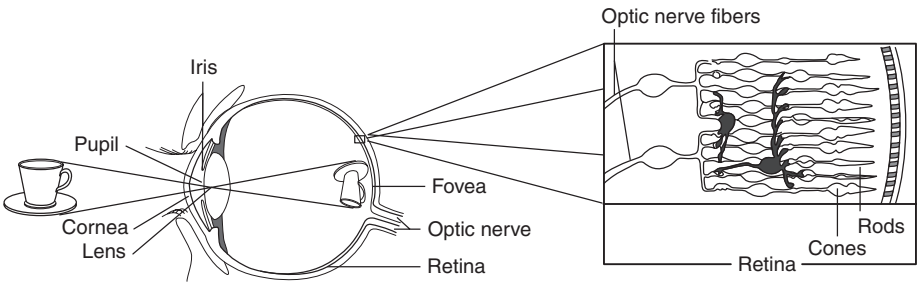



**FIGURE 2** Illustration of the primary structures of the eye, with an object's image focused on the retina. (Adapted from E. B. Goldstein (2002). /Sensation and Perception/ (6th ed.). Pacific Grove, CA: Wadsworth.)

needed for motion perception and detection of abrupt changes. The other is devoted to slower transmission of detailed features from the fovea and plays a role in color and pattern perception.

The optic nerve projects into the lateral geniculate nucleus and then into the primary visual cortex, located at the back of the brain. More than 30 cortical areas subsequent to the primary visual cortex are involved in the processing of visual information [13]. Two different pathways play distinct roles in perception. The ventral pathway, which goes to a region in the temporal lobe, is involved in identifying objects. The dorsal pathway, which goes to a region in the parietal lobe, is involved in determining where objects are located. This dissociation of what and where processing affects performance as well; for example, navigational tasks that rely on "where" information are performed well under low lighting levels at which pattern recognition is impaired [14].

### 4.2 Visual Perception

Sensitivity to light increases for a period after entering the dark (see Figure 3). Several factors contribute to this dark-adaptation process: larger pupil size, photopigments returning to a light sensitive state, and shift from cones to rods. Because cones have a spectral sensitivity function that peaks at higher wavelengths than that for rods, short wavelength stimuli appear relatively brighter when dark adapted. Displays intended for use in the field need to be designed with the different sensitivities of day and night vision taken into account.

Acuity is high in the fovea and decreases as stimulus location becomes more peripheral. The acuity function is due to the density of cones being greatest in the fovea (see Figure 4) and to less convergence of foveal than peripheral photoreceptors in the sensory pathway. Acuity can be measured in several ways, including with a standard Snellen eye chart, that are not perfectly correlated. Resolution acuity can be specified by a spatial

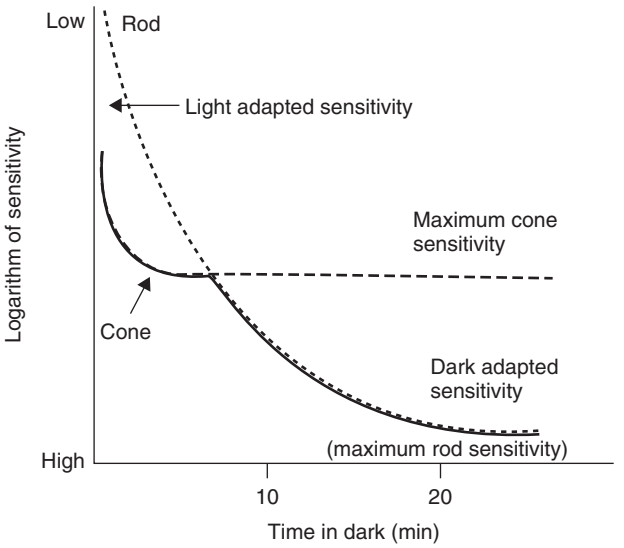



**FIGURE 3** Dark adaptation function illustrating sensitivity to visual stimuli as a function of time in the dark for cone and rods.

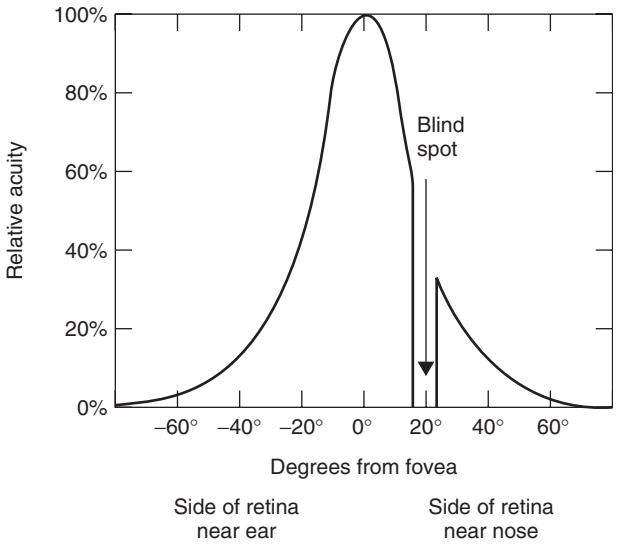



**FIGURE 4** Visual acuity as a function of retinal location.

contrast sensitivity function, which for an adult shows maximum sensitivity at a spatial frequency of 3–5 cycles/degree of visual angle. Because high spatial frequencies convey detail and low frequencies the global properties of stimuli, acuity tests based on contrast sensitivity provide a more detailed analysis than standard acuity tests about aspects of vision necessary for performing various tasks. For example, contrast sensitivity at intermediate and low spatial frequencies predicts detectability of signs at night [15].

An abrupt change in a display to signal a change in system mode may go undetected. The change is more likely to attract attention if it is signaled by a flickering stimulus. Conversely, stimuli such as displays on cathode ray tube (CRT) screens may flicker but with the intent of being seen as continuous. The highest rate at which flicker can be perceived is called the *critical flicker frequency*. A display intended to be seen as flickering should be well below the critical flicker frequency, whereas a display intended to be seen as continuous should be well above that frequency.

People show good lightness constancy, which is that a stimulus appears to be constant on a white-to-black dimension under different amounts of illumination. However, *lightness contrast*, for which an object looks darker when a surrounding or adjacent object is white rather than black, may occur when the intensity of local regions is changed, as in displays or signs.

Because color perception is a function of the output of the three cone types, color vision is trichromatic: Any spectral color can be matched by a combination of three primary colors from the short, middle, and long wavelength regions of the spectrum. This fact is used in the design of color televisions and computer monitors, for which all colors are generated from combinations of pixels of three different colors. For many perceptual phenomena, blue and yellow are paired in opposing manners, as are red and green: One color of the pair may produce an afterimage of the other; a background of one color may induce the other in a figure that would otherwise be seen as a neutral color; combinations of the two colors are not perceived. These complimentary color relations are based in the visual sensory pathways. That is, output from the cones is rewired

into opponent-process neural coding in the optic nerve. A given neuron can signal, for example, blue or yellow, but not both at the same time. Finally, 8% of males are color blind and cannot distinguish all colors that a person with trichromatic vision can, which may cause objects in those colors to be less conspicuous [16]. The use of color to convey information, thus, must be done with care.

### 4.3 Higher-Level Properties of Visual Perception

The patches of light stimulating the photoreceptors must be organized into a perceptual world of meaningful objects. This is done effortlessly in everyday life, with little confusion. However, organization can be critical for constructed displays. A symbol on a sign that is incorrectly grouped may not be recognized as intended. Similarly, if a warning signal is grouped perceptually with other displays, then its message may be lost. The investigation of perceptual organization was begun by Gestalt psychologists.

According to the Gestalt psychologists, perceptual organization follows the *principle of präagnanz*: The organizational processes will produce the simplest possible organization allowed by the conditions [17]. The first step in perceiving a figure requires separating it from the background. The importance of *figure-ground* organization is seen in figures with ambiguous figure-ground organizations, as the well-known Ruben's vase (see Figure 5). When a region is seen as figure, the contour appears to be part of it, the region seems to be in front of the background, and it takes on a distinct form.

Several factors influence figure-ground organization: Symmetric rather than asymmetric patterns tend to be seen as figure; a region surrounded completely by another tends to be seen as figure and the surround as background; the smaller of two regions tends to be seen as figure and the larger as ground. Figure-ground principles can be used to camouflage targets in the field.

The way that the figure is grouped is also important to perception. *Grouping principles* include: proximity—display elements that are located close together will tend to be grouped together; similarity—display elements that are similar in appearance, for example, orientation or color, will tend to be grouped together; continuity—figures will tend to be organized along continuous contours; closure—display elements that make up a closed figure will tend to be grouped together; and common fate—elements with a common motion will tend to be grouped together; connectedness—elements can be grouped

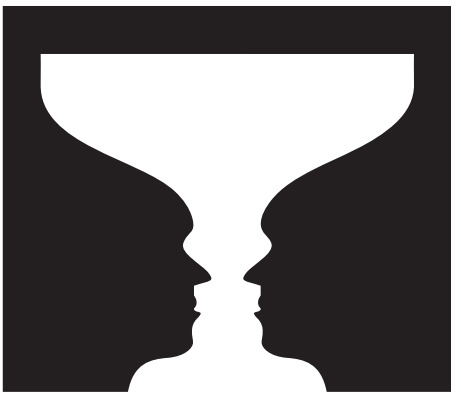


**FIGURE 5** Ruben's vase: An illustration of reversible figure-ground relations.

by lines connecting them; and common region—a contour drawn around elements will cause those elements to be grouped together.

Another distinction is between *integral* and *separable* stimulus dimensions [18]: Stimuli composed from integral dimensions are perceived as wholes, whereas those composed from separable dimensions are perceived in terms of their component dimensions. Speed of classification on one dimension is unaffected by the relation to the other if the dimensions are separable. However, for integral dimensions, classifications are slowed when the value of the irrelevant dimension is uncorrelated with that of the relevant dimension but speeded when the two dimensions are correlated. Combinations of hue, saturation, and lightness, and of pitch and loudness have been classified as integral, and size with lightness or angle as separable.

The distinction between integral and separable dimensions is incorporated in the proximity compatibility principle [19]: If a task requires information to be integrated mentally (i.e. processing proximity is high), then that information should be presented in an integral display (i.e. one with high display proximity). High display proximity can be accomplished by increasing the spatial proximity of the display elements so that the elements are integrated and appear as a distinct object. The idea is to replace the cognitive computations that someone must perform to combine the pieces of information with a less mentally demanding pattern-recognition process.

To survive, a person must be able to perceive locations of objects accurately. Moreover, representational displays should provide the information necessary for accurate spatial perception. Many cues play roles in the perception of distance and spatial relations [20, see Figure 6], and the perceptual system constructs the three-dimensional percept using these cues. Among the possible depth cues are accommodation and vergence angle, which, at relatively close distances, vary systematically as a function of the distance of the fixated object from the observer. Binocular disparity is a cue that is a consequence of the two eyes viewing objects from different positions. A fixated object falls on corresponding points of the two retinas. For objects in front of or behind a curved region passing through the fixated object, the images fall on disparate locations. The direction and amount of disparity indicate how near or far the object is from fixation. Binocular disparity is a strong cue to depth that can enhance the perception of depth relations in displays of naturalistic scenes and may be of value to scientists and

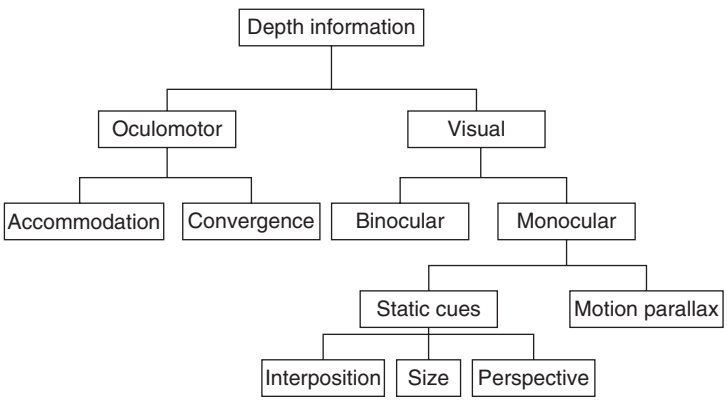



**FIGURE 6** Diagram of oculomotor and visual depth cues. (Adapted from R. Sekuler and R. Blake (1994). /Perception/ (3rd ed.). New York: McGraw Hill.)

others in evaluating multidimensional data sets (e.g. a three-dimensional data set could be processed faster and more accurately to answer questions that required integration of the information if the display was stereoptic than if it was not [21]).

There are many static, or pictorial, monocular cues to depth. These include retinal size—larger images appear to be closer—and familiar size—for example, a small image of a car provides a cue that the car is far away. The cue of interposition is that an object that appears to block part of the image of another object located in front of it. Other cues come from shading, aerial perspective, and linear perspective. Texture gradient, which is a combination of linear perspective and relative size, is important in depth perception [22].

Depth cues become dynamic when an observer moves. If fixation is maintained on an object and as location changes, as when looking out a train window, objects in the background will move in the same direction in the image as you are moving, whereas objects in the foreground will move in the opposite direction. This cue is called *motion parallax*. When you move straight ahead, the optical flow pattern conveys information about how fast your position is changing with respect to objects in the environment [23].

The size of the retinal image of an object varies as a function of the object's distance from the observer. When accurate depth cues are present, size constancy results: Perceived object size does not vary as a function of changes in retinal image size that accompany changes in depth. Size constancy breaks down and illusions of size appear when depth cues are misleading. Misperceptions of size and distance also can occur when depth cues are minimal, as when navigating at night.

For displayed information to be transmitted accurately, the objects and words must be recognized. Pattern recognition is typically presumed to begin with feature analysis. Alphanumeric characters are analyzed in terms of features such as vertical or horizontal line segments (see Figure 7). Confusion matrices obtained when letters are misidentified indicate that an incorrect identification is most likely to be a letter whose features overlap with the one that was displayed. Letters are components of syllables and words. Numerous studies have provided evidence for the need to distinguish several different levels of reading units [24].

Pattern recognition is also influenced by "top-down" information of several types [25]: regularities in mapping between spelling and spoken sounds and orthographic, syntactic, semantic, and pragmatic constraints. For accurate pattern recognition, the possible alternatives need to be physically distinct and consistent with expectancies created by the context.

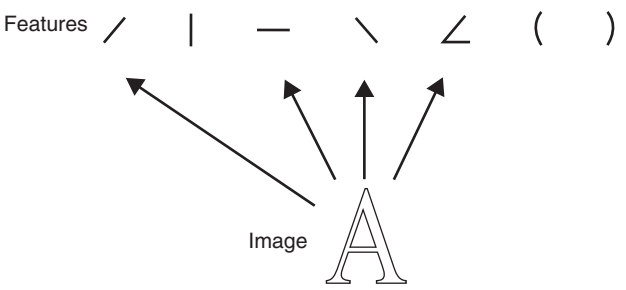



**FIGURE 7** Pattern (letter) recognition through analysis of features.

For a skilled reader, the pattern recognition involved in reading occurs almost instantaneously and relatively automatically. This is true for other pattern recognition skills as well (e.g. identifying enemy tanks or intrusion detection patterns). The important point is that, with experience, people can come to recognize very complex patterns that would seem meaningless to a novice. In fact, it is generally that efficient pattern recognition underlies expertise in most domains [26]. Some stimuli, such as faces, are special in that they are processed by different areas of the brain from other objects and their recognition is more sensitive to global configuration and orientation [27].

## 5 HEARING

The sense of hearing is also used extensively to convey information [2]. It is an effective modality for warnings, due to sound being able to be heard from any direction and because rapid onsets tend to attract attention.

### 5.1 Auditory Sensory System

Sound waves are fluctuations in air pressure produced by mechanical disturbances; the frequency of oscillations correlates with the sound's pitch and the amplitude with its loudness. A sound wave moves outward from its source at 344 m $s^{-1}$, with the amplitude being a decreasing function of distance. When sound reaches the outer ear, it is funneled into the middle ear (see Figure 8). The eardrum, which separates the outer and middle ears, vibrates in response to the fluctuations in air pressure produced by the sound wave. The middle ear contains a system of three bones that move when the eardrum vibrates, and this movement gets transferred to the fluid-filled inner ear. A flexible membrane, the basilar membrane, runs the length of the inner ear. Movement of this membrane bends hair cells, which are the sensory receptors that initiate neural signals.

The pathways from the auditory nerve project to the primary auditory cortex in the temporal lobe after first passing through several neuroanatomical structures. The auditory cortex contains neurons that extract complex features of auditory stimulation.

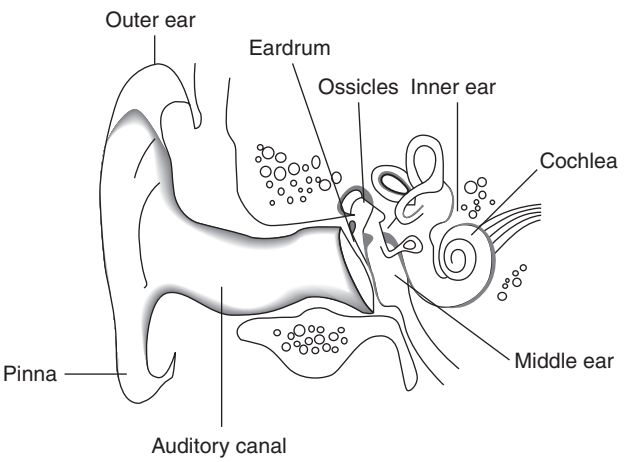



**FIGURE 8** Illustration of the major structures of the ear.

## 5.2 Auditory Perception

Loudness is affected by many factors in addition to amplitude. Humans are insensitive to tones below 200 Hz and, to a lesser extent, to tones exceeding 6 kHz. This is illustrated by equal loudness contours, which show that low and high frequency sounds must be of higher amplitude to be of equal loudness to tones of intermediate frequency (see Figure 9).

Extraneous sounds can mask targeted sounds. This is important for work environments, in which audibility of auditory input must be evaluated with respect to the level of background noise. The amount of masking depends on the spectral composition of the target and noise stimuli. Masking only occurs from frequencies within a critical bandwidth. A masking noise will exert a much greater effect on sounds of higher frequency than on sounds of lower frequency, with this asymmetry due to properties of the basilar membrane.

## 5.3 Higher-Level Properties of Auditory Perception

The principles of perceptual organization apply to auditory stimuli. Grouping can occur on the basis of similarity (e.g. frequency) and spatial and temporal properties (see Figure 10). Tones can be grouped into distinct streams based on similarities on various dimensions [28].

Being able to identify where a threat is coming from is important to survival. Two different sources of information, interaural intensity and time differences, are relied on to

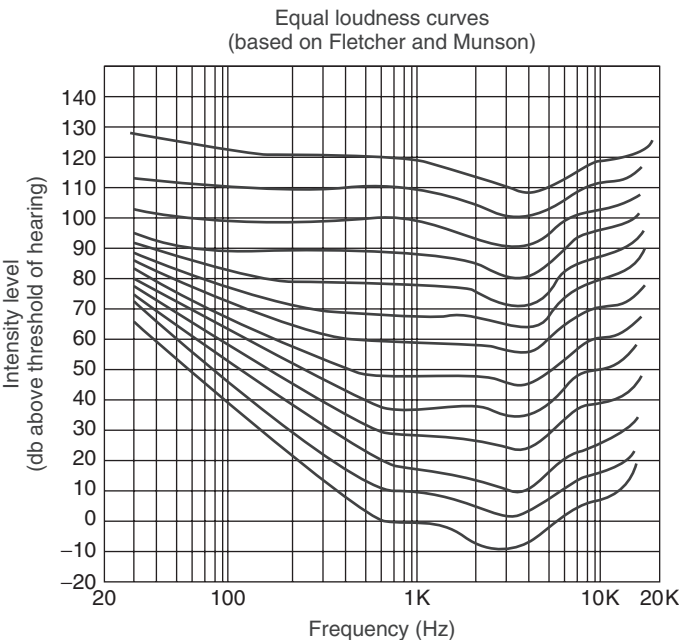



**FIGURE 9** Equal loudness contour curves. Each curve indicates the intensity for tones of different frequencies required for the tones to sound equally loud as a 1KHz tone at the indicated intensity level.

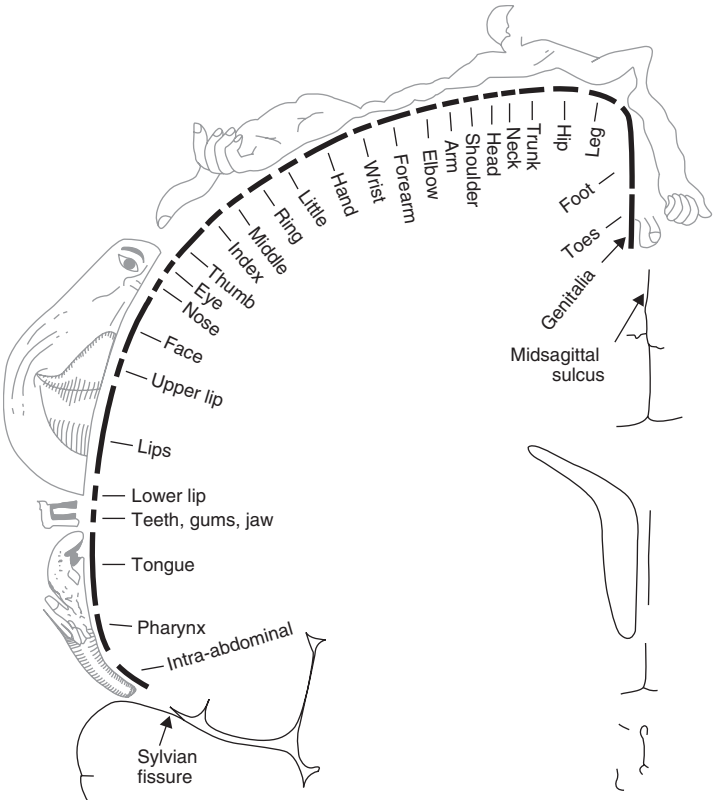



**FIGURE 10** Somatotopic map of the cerebral cortex. (Based on one from W. Penfield & T. Rasmussen (1950). "The cerebral cortex of man." New York: Macmillan.)

perceive the location of sound around us. At the front and back of the listener, the intensity of the sound and the time at which it reaches the ears is equal. As the sound moves progressively toward one side or the other of the listener's head, the sound becomes increasingly more intense at the closer ear than at the farther one, and it also reaches the ipsilateral ear first. The interaural intensity cue is most effective for high frequency tones, and the interaural time cue for low frequency sounds. Localization accuracy is poorest for tones between 2 and 4 kHz, where neither cue is effective. Because both cues are ambiguous at the front and back, front-back confusions of the location of brief sounds often occur.

## 6 BODY SENSES, SMELL, AND TASTE

Though we cannot go into detail on the remaining sensory modalities, they have important implications for homeland security as well.

### 6.1 Touch, Proprioception, Pain, and Temperature

The body senses are composed of four distinct modalities [29]—touch, proprioception, pain, and thermal sensations—that are elicited respectively by mechanical stimulation

of the skin, mechanical displacements of the muscles and joints, stimuli of sufficient intensity to damage tissue, and cool and warm stimuli. The receptors for these senses are the endings of neurons located in the back side of the spinal cord. The fibers follow two major pathways, dorsal and anterolateral. The former pathway conveys information about touch and proprioception, and the latter information about pain and temperature.

The fibers project to the somatosensory cortex, which is organized as a homunculus representing the opposite side of the body. Areas of the body for which sensitivity is greater have larger areas devoted to them than areas with lesser sensitivity (see Figure 10). Some of the cells respond to complex features of stimulation, such as movement of an object across the skin.

*Vibrotaction* is an effective way for transmitting complex information [30]. When mechanical vibrations are applied to a region of skin, the frequency and location of the stimulation can be varied. For frequencies of less than 40 Hz, the size of the contactor area does not influence the absolute threshold for detecting vibration. For higher frequencies, the threshold decreases with increasing size of the contactor, indicating spatial summation of the energy within the stimulated region. For multicontactor devices, which can present complex spatial patterns of stimulation, masking stimuli presented in close temporal proximity to the target stimulus can degrade identification. However, with practice, pattern recognition capabilities with these types of devices can become quite good. As a result, they can be used as reading aids for the blind and to a lesser extent as hearing aids for the hearing impaired [30].

A distinction is commonly made between active and passive touch [31]. Passive touch refers to situations in which the individual does not move her hand, and the touch stimulus is applied passively, as in vibrotaction. Active touch refers to situations in which the individual intentionally moves the hand to manipulate and explore an object. Pattern recognition with active touch is superior to that with passive touch. However, the success of passive vibrotactile displays for the blind indicates that much information can also be conveyed passively.

### 6.2 Smell and Taste

Smell and taste can communicate information about potential danger. The smell of a toxic substance or taste of rancid potato chips may be noxious and convey that they should not be consumed. Contaminated water also may have a noxious smell and taste, and a chemical attack may produce a burning sensation in the throat and nose. Both sensory modalities can be used for warning signals. For example, ethylmercaptan is added to natural gas to warn of gas leaks because humans are sensitive to its odor.

The sensory receptors for taste are groups of cells called *taste buds* located on the tongue, throat, roof of the mouth, and inside the cheeks. Sensory transduction occurs when a taste solution comes in contact with the taste buds. The nerve fibers from the taste receptors project to several nuclei in the brain and then to the insular cortex, located between the temporal and parietal lobes, and the limbic system. Four basic tastes can be distinguished: sweet, sour, salty, and bitter, though many sensations fall outside of their range [32].

For smell, molecules in the air that are inhaled affect receptor cells located in a region of the nasal cavity. Different receptor types have different proteins that bind the odorant molecules to the receptor. The fibers from the smell receptors project to the olfactory

bulb, located in the front of the brain. From there, the fibers project to a cluster of neural structures called the *olfactory brain*. Although odors are useful as warnings, they are not very effective at waking someone from sleep, which is why smoke detectors that emit a loud sound are needed. The sense of smell shows considerable plasticity, with associations of odors to events readily learned and habituation occurring to odors of little consequence [33].

## 7 MULTIMODAL SENSORY INTERACTIONS AND ROLE OF ACTION

In everyday life, we receive input constantly through the various senses. This input must be integrated into a coherent percept. It is important, therefore, to understand how the information from different senses is weighted and combined in perception, and how processing of input from one modality is affected by processing of input from another [34].

Many systems tend to overload the visual system with displays. As a result, there is an increased interest in using multimodal display technologies, which uses other modalities to augment visual perception. For example, auditory and tactile displays have been used to direct an observer's attention to certain areas of a visual display that require further analysis [35]. Multimodal displays also allow information to be presented to users in virtual worlds that represent real-world interactions of the senses [36].

The use of multiple display and control modalities enables different ways of presenting and responding to information, the incorporation of redundancy into displays, and emulation of real-life environments. Multimodal interfaces can reduce mental workload and make human-computer interactions more naturalistic. However, designing effective multimodal interfaces is a challenge because many interactive effects between different modalities may arise. These effects must be taken into account if the full benefits of multimodal interfaces are to be realized.

There is a tendency to think of perception independent from action because "input precedes output." However, a close relation between perception and action exists. For example, it is natural to orient attention to the location of a sound, making auditory displays a good choice for actions that require users to respond to the location of the sound (e.g. fire alarms should be place close to the exit). As a result, the decisions and actions that need to be made in response to a signal or display must be taken into account when designing to optimize perception [37].

## 8 CONCLUSION

Many of the technical devices that have been, and are being, developed to aid in homeland security depend on successful human-system interactions. Human perception is an important aspect of such interactions. Operators must be able to sense and perceive the displayed information accurately and efficiently, and in a way that maps compatibly onto the tasks and actions that they must perform, for the system to achieve its goals. Regardless of the exact forms that future security technologies take, as long as humans are in the system the basic principles and concepts of sensation and perception must be taken into account.

## REFERENCES


1. Sträter, O. (2005). *Cognition and Safety: An Integrated Approach to Systems Design and Assessment*. Ashgate, Burlington, VT.
2. Robinson, D. (2006). Emergency planning: the evolving role of regional planning organizations in supporting cities and counties. In *The McGraw-Hill Homeland Security Book*, D. G. Kamien, Eds. McGraw-Hill, NY, pp. 297–310.
3. Wolfe, J. M., Kluender, K. R., Levi, D. M., Bartoshuk, L. M., Herz, R. S., Klatzky, R. L., and Lederman, S. J. (2006). *Sensation and Perception*. Sinauer, Sunderland, MA.
4. Proctor, R. W., and Proctor, J. D. (2006). Sensation and perception. In *Handbook of Human Factors and Ergonomics*, 3rd ed., G. Salvendy, Ed. John Wiley & Sons, Hoboken, NJ, pp. 53–88.
5. Gescheider, G. A. (1997). *Psychophysics: The Fundamentals*, 3rd ed. Lawrence Erlbaum Associates, Hillsdale, NJ.
6. Marks, L. E., and Gescheider, G. A. (2002). Psychophysical scaling. In *Stevens' Handbook of Experimental Psychology*, *Methodology in Experimental Psychology*, H. Pashler, and J. Wixted, Eds. John Wiley & Sons, New York, pp. 91–138.
7. Walker, B. N. (2002). Magnitude estimation of conceptual data dimensions for use in sonification. *J. Exp. Psychol. [Appl.]* **8**, 211–221.
8. Macmillan, N. A., and Creelman, C. D. (2005). *Detection Theory: A User's Guide*, 2nd ed. Cambridge University Press, New York.
9. See, J. E., Howe, S. R., Warm, J. S., and Dember, W. N. (1995). Meta-analysis of the sensitivity decrement in vigilance. *Psychol. Bull.* **117**, 230–249.
10. Kanwisher, N., and Duncan, J., Eds. (2004). *Functional Neuroimaging of Visual Cognition: Attention and Performance XX*. Oxford University Press, New York.
11. Parasuraman, R., and Rizzo, M. (2007). *Neuroergonomics: The Brain at Work*. Oxford University Press, New York.
12. Schmorrow, D. D., Ed. (2005). *Foundations of Augmented Cognition*. Lawrence Erlbaum Associates, Mahwah, NJ.
13. Frishman, L. J. (2001). Basic visual processes. In *Blackwell Handbook of Perception*, E. B. Goldstein, Ed. Blackwell, Malden, MA, pp. 53–91.
14. Andre, J., Owens, A., and Harvey, L. O., Jr., Eds. (2003). *Visual Perception: The Influence of H. W. Leibowitz*. American Psychological Association, Washington, DC.
15. Evans, D. W., and Ginsburg, A. P. (1982). Predicting age-related differences in discriminating road signs using contrast sensitivity. *J. Opt. Soc. Am.* **72**, 1785–1786.
16. O'Brien, K. A., Cole, B. L., Maddocks, J. D., and Forbes, A. B. (2002). Color and defective color vision as factors in the conspicuity of signs and signals. *Hum. Factors* **44**, 665–675.
17. Palmer, S. E. (2003). Visual perception of objects. In *Experimental Psychology*, *Handbook of Psychology*, A. F. Healy, and R. W. Proctor, Eds., Vol. 4. John Wiley & Sons, Hoboken, NJ, pp. 179–211.
18. Garner, W. (1974). *The Processing of Information and Structure*. Lawrence Erlbaum Associates, Hillsdale, NJ.
19. Wickens, C. D., and Carswell, C. M. (1995). The proximity compatibility principle: its psychological foundation and relevance to display design. *Hum. Factors* **37**, 473–494.
20. Proffitt, D. R., and Caudek, C. (2003). Depth perception and the perception of events. In *Experimental Psychology*, *in Handbook of Psychology*, A. F. Healy, and R. W. Proctor, Eds., Vol. 4. John Wiley & Sons, Hoboken, NJ, pp. 213–236.

21. Wickens, C. D., Merwin, D. F., and Lin, E. (1994). Implications of graphics enhancements for the visualization of scientific data: dimensional integrality, stereopsis, motion, and mesh. *Hum. Factors* **36**, 44–61.
22. Gibson, J. J. (1950). *The Perception of the Visual World*. Houghton Mifflin, Boston, MA.
23. Bruno, N., and Cutting, J. E. (1988). Minimodularity and the perception of layout. *J. Exp. Psychol. Gen.* **117**, 161–170.
24. Healy, A. F. (1994). Letter detection: a window to unitization and other cognitive processes in reading text. *Psychon. Bull. Rev.* **1**, 333–344.
25. Massaro, D. W., and Cohen, M. M. (1994). Visual, orthographic, phonological, and lexical influences in reading. *J. Exp. Psychol. Hum. Percept. Perform.* **20**, 1107–1128.
26. Ericsson, K. A., Charness, N., Feltovich, P. J., and Hoffman, R. R., Eds. (2006). *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press, New York.
27. Farah, M. J., Wilson, K. D., Drain, M., and Tanaka, J. (1998). What is "special" about face perception? *Psychol. Rev.* **105**, 482–498.
28. Bregman, A. S. (1990). *Auditory Scene Analysis: The Perceptual Organization of Sound*. MIT Press, Cambridge, MA.
29. Gardner, E. P., Martin, J. H., and Jessell, T. M. (2000). The bodily senses. In *Principles of Neural Science*, E. R. Kandel, J. H. Schwartz, and T. M. Jessell, Eds., Vol. 4. Elsevier, Amsterdam, pp. 430–450.
30. Summers, I. R., Ed. (1992). *Tactile Aids for the Hearing Impaired*. Whurr Publishers, London.
31. Gibson, J. J. (1966). *The Senses Considered as Perceptual Systems*. Houghton Mifflin, Boston, MA.
32. Schiffman, S. S., and Erickson, R. P. (1993). Psychophysics: Insights into transduction mechanisms and neural coding. In *Mechanisms of Taste Transduction*, S. A. Simon, and S. D. Roper, Eds. CRC Press, Boca Raton, FL.
33. Doty, R. L., Ed. (2003). *Handbook of Olfaction and Gustation*, 2nd ed. Marcel Dekker, New York.
34. Calvert, G., Spence, C., and Stein, B. E., Eds. (2004). *The Handbook of Multisensory Processes*. MIT Press, Cambridge, MA.
35. Proctor, R. W., Tan, H. Z., Vu, K. P. L., Gray, R., and Spence, C. (2005). Implications of compatibility and cuing effects for multimodal interfaces. In *Foundations of Augmented Cognition*, D. D. Schmorrow, Ed. Lawrence Erlbaum Associates, Mahwah, NJ, pp. 3–12.
36. Stanney, K. M., Ed. (2002). *Handbook of Virtual Environments: Design, Implementation, and Applications*. Lawrence Erlbaum Associates, Mahwah, NJ.
37. Proctor, R. W., and Vu, K. P. L. (2006). *Stimulus-Response Compatibility Principles: Data, Theory, and Application*. CRC Press, Boca Raton, FL.

## FURTHER READING

Bolanowski, SJ., and Gescheider, GA., Eds. (1991). *Ratio Scaling of Psychological Magnitude*. Lawrence Erlbaum Associates, Hillsdale, NJ.

Macmillan, N.A. (2002). Signal detection theory. In *Stevens' Handbook of Experimental Psychology*, Methodology in Experimental Psychology, H. Pashler, and Wixted, J., Eds. Vol. 4. John Wiley & Sons, New York, pp. 43–90.

Wickens, TD. (2001). *Elementary Signal Detection Theory*. Oxford University Press, New York.

# HUMAN BEHAVIOR AND DECEPTION DETECTION

MARK G. FRANK AND MELISSA A. MENASCO
*University at Buffalo, State University of New York, Buffalo, New York*
MAUREEN O'SULLIVAN
*University of San Francisco, San Francisco, California*

## 1 INTRODUCTION

Terrorism at its core is a human endeavor. Human beings cultivate what they hate, plan, and then execute terrorist attacks. Thus, any information that can aid the intelligence or security officer to weigh the veracity of the information he or she obtains from suspected terrorists or those harboring them would help prevent attacks. This would then not only add another layer to force protection but would facilitate future intelligence gathering. Yet the face-to-face gathering of information through suspected terrorists, informants, or witnesses is replete with obstacles that affect its accuracy such as the well-documented shortcomings of human memory, honest differences of opinion, as well as what is the focus of this article—outright deception [1].

The evidence suggests that in day-to-day life most lies are betrayed by factors or circumstances surrounding the lie, and not by behavior [2]. However, there are times when demeanor is all a Homeland security agent has at his or her disposal to detect someone who is lying about his or her current actions or future intent. Because a lie involves a deliberate, conscious behavior, we can speculate that this effort may leave some trace, sign, or signal that may betray that lie. What interests the scientist, as well as society at large, is (i) are there clues perceptible to the unaided eye that can reliably discriminate between liars and truth tellers; (ii) do these clues consistently predict deception across time, types of lies, different situations, and cultures?; and if (i) and (ii) are true, then (iii) How well can our counter-terrorism professionals make these judgments, and can they do this in real time, with or without technological assistance?

## 2 SCIENTIFIC OVERVIEW—BEHAVIORAL SIGNS OF DECEPTION

To date no researcher has documented a "Pinocchio response"; that is, a behavior or pattern of behaviors that in all people, across all situations, is specific to deception (e.g. [3]). All the behaviors identified and examined by researchers to date can occur for reasons unrelated to deception. Generally speaking, the research on detecting lies from behavior suggests that two broad families of behavioral clues are likely to occur when someone is lying—clues related to liar's memory and thinking about what they are saying (cognitive clues), and clues related to liar's feelings and feelings about deception (emotional clues) [3–8].

### 2.1 Cognitive Clues

A lie conceals, fabricates, or distorts information; this involves additional mental effort. The liar must think harder than a truth teller to cover up, create events that have not happened, or to describe events in a way to allow multiple interpretations. Additional mental effort is not solely the domain of the outright liar; however, a person who must tell an uncomfortable truth to another will also engage in additional mental effort to come up with the proper phrasing while simultaneously reducing the potential negative emotional reaction of the other. This extra effort tends to manifest itself with longer speech latencies, increased speech disturbances, less plausible content, less verbal and vocal involvement, less talking time, more repeated words and phrases, and so forth [9]. Research has also shown that some nonverbal behaviors change as a result of this mental effort. For example, illustrators—hand or head movements that accompany speech, and are considered by many to be a part of speech (e.g. [10])—will decrease when lying compared to telling the truth [11, 12].

Another way in which cognition is involved in telling a lie is through identification of naturalistic memory characteristics. This means that experienced events have memory qualities that are apparent upon description that are different from events that have not been experienced (the "Undeutsch hypothesis" [13]). Events that were not actually experienced feature more ambivalence, have fewer details, a poorer logical structure, less plausibility, more negative statements, and are less embedded in context. Liars are also less likely to admit lack of memory and have less spontaneous corrections (reviewed by [8, 9]), and may use more negative emotion words and fewer self and other references [14]. Mental effort clues seem to occur more in the delivery of the lie, whereas memory recall clues tend to rest more in the content of the lie.

We note that not all lies will tax mental effort; for example, it is much less mentally taxing to answer a close ended question like "Did you pack your own bags?" with a yes or no than to answer an open ended "What do you intend to do on your trip?" Moreover, a clever liar can appear more persuasive if he or she substitutes an actual experienced event as their alibi rather than creating an entirely new event. This may be why a recent general review paper [9] found consistent nonhomogeneous effect sizes for these mental effort and memory-based cues across the studies they reviewed, as the particular paradigms used by researchers varied greatly in the extent to which the lies that were studied mentally taxed the liars.

### 2.2 Emotional Clues

Lies can also generate emotions, ranging from the excitement and pleasure of "pulling the wool over someone's eyes" to fear of getting caught to feelings of guilt [4]. Darwin [15] first suggested that emotions tend to manifest themselves in the facial expressions, as well as in the voice tones, and that these could be reliable enough to accurately identify emotional states. Research has since shown that for some expressions—e.g. anger, contempt, disgust, fear, happiness, sadness/distress, or surprise—cultures throughout the planet recognize and express these emotions in both the face and voice similarly [16]. To the extent that a lie features higher stakes for getting caught, we would expect to see more of these signs of emotion in liars compared to truth tellers. If the lie is a polite lie that people tell often and effortlessly, there would be less emotion involved (e.g. [17]). Meta-analytic studies suggest that liars do appear more nervous than truth tellers, with

less facial pleasantness, higher vocal tension, higher vocal pitch, greater pupil dilation, and fidgeting [9]. If the lie itself is about emotions—e.g. telling someone that one feels calm, when in fact one is nervous—the research shows that signs of the truly felt emotion appear in the face and voice despite attempts to conceal, although these signs are often subtle and brief [18, 19].

### 2.3 Measurement Issues

One issue in measuring lie signs is to make clear what is meant by the terms cognition and emotion. For example, in deception research, the term arousal is used interchangeably with emotion, but often refers to many different phenomena: an orienting response [20], an expression of fear [21], a more indeterminate affect somewhere between arousal and emotion ([22]; see also discussion by Waid and Orne [23]), as well as physiological states as different as stress, anxiety, embarrassment, and even anger [24].

A second issue in measuring lie signs is to clarify the level of detail of measurement as well as to specify why that level of detail may or may not correlate with lying [25]. Many meta-analyses of behavioral deception clues report insignificant effect sizes, but the variance among effect is not homogeneous (e.g. [3, 9, 26–28]). For example, some studies investigated behavior at the most elemental *physical* units of measurement such as counting the movements in the hands, feet, arms, legs, torso, eye movements, eye blinks, pupil dilation, lip pressing, brow lowering or raising, lip corner puller (smiling), fundamental frequency, amplitude, pauses, filled pauses, response latency, speech rate, length of response, connector words, unique words, self-references, and so forth. Other studies investigated behavior at the most elemental *psychological meaning* units of measurement. Some of these included manipulators—which involve touching, rubbing, etc., of various body parts—which could be composed of a number of hand, finger, and arm movements, but which were scored for theoretical rather than merely descriptive reasons. Other psychologically meaningful units of measurement include illustrators, which accompany speech to help keep the rhythm of the speech, emphasize a word, show direction of thought, etc. or emblems, which are gestures that have a speech equivalent, such as a head nod meaning "yes", or a shrug meaning "I am not sure", or facial emblems such as winking. The psychological meaning units might also include vocal tension, speech disturbances, negative statements, contextual embedding, unusual details, logical structure, unexpected complications, superfluous details, self-doubt, and so forth. Finally, other studies investigated behavior at the most *interpretative/impressionistic* unit level, which are further unarticulated composites of the physical and the psychological meaning units described earlier. Some of these impressionistic variables of the behaviors include fidgeting, involvement, body animation, posture, facial pleasantness, expressiveness, vocal immediacy and involvement; and spoken uncertainty; plausibility; and cognitive complexity (see review by [9]). The problem of course is that as one moves from physical to impressionistic measures, it would seem to become harder to make those judgments reliably. This is not always the case though, for example, the term "smile" has rarely been defined in research reports, yet independent coders are typically above 0.90 reliability when coding smiles (see [29] for a review). Although research works suggest that people can be more accurate when they employ indirect inferences to deception (e.g. does the person have to think hard? [30]), "gut" impressions tend to be uncorrelated with accuracy [26]. This suggests that we must be cautious about clues at the impressionistic level, and

that it may be more productive to study them at their psychological level where they might be more meaningful to understanding deception.

### 2.4 Prognosis on Generalizability of Deception Findings Across Time, Lies, Situations, and Cultures

It is safe to conclude that although there are some clues that betray a lie at rates greater than chance, none of them are exclusive to deception. This conclusion applies to machine based physiological approaches as well. However, the origins of these signs—mental effort, memory, and emotion—are universal. This suggests that if the context in which the information is gathered is controlled, and designed to differentially affect liars and truth tellers, it would increase greatly the chances of being able to distinguish people with deceptive intent from those with truthful intent. Polygraph examination has done this by controlling their question style to improve hit rates, but to date this has not been done systematically in behavioral studies. Thus its effects are unknown, but we can speculate based upon what we know about normal, truthful human behavior. If the lie is of no significance to the person, with no costs for getting caught, and involves a simple yes or no answer, odds are there will not be many clues to distinguish the liar from the truth teller. If the situation has significance to the person, there are consequences for getting caught, and the person is required to recount an event in an open ended question, then we would expect more clues to surface that would distinguish the liar from the truth teller. This may be a curvilinear relationship; a situation of extraordinary high mental effort and emotion—e.g. one in which a person is being beaten, screamed at, and threatened with execution—will generate all the "lie clues" described earlier, but equally in liar and truth teller. Nonetheless, information about mental effort, experienced memory, and emotion can be very useful clues to Homeland Security personnel to identify behavioral "hot spots" [4] that can provide information about issues of importance to the subject. A counter-terrorism Intelligence officer who knows when a subject is feeling an emotion or thinking hard can know what topics to pursue or avoid in an interview, whether the subject is fabricating, concealing information, or merely feeling uncomfortable with the topic, although truthful.

## 3 SCIENTIFIC OVERVIEW—ABILITIES TO SPOT LIARS

Research over the past 30 years suggests that the average person is slightly statistically better than chance at identifying deception, but not practically better. The most recent review of over 100 studies has shown that when chance accuracy is 50%, the average person is approximately 54% accurate [31]. There are a number of reasons for this poor ability; among them poor feedback in daily life (i.e. a person only knows about the lies they have caught); the general tendency among people to believe others until proven otherwise (i.e. a "truth bias"; [32]), and especially a faulty understanding of what liars actually look like (i.e. the difference between people's perceived clues to lying, compared to the actual clues; [26]).

### 3.1 General Abilities of Specialized Groups

Most of the studies reviewed were laboratory based and involved observers judging strangers. But similar results are found even when the liars and truth tellers are known

to the observers (also reviewed by [31]. If the lies being told are low stakes, so that little emotion is aroused and the lie can be told without much extra cognitive effort, there may be few clues available on which to base a judgment. But even studies of high stakes lies, in which both liars and truth tellers are highly motivated to be successful, suggest an accuracy level that is not much different from chance.

Researches that examined unselected professionals involved in security settings—police, federal agents, and so forth—have typically found that they too are not any more accurate in their abilities to spot deception than laypeople (e.g., [27, 33–36]). However, within these studies there have been a handful of groups that have performed better than 60% accurate on both lies and truths, and what these groups are doing might be informative for Homeland Security applications. The first group identified was a group of Secret Service agents who not only were superior, as a group, in detecting lies about one's emotions, but those who were more accurate were more likely to report using nonverbal clues than those who were less accurate. The authors [33] speculated that the Secret Service agents were more accurate than the other groups because they were trained in scanning crowds for nonverbal behaviors that did not fit, and they also dealt with assassination threats, many of which were made by mentally ill individuals. Unlike most police officers whose assumption of guilt in suspects is high [37], reflecting the experience of their daily work, Secret Service agents interviewed suspects where they knew the base rate of true death threats was low. The second set of groups identified included forensic psychologists, federal judges, selected federal law enforcement officers, and a group of sheriffs [34]. A commonality among these groups seemed to be their very high motivation to improve their lie detecting skills. A third set of groups identified were police officers examining real-life lies, who showed 65% overall accuracy in detecting lies and truths [38].

### 3.2 Individual Differences

As with any ability, research suggests that some people are better able to detect deception than others in high-stake lies (e.g. [39]); this skill does not seem to translate to lower-stake lies [32]. One element of better skill in higher-stake settings is the ability to judge micromomentary displays of emotion [33, 39]. Other groups who showed better than 60% accuracy included people with left hemisphere brain lesions that prevented them from comprehending speech [40], and those subjects who scored higher on a test of knowledge of clues to deceit were also more accurate than those who did not [41]. A different approach has been to identify individuals who obtain high scores on lie detection tests and studying them in detail [42]. After testing more than 12,000 people using a sequential testing protocol involving three different lie detection accuracy measures, O'Sullivan and Ekman identified 29 highly accurate individuals. These individuals had a kind of genius with respect to the observation of verbal and nonverbal clues, but since genius often connotes academic intelligence, the expert lie detectors were labeled "truth wizards" to suggest their special talent. Although this term is unfortunate in mistakenly suggesting that their abilities are due to magic rather than talent and practice, the term does reflect the rarity of their abilities. One of the first findings of the Wizard Project was a profession-specific sensitivity to certain kinds of lies. About one-third of the wizards were highly accurate on all three of the tests used. Another third did very well on two of the tests, but not on the third, in which people lied or told the truth about whether they had stolen money. Nearly all of these wizards were therapists who had little, if

any, experience with lies about crime. On the other hand, the remaining third of the wizards were law enforcement personnel—police and lawyers—who did very well on the crime lie detection test, but not on a test in which people lied or told the truth about their feelings. Compared with a matched control group, expert lie detectors are more likely than controls to attend to a wide array of nonverbal behaviors and to be more consciously aware of inconsistencies between verbal and nonverbal behaviors. Although expert lie detectors make almost instantaneous judgments about the kind of person they are observing, they are also more cautious than controls about reaching a final decision about truthfulness.

## 4 CRITICAL NEEDS ANALYSIS

Research on human behavior and deception detection can make a useful contribution to Homeland Security needs as long as scientists and practitioners understand what it is they are observing—signs of thinking or signs of feeling. This rule applies to automated approaches that measure physiology as well. Even with this limitation, training in behavioral hot spot recognition may make security personnel better at spotting those with malfeasant intent. Other critical needs are discussed below.

### 4.1 More Relevant Laboratory Paradigms and Subjects

We must recognize that general meta-analyses of the research literature, although useful, are limited in their applicability to security contexts, since such analyses tend to combine studies that feature lies told with few stakes and cognitive demands with those with higher stakes and stronger cognitive demands. Thus, we should be more selective about which studies to examine for clues that may be useful or relevant to security contexts. This also means it is important for scientists to develop research paradigms that more closely mirror the real-life contexts in which security personnel work. Although laboratory settings are not as powerful as real-world settings, high-stake laboratory deception situations can provide insights with the best chance of applicability. Consistent with this approach, two current airport security techniques capitalize on behaviors identified by research studies on stress, with anecdotal success (i.e. Transportation Security Administration (TSA)'s Screening Passengers by Observation Techniques and the MA State Police Behavioral Assessment System). One way to facilitate this type of progress is to have Homeland Security personnel advise laboratory research, as well as allow researchers to spend on-the-job time with them. We believe that pairing the researchers and practitioners would eventually result in calls for laboratory studies featuring higher stakes to the liars, different subject populations beyond US/Europeans (as research suggests that people can detect deception in other cultures at rates greater than chance; [43, 44]), and differing interview lengths such as examining shorter interviews (i.e. a 30–90 s security screening) and longer interviews (i.e. a 1–4 h intelligence interview).

### 4.2 Examination and Creation of Real-World Databases

There have been very few studies of real-world deception (e.g. [38]), yet the technological capability exists to create many more. The biggest problem with real-world data is determining the ground truth (was the person really lying, or did he or she truly

believe what he or she just stated?). Estimating ground truth—as compared to knowing ground truth—will slow down the identification of any patterns or systems. Clear criteria must be established *a priori* to determine this ground truth. For example, confessions of malfeasance are a good criterion, but false confessions do happen. Catching someone with contraband (i.e. a "hit") is also a good criterion, but occasionally the person may be truthful when he or she states that someone must have snuck it into his or her luggage. Moreover, academics should advise on the capture and recording of these databases, to ensure that the materials are able to be examined by the widest number of researchers and research approaches. For example, most of the police interview video we have seen is of such poor quality that we cannot analyze facial expressions in any detail. It is only when these databases are combined with the laboratory work that we can more sharply identify behaviors or behavioral patterns that will increase the chances of catching those with malfeasant intent. To optimally use this information though, we must also examine in detail known cases of false negatives and false positives as well as correct hits to determine why mistakes were made in these judgments.

### 4.3 Ground Truth Base Rates

Security personnel do not know the base rates for malfeasance in their settings. Although it may be logistically impossible to hand-search every piece of hand luggage in a busy airport, or follow every investigative lead, it would be essential to know this base rate in order to ascertain the effectiveness of any new behavioral observational technique. This would also permit more useful cost–benefit analyses of various levels of security and training. A less satisfying but still useful way to ascertain effectiveness is to compare hit rates for contraband for those using various behavioral observation techniques with those who are stopped randomly (as long as the day of the week and time of the day/year are scientifically controlled).

### 4.4 Optimizing Training

The most recent meta-analysis of the research literature on training people to improve deception detection from behavior has shown that across over 2000 subjects, there was a modest effect for training, despite the use of substandard training techniques [45]. This obviously suggests that better training techniques will yield larger improvements in people's abilities to sort out truth from lie. One training change would be to train on behavioral clues that are derived from similar situations and supported by research. For example, one study trained research subjects to recognize a set of behavioral clues that are believed to be indicative of deception, and are often taught to law enforcement personnel as signs of deception, although many of these signs are not supported by the scientific literature [46]. This study reported a 10% decrease in accuracy for the groups receiving such training. Therefore, the first step in adequate training is to identify what information is useful for training (see above). The second step is to determine the most effective way to deliver that information. For example, what is the training duration that maximizes comprehension—one full day, three full days, or more? Should it be done in a group or self-study? Does it need simple repetition, or more creative approaches, and how many training items are needed? Does it need to be reinforced at particular intervals? How many clues should be taught—i.e. at what point do you overwhelm trainees? How do you train in such a way as to improve accuracy without overinflating confidence? These are just a few of the questions with unknown answers.

### 4.5 Identifying Excellence

Another critical need is to identify who within relevant organizations shows signs of excellence, through their higher hit rates or whatever other clear criteria can be applied. This strategy is similar to the strategy of the "wizards" study [42]. One caution is that to date, most testing material will be laboratory experiment based, and the generalizability of that information to real-world contexts is not perfect. An examination of the convergent validity of laboratory tests of deception detection and other more naturalistic approach measures (peer ratings, field observations in airports, or other points of entry with accuracy determined by the rate of contraband "hits" by individuals compared to random selection) would be a great start.

## 5 FUTURE RESEARCH DIRECTIONS

The aforementioned critical needs suggest several research questions, but by no means is that section comprehensive. As we peer into the future, there is much work to do. A partial list of future directions shown below suggests what we should do.

- Examine the role of technology in facilitating behavioral observation. A number of computer vision algorithms are now available that can aid observation, such as recognizing emotional expressions in the face (e.g. [47]). What is unknown is how robust these algorithms are in real-world contexts. What is also unknown is how best to combine technological observation of behavior with human judgment. Would there be a tendency for humans to overrely upon the technology over time?
- Identify the optimal environmental set up for surveillance, whether with technology or the unaided eye. This includes proxemic placement of tables, lines, stanchions, other individuals, and so forth. One goal would be to create an environment that would reduce the typical stress felt by the normal traveler, which would hopefully increase the salience of any sign of stress exhibited by the malfeasant to increase the chances of its being observed.
- Identify optimal interaction style between security agents and the public. One can aggressively question and threaten travelers, but that might render behavioral observation useless due to the overall stress engendered. A rapport-building approach (e.g. [48]) might be better, but this needs more research.
- Identify the optimal interview style. Phrasing of questions is important in obtaining information, but this has not been researched in the open literature. Small changes in phrasing—e.g. open versus close ended—might add to the additional cognitive burden of the liar and thus could be useful. The order of questions will also be important, as well as whether one should make a direct accusation. But only additional research will tell.
- Identify the optimal way to combine behavioral clues. Research tends to examine individual behavioral clues to ascertain their effectiveness, yet more modern neural network and machine learning approaches may be successful in identifying patterns and combinations of behaviors that better predict deception in particular contexts.
- Identify the presence of countermeasures. An inevitable side effect of the release of any information about what behaviors are being examined by security officers, to

identify riskier individuals in security settings, is that this information will find its way onto the Internet or other public forums. This means a potential terrorist can learn what to do and what not to do in order to escape further scrutiny. The problem is that we do not know yet whether one can conceal all their behaviors in these real-life contexts. Moreover, some of these behaviors, like emotional behavior, is more involuntary [16] and should be harder to conceal than more voluntary behavior like word choice. Thus it remains an open question as to whether a potential terrorist can countermeasure all of the critical behaviors.

Space limitations preclude an exhaustive list of needs, future directions, and research. In general, the research suggests that there are limited clues that are useful to sorting out liars and truth tellers, but most people cannot spot them. However, a closer examination of this literature suggests that some behavioral clues can be useful to security personnel, and some people can spot these clues well. We feel that it may be ultimately most productive to expand our thinking about behavioral clues to deceit to include thinking about behavioral clues to a person's reality—clues that someone is recounting a true memory, thinking hard, or having an emotion he or she wishes to hide. This would enable a security officer to make the most accurate inference about the inner state of the person they are observing, which, when combined with better interaction and interviewing techniques, would enable them to better infer the real reasons for this inner state, be it intending us harm, telling a lie, or telling the truth.

## REFERENCES


1. Haugaard, J. J., and Repucci, N. D. (1992). Children and the truth. In *Cognitive and Social Factors in Early Deception*, S. J. Ceci, M. DeSimone-Leichtman, and M. E. Putnick, Eds. Erlbaum, Hillsdale, NJ.
2. Park, H. S., Levine, T. R., McCornack, S. A., Morrison, K., and Ferrar, M. (2002). How people really detect lies. *Commun. Monogr.* **69**, 144–157.
3. Zuckerman, M., DePaulo, B. M., and Rosenthal, R. (1981). Verbal and nonverbal communication of deception. In *Advances in Experimental Social Psychology*, L. Berkowitz, Ed. Academic Press, San Diego, CA, Vol. 14, pp. 1–59.
4. Ekman, P. (1985/2001). *Telling Lies*. W. W. Norton, New York.
5. Ekman, P., and Frank, M. G. (1993). Lies that fail. In *Lying and Deception in Everyday Life*, M. Lewis, and C. Saarni, Eds. Guilford Press, New York, pp. 184–200.
6. Hocking, J. E., and Leathers, D. G. (1980). Nonverbal indicators of deception: A new theoretical perspective. *Commun. Monogr.* **47**, 119–131.
7. Knapp, M. L., and Comadena, M. E. (1979). Telling it like it isn't: A review of theory and research on deceptive communication. *Hum. Commun. Res.* **5**, 270–285.
8. Yuille, J. C., Ed. (1989). *Credibility Assessment*. Kluwer Academic Publishers, Dordrecht.
9. DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., and Cooper, H. (2003). Cues to deception. *Psychol. Bull.* **129**, 74–112.
10. McNeill, D. (1992). *Hand and Mind. What Gestures Reveal about Thought*. Chicago of University Press, Chicago.
11. Ekman, P., and Friesen, W. V. (1972). Hand movements. *J. Commun.* **22**, 353–374.
12. Vrij, A. (1995). Behavioral correlates of deception in a simulated police interview. *J. Psychol.* **129**, 15–28.

13. Undeutsch, U. (1967). Beurteilung der glaubhaftigkeit von aussagen. In *Handbuch derPsychologie. Bd. II: Forensische Psychologie*, U. Undeutsch, Ed. Verlag fur Psychologie, Goettingen, pp. 26–181.
14. Newman, M. L., Pennebaker, J. W., Berry, D. S., and Richards, J. M. (2003). Lying words: predicting deception from linguistic styles. *Pers. Soc. Psychol. Bull.* **29**, 665–675.
15. Darwin, C. (1872/1998). *The Expression of the Emotions in Man and Animals*, 3rd ed. (w/ commentaries by Paul Ekman). Oxford University Press, New York.
16. Ekman, P. (2003). *Emotions Revealed*. Henry Holt, New York.
17. DePaulo, B. M., Kashy, D. A., Kirkendol, S. E., Wyer, M. M., and Epstein, J. A. (1996). Lying in everyday life. *J. Pers. Soc. Psychol.* **70**, 979–995.
18. Ekman, P., Friesen, W. V., and O'Sullivan, M. (1988). Smiles when lying. *J. Pers. Soc. Psychol.* **54**, 414–420.
19. Ekman, P., O'Sullivan, M., Friesen, W. V., and Scherer, K. (1991). Invited article: face, voice, and body in detecting deceit. *J. Nonverbal Behav.* **15**, 125–135.
20. deTurck, M. A., and Miller, G. R. (1985). Deception and arousal: isolating the behavioral correlates of deception. *Hum. Commun. Res.* **12**, 181–201.
21. Frank, M. G. (1989). *Human Lie Detection Ability as a Function of the Liar's Motivation*, Unpublished doctoral dissertation, Cornell University, Ithaca.
22. Burgoon, J. E., and Buller, D. B. (1994). Interpersonal deception: III. Effects of deceit on perceived communication and nonverbal behavior dynamics. *J. Nonverbal Behav.* **18**, 155–184.
23. Waid, W. M., and Orne, M. T. (1982). The physiological detection of deception. *Am. Sci.* **70**, 402–409.
24. Steinbrook, R. (1992). The polygraph test: a flawed diagnostic method. *N. Engl. J. Med.* **327**, 122–123.
25. Frank, M. G. (2005). Research methods in detecting deception research. In *Handbook of Nonverbal Behavior Research*, J. Harrigan, K. Scherer, and R. Rosenthal, Eds. Oxford University Press, London, pp. 341–368.
26. DePaulo, B. M., Stone, J., and Lassiter, D. (1985). Deceiving and detecting deceit. In *The Self and Social Life*, B. R. Schlenker, Ed., McGraw-Hill, New York, pp. 323–355.
27. Vrij, A. (2000). *Detecting Lies and Deceit: The Psychology of Lying and the Implications for Professional Practice*. John Wiley & Sons, Chichester.
28. Zuckerman, M., and Driver, R. E. (1985). Telling lies: verbal and nonverbal correlates of deception. In *Multichannel Integration of Nonverbal Behavior*, W. A. Siegman, and S., Feldstein, Eds. Erlbaum, Hillsdale, NJ, pp. 129–147.
29. Frank, M. G. (2003). Smiles, lies, and emotion. In *The Smile: Forms, Functions, and Consequences*, M., Abel, Ed. The Edwin Mellen Press, New York, pp. 15–43.
30. Vrij, A., Edward, K., and Bull, R. (2001). Police officers' ability to detect deceit: the benefit of indirect deception detection measures. *Leg. Criminol. Psychol.* **6**, 185–196.
31. Bond, C. F. Jr., and DePaulo, B. M. (2006). Accuracy of deception judgments. *Pers. Soc. Psychol. Rev.* **10**, 214–234.
32. DePaulo, B. M., and Rosenthal, R. (1979). Telling lies. *J. Pers. Soc. Psychol.* **37**, 1713–1722.
33. Ekman, P., and O'Sullivan, M. (1991). Who can catch a liar? *Am. Psychol.* **46**, 913–920.
34. Ekman, P., O'Sullivan, M., and Frank, M. G. (1999). A few can catch a liar. *Psychol. Sci.* **10**, 263–266.
35. DePaulo, B. M., and Pfeifer, R. L. (1986). On-the-job experience and skill at detecting deception. *J. Appl. Soc. Psychol.* **16**, 249–267.
36. Kraut, R. E., and Poe, D. (1980). Behavioral roots of person perception: the deception judgments of customs inspectors and laymen. *J. Pers. Soc. Psychol.* **39**, 784–798.

37. Meissner, C. A., and Kassin, S. M. (2002). :"He's guilty!": investigator bias in judgments of truth and deception. *Law Hum. Behav.* **26**, 469–480.
38. Mann, S., Vrij, A., and Bull, R. (2004). Detecting true lies: police officers' abilities to detect suspects' lies. *J. Appl. Psychol.* **89**, 137–149.
39. Frank, M. G., and Ekman, P. (1997). The ability to detect deceit generalizes across different types of high stake lies. *J. Pers. Soc. Psychol.* **72**, 1429–1439.
40. Etcoff, N. L., Ekman, P., Magee, J. J., and Frank, M. G. (2000). Superior lie detection associated with language loss. *Nature* **405**(11), 139–139.
41. Forrest, J. A., Feldman, R. S., and Tyler, J. M. (2004). When accurate beliefs lead to better lie detection. *J. Appl. Soc. Psychol.* **34**, 764–780.
42. O'Sullivan, M., and Ekman, P. (2004). The wizards of deception detection. In *The Detection of Deception in Forensic Contexts*, P. A. Granhag, and L. Stromwell, Eds. Cambridge University Press, Cambridge, pp. 269–286.
43. Bond, C. F. Jr., and Atoum, A. O. (2000). International deception. *Pers. Soc. Psychol. Bull.* **26**, 385–395.
44. Bond, C. F., Omar, A., Mahmoud, A., and Bonser, R. N. (1990). Lie detection across cultures. *J. Nonverbal Behav.* **14**, 189–204.
45. Frank, M. G., and Feeley, T. H. (2003). To catch a liar: challenges for research in lie detection training. *J. Appl. Commun. Res.* **31**, 58–75.
46. Kassin, S. M., and Fong, C. T. (1999). "I'm innocent!": effects of training on judgments of truth and deception in the interrogation room. *Law Hum. Behav.* **23**, 499–516.
47. Bartlett, M. S., Littlewort, G., Frank, M. G., Lainscsek, C., Fasel, I., and Movellan, J. (2006). Fully automatic facial action recognition in spontaneous behavior. *J. Multimedia* **6**, 22–35.
48. Collins, R., Lincoln, R., and Frank, M. G. (2002). The effect of rapport in forensic interviewing. *Psychiatry Psychol. Law* **9**, 69–78.

# SPEECH AND VIDEO PROCESSING FOR HOMELAND SECURITY

MARK MAYBURY
*Information Technology Center, The MITRE Corporation, Bedford, Massachusetts*

## 1 SPEECH AND VIDEO FOR HOMELAND SECURITY

As articulated in the National Strategy for Homeland Security (www.whitehouse.gov/homeland/book) [1], homeland security requires effective performance of a number of

primary missions such as border and transportation security and critical infrastructure protection. These activities are human intensive, both in terms of the objects of focus (e.g. citizens or foreigners crossing a border) as well as the government or contractor personnel performing these function (e.g. TSA at US airports). Automation is necessary to ensure effective, objective, and affordable operations. Speech and video processing are important technologies that promise to address some of the severe challenges of the homeland security mission. Furthermore, there is some hope that the detection of visual or acoustic anomalies (e.g. unnatural human motion and voice stress) could yield improved deception detection.

With thousands of miles of border with Mexico and Canada and 95,000 miles of shoreline, border and transportation security is a daunting challenge. Some important applications include the following:

- Video surveillance for anomalous and/or hostile behavior detection has important applications at border crossings as well as monitoring remote border areas.
- Identification and tracking of individuals using biometrics (e.g. speech, face, gait, and iris). For example, speaker identification can be used for authentication for both physical access control and computer account access. While details of biometrics are beyond the scope of this article, we refer the reader to an overview text [2] or a more detailed algorithmic approach [3].

Other critical homeland security applications are as follows:

- Critical infrastructure protection to include key site monitoring (e.g. transportation, energy, food, and commerce) or video surveillance of public areas. This could include automated video understanding, in particular the detection, classification, and tracking of objects such as cars, people, or animals in time and space in and around key sites. Beyond object detection and tracking, it would include recognition of relationships and events.
- Automated processing of audio and video to understand broadcast news and/or index video surveillance archives.
- Audio hot spotting for surveillance at a border crossing or large-scale public events.
- The use of audio or video analysis to detect deception (e.g. irregular physical behavior and/or speech patterns) but also audio and video cryptography to obscure message content or audio and video stenography to hide its very existence, and countermeasures thereof.

Some of the requirements for these applications are severe. These include

- broad area surveillance;
- long duration: $24 \times 7$ detection;
- real-time detection;
- high accuracy and consistency;
- completely autonomous operation;
- low or intermittent communications bandwidth (e.g. for storage and exfiltration);
- low acquisition and maintenance cost.

Some deployments may also require low power consumption (and/or long battery life), limited storage, and intermitted connectivity.

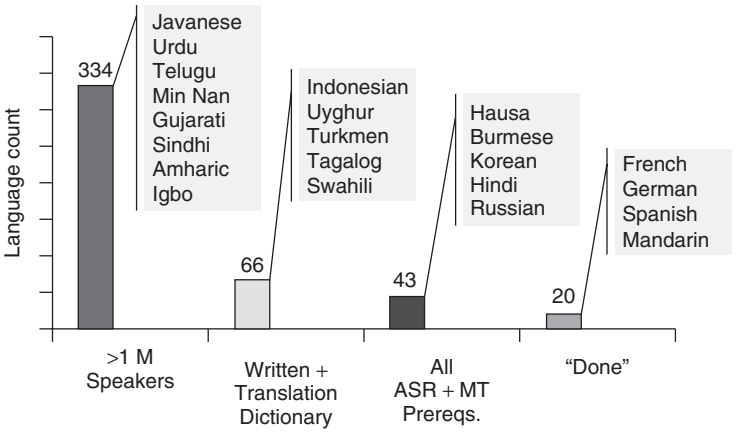
## 2 THE CHALLENGE OF SPEECH

The ability to detect and track criminal or adversary communications is essential to homeland security. Whether for law enforcement or intelligence, searching conversational speech is a grand challenge. Telephone conversations alone illustrate the scale of the challenge with over a billion fixed lines worldwide creating 3785 billion minutes (63B hours) of conversations annually, equivalent to about 15 exabytes of data (ITU 2002). Add to this rapidly growing mobile and wireless communication. In addition, 47,776 radio stations add 70 million hours of original radio programming per year. Further complicating this, approximately 6800 languages and as much as 10,000 dialects are spoken globally. In spite of this untapped audio gold mine, audio search requirements are only beginning to appear.

As Figure 1 illustrates, there are over 300 spoken languages with more than one million speakers, but only 66 of these are written and for which we have a translation dictionary. Of these, we have ASR and MT for only 44, and only 20 of these are considered "done" in the sense that systems exist for automated transcription and translation.

In addition to the challenge of lack of written materials, which we will return to subsequently, there are many challenges beyond scale. These include challenges with language in general, such as polysemy, ambiguity, imprecision, malformedness, intention, and emotion. And in addition to the traditional set of challenges with automated speech recognition such as noise, microphone variability, and speaker disfluencies, the kind of conversational speech that occurs in telephone calls, meetings, interviews has the following additional challenges:

- *Multiparty.* Multiple, interacting speakers.
- *Talkover.* Multiple simultaneous speakers talk over speaker turns.




(Source: Linguistic Data Consortum's DARPA Surprise Language Experiment assessment of FL resources, 2003)

**FIGURE 1** Spoken foreign language systems and needs.

- *Spontaneity.* Unpredictable shifts in speakers, topics, and acoustic environments.
- *Diverse settings.* Conversation is found in many venues including outdoor border crossings, indoor meetings, radio/TV talk shows, interviews, public debates, lectures or presentations that vary in degree of structure, roles of participants, lengths, degree of formality, as well as variable acoustic properties.
- *Acoustic challenges.* Spoken conversations often occur over cell phones or handheld radios which come in and out of range and have highly variable signal to noise ratios.
- *Nonacoustic conversational elements.* Speakers use clapping, laughing, booing, whistling, and other sounds and gestures to express agreement, disagreement, enjoyment, and other emotions, as well as outdoor noise (e.g. weather and animals) and indoor noise (e.g. machinery and music).
- *Real time and retrospective.* Access during the speech event (e.g. real-time stream processing) or after.
- *Tasks.* Speaker identification, word hot spotting, audio document routing (doc/passage/fact), retrieval or question/answering, tracking entities and events, and summarization (e.g. speakers and topics)
- *Multilingual.* Multiple languages, sometimes from the same speaker.
- *References.* Since conversations are often performed in a physical context, the language often contains references to items therein (exophora).

Compounding these challenges, expert translators, particularly for low density languages are expensive and scarce.

In addition to the challenges with speech, for large collections of audio, there exist many retrieval challenges such as triage, storage, query formulation, query expansion, query by example, results display, browsing, and so on.

## 3 AUTOMATED SPEECH PROCESSING

Figure 2 illustrates the significant progress made over the years in spoken language processing. The figure shows best systems each year in evaluations administered by NIST to objectively benchmark performance of speech recognition systems over time. The graph reports reduction of word error rate (WER) over time. The systems were assessed based on a wide range of increasingly complex and challenging tasks moving from read speech, to broadcast (e.g. TV and radio) speech, to conversational speech, to spontaneous speech, to foreign language speech (e.g. Chinese Mandarin and Arabic). Over time, tasks have ranged from understanding read Wall Street Journal text, to understanding foreign television broadcasts, to the so-called "switchboard" (fixed telephone and cellphone) conversations. Future plans include meeting room speech recognition (NIST; [4]).

As Figure 2 illustrates, while recognition, rates of word error for English (clean, well-formed, single speaker, speaking clearly to computer) are well below 10%. For example, computers can understand someone reading the Wall Street Journal with a 5% word error rate (WER) (1 word in 20 wrong). Conversations are harder, with broadcast news often achieving only a 15–20% WER and the CALLHOME data collection (phone calls) achieving 30–40% WER.

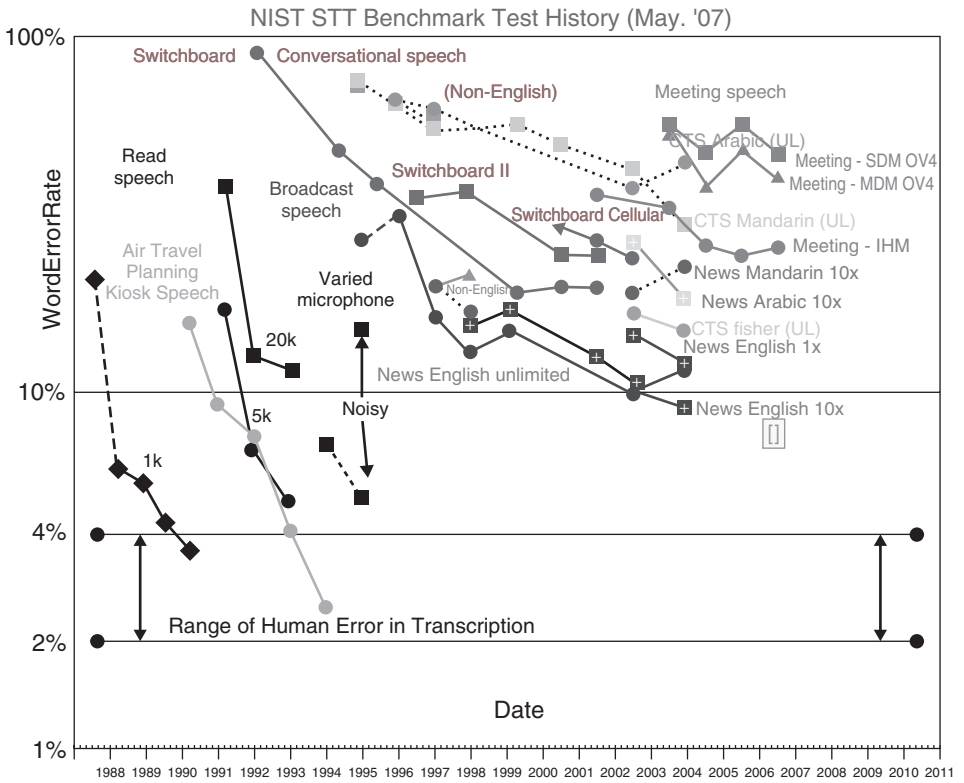



**FIGURE 2** NIST benchmarks over time. (http://www.nist.gov/speech/history.)

## 4 AUDIO HOT SPOTTING

As an illustration of the state of the art, the Audio Hot Spotting project [5–7] aims to support natural querying of audio and video, including meetings, news broadcasts, telephone conversations, and tactical communications/surveillance. As Figure 3 illustrates, the architecture of AHS integrates a variety of technologies including speaker ID, language ID, nonspeech audio detection, keyword spotting, transcription, prosodic feature and speech rate detection (e.g. for speaker emotional detection), and cross language search.

An important innovation of AHS is the combination of word-based speech recognition with phoneme-based audio retrieval for mutual compensation for keyword queries. Phoneme-based audio retrieval is fast, more robust to spelling variations and audio quality, and may have more false positives for short-word queries. In addition, phoneme-based engines can retrieve proper names or words not in the dictionary (e.g. "Shengzhen") but, unfortunately, produces no transcripts for downstream processes. In contrast, word-based retrieval is more precise for single-word queries in good quality audio and provides transcripts for automatic downstream processes. Of course it has its limitations too. For example, it may miss hits for phrasal queries, out-of-vocabulary words, and in noisy audio, and is slower in preprocessing.

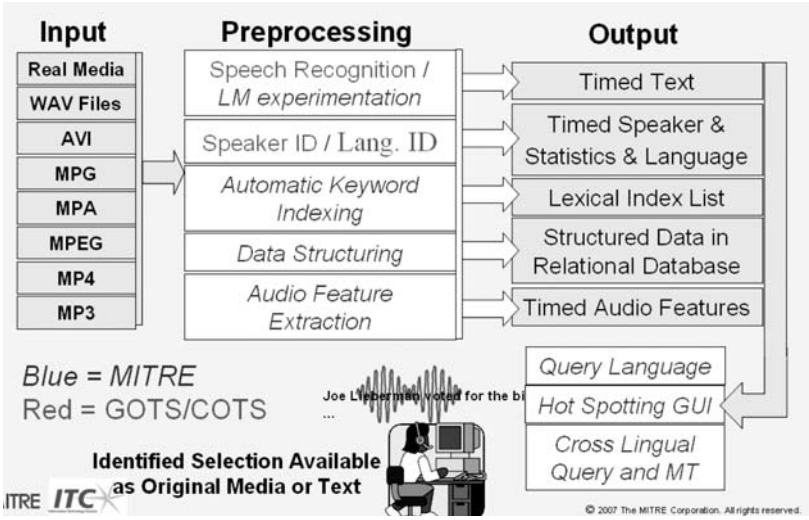



**FIGURE 3** AHS architecture.

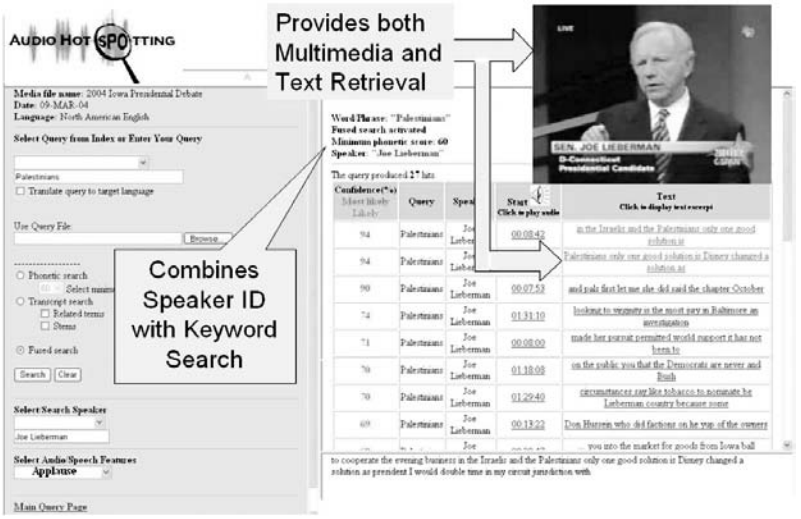



**FIGURE 4** AHS search interface.

Figure 4 illustrates the user interface for speech search, and includes a speaker and keyword search facility against both video and audio collections. The user can also search by nonspeech audio (e.g. clapping and laughter).

For crosslingual needs, a query in English is translated to a foreign language (e.g. Spanish and Arabic) and is used to retrieve hot spots in a transcription of the target media, which is then retrieved and translated into the query language. This process is illustrated in Figure 5. The user typed in word “crisis” is translated into Arabic query term and is used to search the target media, which is subsequently translated as shown.

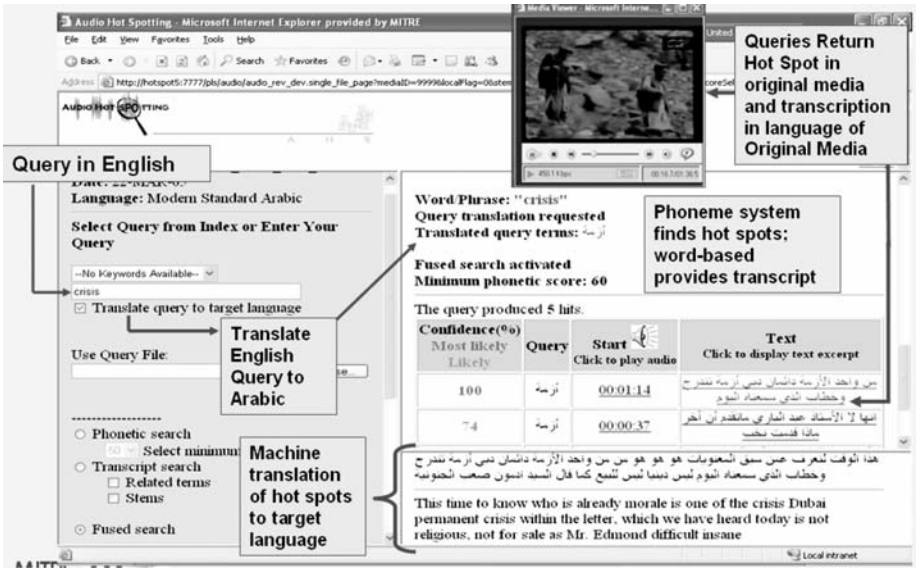



**FIGURE 5** AHS crosslingual audio hot spotting.

## 5 DECEPTION DETECTION

Detection of deception is important for assessing the value of informants, identifying deception at border crossing, and for antifraud, and can be revealed by face, voice, and body [8]. Evidence of increased pitch and vocal tension in deceptive subjects has been found from the literature survey [9]. The most widely cited sources of evidence of deception using speech include latency, filled pauses, discourse coherence, and the use of passive voice and contractions. However, most research on deceptive behavior has focused on visual cues such as body and facial gestures or on descriptive as opposed to empirical studies much less automated means of detection.

Hirschberg et al. [10] and Graciarena et al. [11] report on the use of a corpus-based machine learning approach to automated detection of deception in speech. Both leverage the Columbia-SRI-Colorado (CSC) corpus that consists of 22 native American English speakers who were motivated by financial reward to deceive an interviewer on two tasks out of six in sessions lasting between 25 and 50 min. Using a support vector machine based on prosodic/lexical features combined with a Gaussian mixture model based on acoustic features, Graciarena et al. [11] report 64.4% accuracy in automatically distinguishing deceptive from nondeceptive speech. Although these efforts are promising, one national study [12] argues for the need for significant interdisciplinary research in this important area.

## 6 THE CHALLENGE OF VIDEO

Just as acoustic information provides vital information for homeland security, so too visual information is a critical enabler. Although static images are commonly used to

identify suspects, characterize facilities, and/or describe weapons and threats, motion pictures have become increasing valuable because of their ability to capture not only static objects and their properties but also dynamic events. The following are the challenges faced by video processing:

- *Broad area coverage.* 24 × 7 video surveillance of a broad area poses challenges with processing, storage, power, and sustainability. For example,
  - thousands of cameras are deployed in the United Kingdom for tasks such as facility surveillance, traffic monitoring, and environmental observations (e.g. river levels).
- *Real-time processing.* Events (e.g. border crossing and crimes) occur in real time and frequently require immediate intervention. For example,
  - a new nationwide network of cameras at the National Automatic Number Plate Recognition Data Centre north of London will record up to 50 million license plates a day to detect duplicates and track criminals.
- *Massive volume.* Video requires roughly 10 times as much storage as audio therefore methods for compression should be efficient for storage and dissemination. Moreover, real-time or retrospective human review of material is tedious and an ideal opportunity for automation.
- *Accuracy and consistency of detection, identification, and tracking.* Object and event detection and recognition in a broad range of conditions (lighting, occlusion, and resolution) are severe challenges.
- *Privacy preservation.* The broad deployment of cameras raises challenges for privacy as well as cross boundary sharing identical systems.
- *Processing.* Effective understanding of video requires many subchallenges including format conversion, detection, segmentation, object/face recognition, gesture and gait recognition, and event understanding.
- *Nature.* Occlusion (e.g. fog and rain), lighting, object orientation, and motion require size, rotation, shape, and motion invariant detection that are robust to natural variation.
- *Noise.* Noise from lenses, cameras, the environment (e.g. lighting and smoke/fog/snow), storage, and transmission.
- *Variability.* The natural variability in foreground, background, objects, relationships, and behaviors as well as wide variations in illumination, pose, scale, motion, and appearance.

There are many benefits of automated video processing including the followin:

- Automated identification and tracking.
- Correlation. Storage and indexing can enable correlation of objects across time and space, pattern detection, forensics as well as trend analysis.
- Cross cuing. Initial detection of objects or events can cue more complete or higher quality tracking.
- Compression. Object ID and tracking can dramatically reduce storage and dissemination needs.

There are many important application areas of video processing, from interview deception detection to monitoring of border crossings or facilities (e.g. airport and military base entrances). For example, the Bordersafe project [13] automatically extracts license plate numbers from video as cars travel in and around Tucson, Arizona. The Tuscon Customs and Border Protection (CBP) has captured over 1 million records of license plate numbers, state, date, and time from over 225,000 distinct vehicles from both the United States and Mexico. Comparison revealed that plates from over 13,000 of those border crossing vehicles (involved in nearly 60,000 border crossings) were associated with criminal records from Tuscon and Pima County law enforcement.

## 7 AUTOMATED VIDEO PROCESSING

The key elements necessary for automated understanding of video have been explored since the early days of vision research in robotics in artificial intelligence. In addition to systems to process imagery from security surveillance cameras, algorithms are needed to analyze the 31 million hours of original television programming per year from over 20,000 broadcast stations around the world. For example, as illustrated in Figure 6, using an integration of text, audio, imagery, and video processing, the Broadcast News Navigator [14] enables a user to browse and perform content-based search on videos personalized to their interests. Users can find content two and one half times faster over sequential video search with no loss in accuracy by searching directly for specific content. The related Informedia system (www.informedia.cs.cmu.edu) has explored video privacy protection via methods such as face pixelizing, body scrambling, masking, and body replacement.

Homeland security users may need to monitor not only broadcast news, but other video sources such as security cameras. As illustrated in Figure 7, research at MIT has

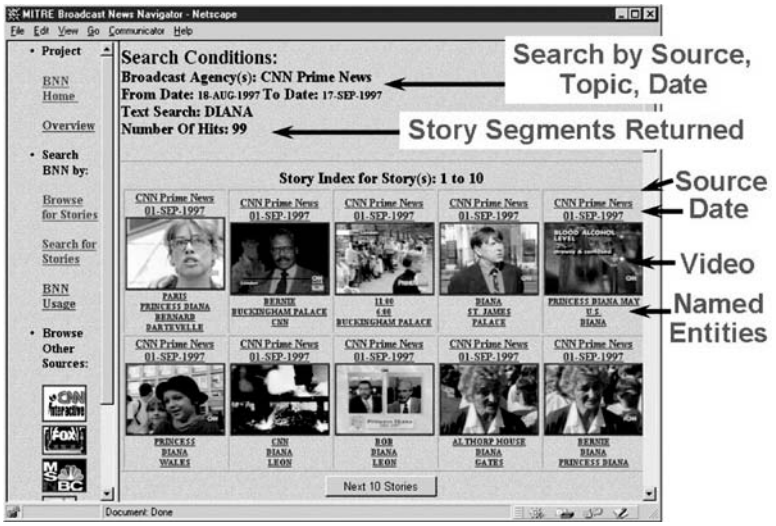



**FIGURE 6** Broadcast news navigation.

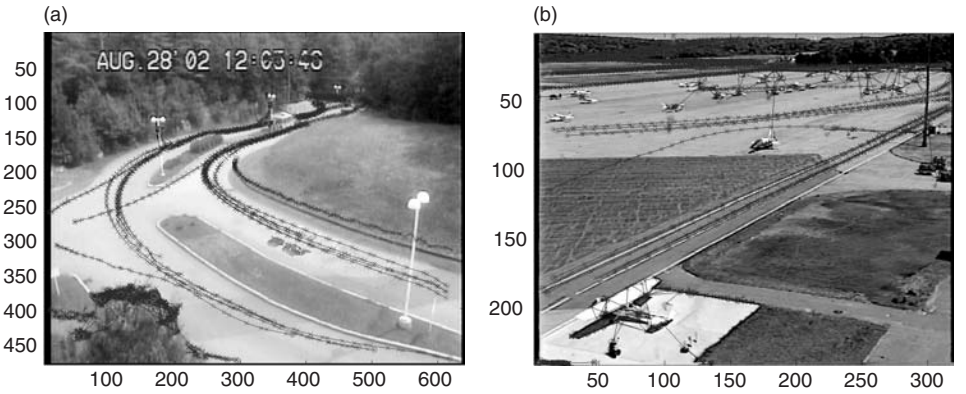



**FIGURE 7** Motion tracks detected on airport tarmac (a) and office park (b).

integrated question answering technology together with video understanding methods to create a video question answering system.

Figure 7 illustrates motion tracks detected in two different settings: an airport tarmac (a) and an entrance gate to an office park (b). This is used by Katz et al. [15] in a prototype information access system, called *Spot*, that combines a video understating system together with a question answering natural language front end to answer questions about video surveillance footage taken around the Technology Square area in Cambridge, Massachusetts. Spot can answer questions such as the following:

- "Show me all cars leaving the garage."
- "Show me cars dropping off people in front of the white building"
- "Did any cars leave the garage toward the north?"
- "How many cars pulled up in front of the office building?"
- "Show me cars entering Technology Square."
- "Give me all northbound traffic."

This kind of intuitive, query-based access to information can dramatically enhance both facility situational awareness and enable focused investigation.

## 8 MULTICAMERA VIDEO ANALYSIS

In addition to moving object detection, identification, and tracking, employment of active multicamera systems enables wide area surveillance, mitigates occlusion, and reveals 3D information [16]. However, multicamera systems require solutions for emplacement and use, selection of best views, cross camera handoff of tracked objects, and multisensor fusion. These have been successfully used for surveillance of people at the SuperBowl or for traffic monitoring. Active cameras—that support active pan, tilt, and zoom—allow automated focus attention on objects of interest in scenes. In addition to the visible spectrum, infrared sensors can help track humans, animals, and vehicles hidden in dense foliage. Multicamera environments can enable, for example, continuous monitoring of critical infrastructure (e.g. air or seaport, military facility, and power plant), detect

perimeter breaches, track moving people or vehicles, pan/tilt/zoom for identification, and issue alerts.

## 9 STATE OF THE ART

With all of the rapid advances in video processing, how well do these systems work? As illustrated in Figure 8, NIST organizes an annual benchmarking activity to compare the performance of video understanding systems. As can be seen, this annual event has grown from a few participants in 2001 processing about a dozen hours of video to dozens of participants processing hundreds of hours worth of video to support search for particular video segments.

For example, in the 2004 NIST TRECVID benchmarking activities [17], participants included IBM Research, Carnegie Mellon University, University of Amsterdam. They applied their systems to four tasks required to find relevant segments in video data sets: shot boundary, story boundary, and feature detection as well as search. The video data set contained over 184 h of digitized news episodes from ABC and CNN with the task of discovering 10 types of segment, in particular:

- *Boat/ship.* Segment contains video of at least one boat, canoe, kayak, or ship of any type.
- *Bill Clinton.* Segment contains video of Bill Clinton.
- *Madeleine Albright.* Segment contains video of Madeleine Albright.
- *Train.* Segment contains video of one or more trains or railroad cars that are part of a train.
- *Beach.* Segment contains video of a beach with the water and the shore visible.
- *Airplane takeoff.* Segment contains video of an airplane taking off, moving away from the viewer.
- *People walking/running.* Segment contains video of more than one person walking or running.

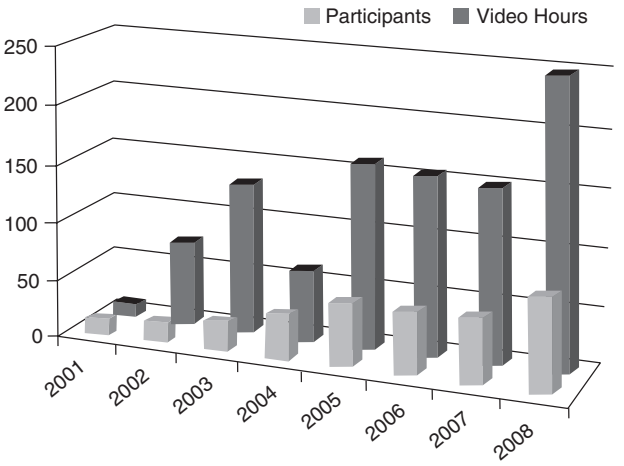



**FIGURE 8** TRECVID trends.

- *Physical violence.* Segment contains video of violent interaction between people and/or objects.
- *Road.* Segment contains video of part of a road, any size, paved or not.
- *Basket scored.* Segment contains video of a basketball passing down through the hoop and into the net to score a basket—as part of a game or not.

To address the diversity of potential video data and to continually challenge researchers, each year the data sets grow and the evaluation tasks are expanded. For example, the TRECVID 2005 data set added multilingual video (Chinese and Arabic in addition to English) and the topics were slightly different and ranged from finding video segments of people (e.g. prisoner), places (e.g. mountain, building exterior, and waterscape/waterfront), things (e.g. car, map, and US flag) to events (e.g. people walking/running, explosion or fire, and sports). In 2007, a video summary task was added to the existing shot boundary, search, and feature detection tasks and in 2008 surveillance event detection was added along with 100 h of airport surveillance video.

Effectiveness on video segment retrieval is measured primarily using mean average precision (the mean of the average precision of each query), which ranges widely by topic. Other measures include search processing time and precision at various depths. For interactive searches, participants are encouraged to collect data on usability as seen by each searcher. For example, in 2006, interactive retrieval of Tony Blair segments were achieved at nearly 90% mean average precision, whereas segments of people entering or leaving a building were recognized at only the 10% level.

## 10 FUTURE RESEARCH

The challenges of audio and video analysis are daunting but with the rapid growth of sources, the need is equally great. Spoken dialog retrieval is an exciting research area precisely because it contains all the traditional challenges of spoken language processing together with the challenges imposed by the retrieval task. Some important spoken conversation processing challenges include [18]

- dealing with multiple speakers;
- dealing with foreign language and associated accents;
- incorporating nonspeech audio dialog acts (e.g. clapping and laughter);
- conversational segmentation and summarization;
- discourse analysis, such as analyzing speaking rates, turn taking (frequency and durations), concurrence/disagreement, which often provides insights into speaker emotional state, attitudes toward topics and other speakers, and roles/relationships.

Some important speech retrieval challenges include the following:

- How can we provide a query by example for a speech or audio signal, for example, find speech that sounds (acoustically and perceptually) like this? (See Sound Fisher in Reference 19.)
- How can we provide (acoustic) relevancy feedback to enhance subsequent searchers?

- How do we manage whole story/long passage retrieval that exposes users to too much errorful ASR output or too much audio to scan?
- Because text-based keyword search alone is insufficient for audio data, how do we retain and expose valuable information embedded in the audio signal?
- Are nonlinguistic audio cues detectable and useful?
- Can we utilize speech and conversational gists (of sources or segments) to provide more efficient querying and browsing.

Some interesting application challenges are raised, such as dialog visualization, dialog comparison (e.g. call centers), or dialog summarization, simultaneously with the challenge of addressing speech and dialog.

Like audio analysis, video analysis has many remaining research challenges. These include

- scalable processing to address large-scale video collections;
- processing of heterogeneous video sources from cell phone cameras to handheld video cameras to high definition mobile cameras;
- robustness to noise, variability, and environmental conditions;
- bridging the "semantic gap" between low level features (e.g. color, shape, and texture) and high level objects and events.

The combination of both audio and video processing is an area of research that promises combined effects. These include

- cross modal analysis to support cross cuing for tasks such as segmentation and summarization;
- cross modal sentiment analysis for detection of bias and/or of deception;
- cross media analysis for biometrics for identity management to overcome the noise and errorful detection in single media (e.g. audio and video) identification;
- utilization of speech and conversational gists (of video sources or segments) to provide more efficient video querying and browsing.

In conclusion, speech and video processing promise significant enhancement to homeland security missions. Addressing challenges such as scalability, robustness, and privacy up front will improve the likelihood of success. Mission-oriented development and application promises to detect dangerous behavior, protect borders, and, overall, improve citizen security.

## REFERENCES

1. Office of Homeland Security (2002). *National Strategy for Homeland Security*. http://www.whitehouse.gov/homeland/book.
2. Woodward, J., Orlans, N., and Higgins, P. (2003). *Biometrics: Identity Assurance in the Information Age*. McGraw-Hill, Berkely, CA.
3. Gonzales, R., Woods, R., and Eddins, S. (2004). *Digital Image Processing using MATLAB*. Prentice-Hall, Upper Saddle River, NJ.

4. Zechner, K., and Waibel, A. (2000). DiaSumm: flexible summarization of spontaneous dialogues in unrestricted domains. *Proceedings of the 18th Conference on Computational Linguistics*, Saarbrücken, Germany, pp. 968–974.
5. Hu, Q., Goodman, F., Boykin, S., Fish, R., and Greiff, W. (2003). Information discovery by automatic detection, indexing, and retrieval of multiple attributes from multimedia data. *The 3rd International Workshop on Multimedia Data and Document Engineering*. September 2003, Berlin, Germany, pp. 65–70.
6. Hu, Q., Goodman, F., Boykin, S., Fish, R., and Greiff, W. (2004). Audio hot spotting and retrieval using multiple audio features and multiple ASR engines. *Rich Transcription 2004 Spring Meeting Recognition Workshop at ICASSP 2004*. Montreal.
7. Hu, Q., Goodman, F., Boykin, S., Fish, R., and Greiff, W. (2004). Audio hot spotting and retrieval using multiple features. *Proceedings of the HLT-NAACL 2004 Workshop on Interdisciplinary Approaches to Speech Indexing and Retrieval*. Boston, USA, pp. 13–17.
8. Ekman, P., Sullivan, M., Friesen, W., and Scherer, K. (1991). Face, voice and body in detecting deception. *J. Nonverbal Behav*. **15**(2), 125–135.
9. DePaulo, B. M., Lindsay, J. J., Malone, B. E., Muhlenbruck, L., Charlton, K., and Cooper, H. (2003). Cues to deception. *Psychol. Bull*. **129**(1), 74–118.
10. Hirschberg, J., Benus, S., Brenier, J., Enos, F., Friedman, S., Gilman, S., Girand, C., Graciarena, M., Kathol, A., Michaelis, L., Pellom, B., Shriberg, D., Stolcke, A. (2005). Distinguishing deceptive from non-deceptive speech. *Interspeech 2005*. September 4–8, Lisbon, Portugal, pp. 1833–1836.
11. Graciarena, M., Shriberg, E., Stolcke, A., Enos, F., Hirschberg, J. and Kajarekar, S. (2006). Combining prosodic, lexical and cepstral systems for deceptive speech detection. *Proceedings of IEEE ICASSP*. Toulouse.
12. Intelligence Science Board (2006). *Educing Information. Interrogation: Science and Art*. National Defense Intelligence Council Press, Washington, DC, http://www.dia.mil/college/pubs/pdf/3866.pdf.
13. Chen, H., Wang, F.-Y., and Zeng, D. (2004). Intelligence and security informatics for homeland security: information, communication, and transportation. *IEEE Trans. Intell. Transp. Syst*. **5**(4), 329–341.
14. Maybury, M., Merlino, A., and Morey, D. (1997). Broadcast news navigation using story segments, *ACM International Multimedia Conference*. November 8–14, Seattle, WA, pp. 381–391.
15. Katz, B., Lin, J., Stauffer, C., and Grimson, E. (2004). Answering questions about moving objects in videos. In *New Directions in Question Answering*, Maybury, M., Ed. MIT Press, Cambridge, MA, pp. 113–124.
16. Trivedi, M. M., Gandhi, T. L., and Huang, K. S. (2005). Distributed interactive video arrays for event capture and enhanced situational awareness. *IEEE Intell. Syst*. **20**(5), 58–66.
17. Smeaton, A. F., Over, P., and Kraaij, W. (2006). Evaluation campaigns and TRECVid. In *Proceedings of the 8th ACM international Workshop on Multimedia information Retrieval* (Santa Barbara, California, USA, October 26–27, 2006). MIR '06. ACM, New York, NY, pp. 321–330.
18. Maybury, M. (2007). Searching conversational speech. Keynote at workshop on searching spontaneous conversational speech. *International Conference on Information Retrieval (SIGIR-07)*. 27 July 2007. Seattle, WA.
19. Maybury, M. Ed. (1997). *Intelligent Multimedia Information Retrieval*. AAAI/MIT Press, Menlo Park, CA, ( http://www.aaai.org:80/Press/Books/Maybury-2/).

## FURTHER READING

Maybury, M. Ed. (2004). *New Directions in Question Answering*. AAAI/MIT Press, Cambridge, MA.

*NIST Meeting Room Project: Pilot Corpus*. http://www.nist.gov/speech/test_beds.

Popp, R., Armour, T., Senator, T., and Numrych, K. (2004). Countering terrorism through information technology. *Commun. ACM* **47**(3), 36–43.

Tao, Li., Tompkins, R., and Asari, V. K. (2005). *An Illuminance-Reflectance Nonlinear Video Enhancement Model for Homeland Security Applications*, *aipr*, 34th Applied Imagery and Pattern Recognition Workshop (AIPR'05), pp. 28–35.

# TRAINING AND LEARNING DEVELOPMENT FOR HOMELAND SECURITY

EDUARDO SALAS AND ELIZABETH H. LAZZARA
*University of Central Florida, Orlando, Florida*

## 1 INTRODUCTION

On December 22, 2001, Richard Colvin Reid hid explosives in his shoes in an effort to destroy American Airlines Flight 63 bound to the United States from Paris (BBC News 2008) [1]. His attempt was ultimately unsuccessful because other passengers were able to resolve the situation; however, the world would come to know this man as the "shoe bomber". This incident marked a drastic change in the policies and procedures for commercial airlines in order to ensure the safety of all people onboard. Due to the high-risk nature of the situation and the consequences of possible outcomes, all employees responsible for screening passengers boarding aircrafts would be mandated to undergo intense training to be able to detect any clues to prevent another such occurrence happening in the future.

This example illustrates the importance of training and learning development in Homeland Security (HS). Recently, Salas and colleagues [2] define training as "the systematic acquisition of knowledge (i.e. what we need to know), skills (i.e. what we need to do), and attitudes (i.e. what we need to feel) (KSAs) that together lead to improved performance in a particular environment" (p. 473). Learning occurs when there is a permanent cognitive and behavioral change by acquiring the requisite competencies to perform the

job. We submit that learning is facilitated when the training design and delivery is guided by the findings from the science of learning (and training). The purpose of this article is to provide some insights about the science and offer some principles to help in designing, developing, implementing, and evaluating training.

## 2 THE PHASES OF TRAINING

The design of training is a process that consists of a set of interrelated phases that have to be effective; it must be applied systematically. In this article, we discuss four general training phases. These phases, and associated principles and guidelines, represent what we know from the science that works and must be done when designing and delivering training in any organization. We hope that these will guide those in the practice of designing and implementing training for HS purposes. As noted, effective training requires attention to four phases [3]. These are discussed below with specific principles to guide the focus and shape the actual elements in each phase.

### 2.1 Phase 1: Analyze the Organizational Training Needs

This is one of the most critical phases of training because many important decisions are made at this juncture. It is in this phase where skill deficiencies are determined and where the environment is prepared and set for learning and transfer to occur in the organization. Therefore, before training can be successfully designed and implemented, it is necessary to assess the needs of the organization. This is done in order to properly set up the learning environment to uncover the necessary KSAs and prepare the organization for the training.

***2.1.1 Uncover the Required KSAs.*** To determine what KSAs are needed, all of the required tasks to be performed must be analyzed. Ideally, the analysis focuses on the competencies that must be acquired and not on the actual tasks to be performed because competencies are common throughout a variety of tasks. To uncover the requisite KSAs, organizations should conduct a task analysis and/or cognitive task analysis. Task analyses are needed to determine what competencies are needed to perform a job successfully. Cognitive tasks analysis goes deeper and uncovers the knowledge or cognitions underneath job performance. These analyses set the foundation for designing a successful training program. It helps in establishing the training objectives, the learning outcomes, and provides the learning expectations for both trainers and trainees. Furthermore, the training objectives outline the conditions that will take place during job performance, and they provide the acceptable criterion to measure performance [4].

In addition to uncovering and analyzing the necessary competencies, it is also critical to determine who exactly needs to be trained and what they need to be trained on. Conducting a person analysis ensures that the right people get the appropriate training. Employees possess and need different KSAs; therefore, they do not necessarily require the same kind of training. More experienced employees would not need an extensive, intense training session compared to new, inexperienced employees.

***2.1.2 Prepare the Organization.*** Before a training system can be designed and implemented, the organization needs to be prepared. Goldstein and Ford [5] proposed that some aspects of the organization to be considered include "an examination of organizational goals, resources of the organization, transfer climate for training, and internal and external constraints present in the environment" (p. 41). In other words, do the goals of the organization and training program align? Does the training support the strategic goals of the organization? What are the available resources (e.g. finances, technology, and so on)? What are the possible limitations that the training might encounter based upon the existing resources? Lastly, is the organizational climate fostering learning and the importance of the training? That is, is the climate and culture conducive in transferring the newly acquired KSAs to the actual operating environment? Is the organization motivating the trainees to attend training? To set up the appropriate climate, organizations need to send out positive messages about training so that trainees will see the value of the training. Trainees will also be more supportive of the training system if it is voluntary rather than being mandatory. If training must be mandatory, make it with as few obstacles as possible. Overall, the organizational climate should support and encourage the training to ensure its success.

In total, determining the precise training needs is imperative. Knowing what, why, who, when, and how to train before designing training is a must. Organizations get the most out of training when the required KSAs are uncovered and the organizations prepare the training and set its climate to support learning.

## 2.2 Phase 2: Design and Develop Instruction

The second phase is about designing and developing the instructional content, storyboards, lesson plans, materials, curriculum, and preparing all the resources needed to deliver and implement the training. A number of factors are important here; most notably, the reliance of the science of training to drive the decision as much as possible. This science has produced many guidelines, tips and examples that can be applied [3, 6, 7].

***2.2.1 Rely on Scientifically Rooted Instructional Principles.*** Clearly, effective training is about applying pedagogically sound principles to the design of instruction. It is about using the science to create a learning environment that will engage, motivate, propel, and immerse the trainee in acquiring KSAs. Thus, it is critical when designing training to consider individual factors (e.g. cognitive ability, self efficacy, and motivation) as well as organizational factors (e.g. policies, procedures, prepractice conditions, and feedback) because they are extremely influential in the learning outcomes. For example, a trainee's motivation level can determine their ability to acquire, retain, and apply trained skills; therefore, training should be designed to enhance the motivation to learning of the trainees [8, 9].

***2.2.2 Set up Prepractice Conditions.*** In addition to establishing a positive organizational climate, organizations must set up prepractice conditions to enhance the effectiveness of the training system [10]. The efforts made prior to training will positively affect learning and ultimately performance; therefore, trainees should be prepared even before training begins. They should receive preparatory information about the training

(e.g. brochures and pamphlets) or advanced organizers to manage the information [11]. Furthermore, providing trainees with attentional advice can guide them in deciding what strategies will foster learning [3]. The benefit of setting up the prepractice conditions is that not only will it benefit trainees by optimizing learning but it is also a cost-effective way to facilitate the success of the training system.

***2.2.3 Create Opportunities to Practice and Receive Feedback.*** Any training seeks to give information about needed concepts, demonstrate required cognitions and behaviors, and creates opportunities to practice and receive feedback. The instructional delivery should be guided by training objectives; and the information, demonstration, and/or practice-based strategy demonstrations should target the wanted KSAs. The practice opportunities should be challenging and vary in difficulty because it is not the quantity of practice per se that is important but rather the quality of practice. Mere repetition does not necessarily enhance learning; therefore, as trainees learn and improve their KSAs, the scenarios should be more difficult and varied. To ease comparisons and ensure standardizations, scenarios should be designed a priori [12]. Moreover, developing the scenarios prior to training eases the burden on trainers by allowing them more control. In addition, instructors can focus on providing trainees with feedback because it will foster training by providing guidance on what areas are lacking and still need improvement [13].

***2.2.4 Seek to Diagnose KSAs' Deficiences.*** In order to establish whether trainees learned the requisite KSA, performance measures must be created to assess the trained competencies against the stated objectives. Ideally, performance measures evaluate processes as well as outcomes on both the individual and team level (if applicable; [3]). The effectiveness of the training lies heavily on the ability to assess and diagnose performance [14]. Therefore, organizations should take careful consideration when deciding what tool to use to evaluate performance against the trained objectives. One approach is to utilize a behavioral checklist (e.g. Targeted Acceptable Responses to Generated Events or Tasks (TARGETS)—), which evaluates trainees by recording the presence or absence of desired behaviors to scripted events [15]. Other approaches are available as well (see [16]).

## 2.3 Phase 3: Implement the Training

The third phase is the implementation or actual execution of the training program or system. This is the more "mechanical" part, but pay attention to the location, resources, instructor, and the delivery of the instructional system (e.g. information or practice based).

***2.3.1 Put Everything into Action.*** After the training has been designed, it is time to implement it. Now, it is time to identify the training site and ensure that it is prepared prior to training. The training site should be a comfortable setting and equipped with the proper resources. Instructors must also be trained and prepared to be able to address any issues/concerns that may arise during training. At this point, any instructional materials are finally carried out and the training is completely functional. Preferably, the fully

functioning training should be pilot tested to discover any potential problems and to be able to make the appropriate adjustments [17]. Because of the possibility that things will go wrong, relapse prevention procedures should be created in order to solve any dilemmas.

### 2.4 Phase 4: Evaluate the Training

The fourth phase is one that most organizations want to implement; however, most avoid it altogether or just simply do not go deep enough to truly determine the effectiveness of the training. Evaluations are designed to determine what worked and to assess the impact of the training system on the organization.

***2.4.1 Use a Multilevel Approach.*** Incorporating a training program into an organization does not stop once it has been implemented. The training must be evaluated to truly determine its effectiveness. Ideally, researchers suggest taking a multilevel approach to evaluation in order to obtain the complete picture. Kirkpatrick [18] devised a popular evaluation strategy measuring reactions, learning, behavioral change, and organizational impact. A multilevel approach will identify the successful aspects of the training program as well as the elements that are still lacking and need further adjustments in order to improve. When evaluations are based on only one dimension, it is easy to obtain an inaccurate assessment of the impact of the training intervention. For example, it is possible that trainee reactions are positive, yet learning did not take place [19]. Therefore, it is beneficial to examine at higher levels (e.g. learning and behavioral change; [20]). Assessments at the behavioral level will indicate whether the trained KSAs will be transferred to on the job performance [5]. Thus, it is not only crucial that trainees react positively and learn the material, but it is also important that they apply the trained KSAs to the job.

***2.4.2 Ensure Transfer of the Acquired KSAs.*** Training is only beneficial to the organization when the learned KSAs are not only learned during the training but also applied and maintained on the job [7, 21]. Hence, organizations must prepare the climate to facilitate using the KSAs learned during training [22]. For example, trainees need opportunities to perform [23] because a substantial delay between training and job performance can lead to significant skill decay [24]. Supervisors should also encourage trainees to use their trained skills on the job by providing positive reinforcement (e.g. verbal praise and monetary reward; [25]). Positive reinforcement when applied appropriately (i.e. immediately following behavior) will lead to repetition [26]. Having supervisory support and providing reinforcements sends out a positive message to trainees, which is imperative to the success and effectiveness of training.

## 3 LEARNING DEVELOPMENT

Now that we have an understanding of the science behind designing, developing, implementing, and evaluating a training program, we can discuss some of the possible training strategies. Because employees must implement a variety of information and skills on a

daily basis, it is necessary to possess a variety of training strategies in your arsenal to be able to customize and adapt to all of the different requisite competencies required to perform each task. As technology permeates throughout businesses, more complex skills are required to complete tasks in the work environment; therefore, it is necessary that our training strategies become more complex as well to adjust to the growing changes. Due to the popularity of technology and the growing demand of organizations to use teams to perform complex tasks, we will elaborate on simulation-based training (SBT) and games as a learning development strategy. Moreover, because organizations often lack the time to implement a formal training program, we will discuss an informal technique called *on-the-job training* (OJT).

### 3.1 Simulation-based Training

SBT is an interactive, practice-based instructional strategy which provides opportunities for trainees to develop the requisite competencies and enhance their expertise through scenarios and feedback [12]. The scenarios serve as the "curriculum". In other words, the learning objectives derived from the training needs analysis are embedded within the scenarios. The SBT "life cycle" consists of a number of interrelated and critical stages and each step is fundamental to the next [27]. The first step is to verify trainees' existing skills and their previous performance record. Next, determine the tasks and competencies that will be emphasized during training. As a result of the second step, the training/learning objectives can be established. Upon the completion of all of these steps, scenarios can be created. The scenarios are scripted and designed to elicit the requisite competencies by incorporating "trigger" events. Afterwards, performance measures must be developed to assess the effectiveness of the training. Then, the performance data is collected and compared to the existing, previous data. The collected data serves as the foundation and guide for providing feedback to the trainees. Lastly, all of the information can then be used to make any adjustments or modifications to the training program.

SBT can be an optimal instructional strategy because it has many benefits. First, SBT mimics the job environment; therefore, it is very realistic, which makes transferring skills to the job easier [28]. In addition, SBT allows an organization to explore training with a variety of scenarios, which facilitates and accelerates expertise [2]. Third, SBT is interactive and engaging. Being engrossed in training is influential to motivation, and researchers have shown that motivation enhances learning [29]. Last, SBT when utilizing carefully crafted scenarios and measures, can facilitate the diagnosis of performance.

### 3.2 Games

Recently, the military along with other organizations have started to use games as instructional tools to acquire knowledge, skills, and attitudes applicable in the work place as well as other settings. Games can be defined as "a set of activities involving one or more players. It has goals, constraints, payoffs, and consequences. A game is rule-guided and artificial in some respects. Finally, a game involves some aspect of competition, even if that competition is with oneself" [30], p. 159. Although the definition of what constitutes

a game is being debated by researchers because they are available in a wide array of formats (e.g. board games, console-based games PC-based games), there is agreement that games provide educational benefits to learning as a training tool. For example, Vogel and colleagues [31] conducted a meta-analysis and found that cognitive and attitudinal abilities were enhanced in participants when they used interactive games and simulations as opposed to traditional instruction methods.

Games have become a popular instructional tool because they not only benefit the learner but are also advantageous for the developers and instructors. Users benefit by "playing" because the skills necessary to accomplish the goals within the game are applicable to other situations. Furthermore, games elicit motivation in users because they are interactive, fun, and engaging [32]. Developers and instructors benefit from leveraging games as well because they are modifiable (i.e. instructional features can be added in some cases with ease) and a cost-effective approach to learning.

### 3.3 On-the-Job Training

Frequently, in HS and in other organizations there is not sufficient time or resources to implement a formal training because new policies and procedures must be integrated immediately; therefore, OJT is one possible solution. OJT is "job instruction occurring in the work setting and during the work" [33] p.3. Because it occurs on the job and does not require instructors or trainees to leave the job site, it is a very economical alternative. Moreover, occurring in the actual work environment has the added benefit of facilitating training transfer since trainees can see that the training is relevant and applicable to completing the job tasks. Therefore, the KSAs have more significance.

However, in order to reap the benefits of such an applicable, customizable, low cost alternative, OJT needs to be executed correctly. All OJT is not created equal. Practitioners need to abide by several learning principles in order to optimize the effectiveness of OJT. First, as with any other training, the top of the organization and its leaders needs to support the OJT. For example, as noted, earlier organizations can show support through rewards and incentive programs [34]. Second, OJT facilitators also need to be included throughout the process [35]. OJT facilitators need to be involved in designing and developing the program as well as being trained on instructional techniques (e.g. coaching and mentoring). Often, facilitators are knowledgeable in their field; however, they lack the expertise to effectively teach others. Once the organization and the training facilitators are supportive, the trainees must be prepared. Preparatory information about the content of the upcoming OJT will not only establish the appropriate expectations, it will also foster motivation [10]. Third, it is absolutely critical that the OJT be structured and guided to be optimally effective. A structured OJT ensures standardizations reducing discrepancies in the way training is delivered and executed. OJT is a useful strategy when guided by the science of learning as well.

## 4 CONCLUDING REMARKS

Regardless of the strategy (e.g. SBT, games, and OJT) being implemented, training must follow the basic principles to ensure its success [6]. It must be developed

systematically because all of the facets are interrelated, serving as the foundation for the next component—assessing the needs of the organization, identifying the necessary resources, developing the practice scenarios, evaluating the effectiveness, and providing feedback to make adjustments. But to ensure that trainees learn the requisite KSAs, the design, delivery, implementation, and evaluation of the training must be provided with the science of learning and training.

## REFERENCES


1. BBC News (2008). *Who is Richard Reid?* (2001, December 28). Retrieved January 14, from http://news.bbc.co.uk/1/hi/uk/1731568.stm.
2. Salas, E., Priest, H. A., Wilson, K. A., and Burke, C. S. (2006). Scenario-based training: Improving military mission performance and adaptability. In *Minds in the Military: The Psychology of Serving in Peace and Conflict*, Vol. 2, *Operational Stress*, A. B. Adler, C. A. Castro, and T. W. Britt, Eds. Praeger Security International, Westport, CT, pp. 32–53.
3. Salas, E., and Cannon-Bowers, J. A. (2000a). Design training systematically. In *The Blackwell Handbook of Principles of Organizational Behavior*, E. A. Locke, Ed. Blackwell Publisher Ltd, Malden, MA, pp. 43–59.
4. Goldstein, I. L. (1993). *Training in Organizations*, 3rd ed., Brooks, Pacific Grove, CA.
5. Goldstein, I. L., and Ford, J. K. (2002). *Training in Organizations: Needs Assessment, Development, and Evaluation*, 4th ed., Wadsworth, Belmont, CA.
6. Salas, E., and Cannon-Bowers, J. A. (2000b). The anatomy of team training. In *Training and Retraining: A Handbook for Business, Industry, Government, and the Military*, S. Tobias, and J. D. Fletcher, Eds. MacMillan Reference, New York, pp. 312–335.
7. Salas, E., and Cannon-Bowers, J. A. (2001). The science of training: A decade of progress. *Annu. Rev. Psychol.* **52**, 471–499.
8. Quinones, M. A. (1995). Pretraining context effects: training assignment as feedback. *J. Appl. Psychol.* **80**, 226–238.
9. Quinones, M. A. (1997). Contextual influencing on training effectiveness. In *Training for a Rapidly Changing Workplace: Applications of Psychological Research*, M. A. Quinones, and A. Ehrenstein, Eds. American Psychological Association, Washington, DC, pp. 177–200.
10. Cannon-Bowers, J. A., Rhodenizer, L., Salas, E., and Bowers, C. A. (1998). A framework for understanding pre-practice conditions and their impact on learning. *Pers. Psychol.* **51**, 291–320.
11. Cannon-Bowers, J. A., Burns, J. J., Salas, E., and Pruitt, J. S. (1998). Advanced technology in scenario-based training. In *Making Decisions Under Stress: Implications for Individual and Team Training*, J. A. Cannon-Bowers, and E. Salas, Eds. American Psychological Association, Washington, D.C., pp. 365–374.
12. Fowlkes, J., Dwyer, D. J., Oser, R. L., and Salas, E. (1998). Event-based approach to training (EBAT). *Int. J. Aviat. Psychol.* **8**(3), 209–221.
13. Salas, E., and Cannon-Bowers, J. A. (1997). Methods, tools, and strategies for team training. In *Training for a Rapidly Changing Workplace: Applications of Psychological Research*, M. A. Quinones, and A. Ehrenstein, Eds. APA, Washington, DC, pp. 249–280.
14. Salas, E., Wilson, K. A., Priest, H. A., and Guthrie, J. W. (2006). Training in organizations: the design, delivery and evaluation of training systems. In *Handbook of Human Factors and Ergonomics*, 3rd ed., G. Salvendy, Ed. John Wiley & Sons, Hoboken, NJ, pp. 472–512.
15. Fowlkes, J. E., and Burke, C. S. (2005). Targeted acceptable responses to generated events or tasks (TARGETs). In *Handbook of Human Factors and Ergonomics Methods*, N. Stanton, H. Hendrick, S. Konz, K. Parsons, and E. Salas, Eds. Taylor & Francis, London, pp. 53-1–53-6.

16. Brannick, M. T., Salas, E., and Prince, C., Eds. (1997). *Team Performance Assessment and Measurement: Theory, Methods, and Applications*, Lawrence Erlbaum Associates, Mahwah, NJ.
17. Clark, D. (2000). *Introduction to Instructional System Design*, Retrieved January 17, 2008 from http://www.nwlink.com/~donclark/hrd/sat1.html#model.
18. Kirkpatrick, D. L. (1976). Evaluation of training. In *Training and Development Handbook: A Guide to Human Resource Development*, 2nd Ed., R. L. Craig, Ed. McGraw-Hill, New York, pp. 1–26.
19. Howard, S. K., Gaba, D. M., Fish, K. J., Yang, G., and Sarnquist, F. H. (1992). Anesthesia crisis resource management training: Teaching anesthesiologists to handle critical incidents. *Aviat. Space Environ. Med.* **63**, 763–770.
20. Salas, E., Wilson, K. A., Burke, C. S., and Wightman, D. (2006). Does CRM training work? An update, extension, and some critical needs. *Hum. Factors* **48**(2), 392–412.
21. Balwin, T. T., and Ford, J. K. (1988). Transfer of training: a review and directions for future research. *Pers. Psychol.* **41**, 63–105.
22. Tracey, B. J., Tannenbaum, S. I., and Kavanagh, M. J. (1995). Applying trained skills on the job: the importance of the work environment. *J. Appl. Psychol.* **80**, 239–252.
23. Ford, J. K., Quinones, M. A., Sego, D. J., and Sorra, J. S. (1992). Factors affecting the opportunity to perform trained tasks on the job. *Pers. Psychol.* **45**, 511–527.
24. Arthur, W., Bennett, W., Stanush, P. L., and McNelly, T. L. (1998). Factors that influence skill decay and retention: a quantitative review and analysis. *Hum. Perform.* **11**, 79–86.
25. Rouiller, J. Z., and Goldstein, I. L. (1993). The relationship between organizational transfer climate and positive transfer of training. *Hum. Resour. Dev. Q.* **4**, 377–390.
26. McConnell, C. R. (2005). Motivating your employees and yourself. *Health Care Manag. (Frederick)* **24**(3), 284–292.
27. Salas, E., Wilson, K. A., Burke, C. S., and Priest, H. A. (2005). Using simulation-based training to improve patient safety: What does it take? *Jt. Comm. J. Qual. Patient Saf.* **31**(7), 363–371.
28. Oser, R. L., Cannon-Bowers, J. A., Salas, E., and Dwyer, D. J. (1999). Enhancing human performance in technology-rich environments: Guidelines for scenario-based training. In *Human/technology Interaction in Complex Systems*, E. Salas, Ed. JAI Press, Greenwich, CT, Vol. 9, pp. 175–202.
29. Colquitt, J. A., LePine, J. A., and Noe, R. A. (2000). Toward an integrative theory of training motivation: A meta–analytic path analysis of 20 years of research. *J. Appl. Psychol.* **85**(5), 678–707.
30. Dempsey, J. V., Haynes, L. L., Lucassen, B. A., and Casey, M. S. (2002). Forty simple computer games and what they could mean to educators. *Simul. Gaming* **33**(2), 157–168.
31. Vogel, J. J., Vogel, D. S., Cannon–Bowers, J., Bowers, C. A., Muse, K., and Wright, M. (2006). Computer gaming and interactive simulations for learning: A meta–analysis. *J. Educ. Comput. Res.* **34**(3), 229–243.
32. Garris, R., Ahlers, R., and Driskell, J. E. (2002). Games, motivation and learning: a research and practice model. *Simul. Gaming* **33**(4), 441–467.
33. Rothwell, W. J., and Kazanas, H. C. (1994). *Improving on-the-job Training: Hw to Establish and Operate a Comprehensive OJT Program*, Jossey–Bass, San Francisco.
34. Levine, C. I. (1996). Unraveling five myths of OJT. *Techn. Skills Train.* **7**, 14–17.
35. Derouin, R. E., Parrish, T. J., and Salas, E. (2005). On-the-job training: Tips for ensuring success. *Ergon. Des.* **13**(2), 23–26.

# TRAINING FOR INDIVIDUAL DIFFERENCES IN LIE DETECTION ABILITY

MAUREEN O' SULLIVAN
*University of San Francisco, San Francisco, California*
MARK G. FRANK
*University of Buffalo, State University of New York, Buffalo, New York*
CAROLYN M. HURLEY
*University of Buffalo, State University of New York, Buffalo, New York*

## 1 INTRODUCTION

Catching terrorists is a multilayered process. Although technological sensors are both rapid and reliable, as in the use of thermographic or facial and body analysis programs (see Human Behavior and Deception Detection), there are points in the process of assessing deception where only a human lie detector can be used. This may occur after the automated system shows a "hit" on an individual, which subjects him or her to further scrutiny, or in other security domains where access to technology is limited or nonexistent. Given these situations, it is important to determine who should interview such potential terrorists. Should we train all security personnel to improve their basic abilities? Or, should we select those most amenable to training, because of their motivation, skill, or other characteristics? Or, should we select already expert lie catchers; and if we do, how do we find them?

The literature on how to increase lie detection accuracy through training has been sparse, although an increasing number of scientists are addressing this issue. This overview will enumerate some of the factors involved in designing a good training study and examine the current state of knowledge concerning training for improved lie detection accuracy.

## 2 INDIVIDUAL DIFFERENCES IN LIE DETECTION ABILITY

Over the last 50 years, a general presumption has been that lie detection accuracy is a particular ability or cognitive skill [1] that might be an aspect of social-emotional intelligence [2]. This widely held belief implies something approximating a normal distribution of lie detection accuracy scores, with most scores in the average range and a few being very high or very low. However, a recent study questioned this assumption. A 2008 meta-analysis [3] of 247 lie detection accuracy samples concluded that although there was reliable evidence that people vary in the ease with which their lies can be detected,

there is no evidence of reliable variance in the ability to detect deception. This rather controversial conclusion was criticized on a variety of grounds [4, 5]: most of the studies used college students, not professional lie catchers; the statistical model did not satisfy the classical test theory on which it was based; the metric used was standard deviations without reference to means, a highly misleading unit of measurement; and the authors ignored a substantial literature demonstrating convergent validity between lie detection accuracy and various social and psychological variables. Furthermore, in the last several years, as researchers use lie scenarios more appropriate to security personnel in their research, the number of reports in which highly accurate groups have been identified has increased [6].

The study of highly accurate individual lie detectors has been less common [7–9]. These studies suggest, however, that practice and motivation to detect deception are important variables. Moreover, expert lie detectors are more accurate with lies relevant to their profession [5, 9, 10]. Frank and Hurley [10] found that among law enforcement personnel, accuracy was greater for those with more experience in different domains of law enforcement. Homicide investigators, for example, were more accurate than fraud investigators who were more accurate than patrolmen walking a beat. Similarly, O'Sullivan [11] found, as predicted, that college administrators were more accurate in detecting the lies of college students than other non-faculty college personnel. In addition to supporting the view that experience makes a difference in lie detection accuracy, some of these studies support the view that experience with a particular kind of lie is important in lie detection. By extension, training to enhance lie detection accuracy should emphasize the particular lie of interest. Evidence relating to this point is reviewed below.

## 3 HOW EFFECTIVE IS TRAINING TO INCREASE LIE DETECTION ACCURACY?

In a review of 11 lie detection training studies completed between 1987 and 1999, Frank and Feeley [12] reported a small, but significant, positive effect of training. Their methodological review suggested that the literature was hindered by several weaknesses in the research designs of most of the studies performed. They emphasized the importance of several variables in designing training programs and evaluating them: (i) the *relevance* of the lie to the lie detectors being trained. Training college students to detect lies about friends told by other college students may not generalize to training law enforcement personnel about lies about past or present crimes; (ii) whether the lie scenario uses *high stakes* lies—lies that involve strong rewards and punishments for successful and unsuccessful deceiving—may affect both lie detection accuracy, and training conducted with them. A recent meta-analysis [6] suggests that even professional lie catchers, such as police personnel, will not be accurate in detecting low stakes lies, lies that are not important to the liars' or the truth tellers' self-identity, or lies without significant rewards or punishments. Their meta-analysis found that the average lie detection accuracy of police tested with high stakes lies was significantly higher than that of police tested with low stakes lies; (iii) in many studies, *training* consists of a brief, written description of potential cues to deception with no actual examples of the behaviors, no feedback, and no practice with similar or related kinds of behavior. Adequate training needs practice, feedback, and exemplars similar to the materials; (iv) basic experimental protocol should be followed, ideally, through the use of randomly determined experimental (trained) and control (untrained) groups with pre- and post-*testing* of both the experimental and

the control groups. Different liars and truth tellers should be included in the pre- and post-testing measures. And, of course, the difficulty of the two measures should be calibrated for equivalence; (v) assuming that a *bona fide* training effect is found (based on a standard experimental protocol), and that training with one kind of lie has been shown to increase accuracy with that lie, another issue is whether the training is lie-specific or *generalizes* to increased accuracy with other kinds of lies; (vi) in addition to generalization to other kinds of lies (what Frank and Feeley [12] called Situational Generality), a related issue is *time generality*. How long does such increased accuracy last? Is it a permanent learning effect? Or one that dissipates outside of the training environment?

These six factors are *sine qua nons* for lie detection training research. In a more recent methodological review, Frank [13] expanded the discussion of these topics and included many suggestions about ways in which to improve lie detection accuracy studies. In the present overview, however, we use the Frank and Feeley [12] paradigm to examine the nine lie detection training studies that were completed from 2000 to 2007. Table 1 summarizes the strengths and defects of these studies in the light of the Frank and Feeley paradigm. In conclusion, we will discuss the importance of individual differences in designing training programs, over and above the variation in individual lie detection accuracy.

As Table 1 shows, of the nine training studies, three found no significant training effect; in one of these studies the lie scenario may have been irrelevant to the test takers [14]. In the others, the training may have been inadequate [18, 20]. Among 16 different groups tested, nine (Table 1, groups 4–8, 12,13, 15, 16) showed a significant lie detection accuracy increase, ranging from 2% to 37% (median increase = 20%).

## 4 RELEVANCE

Frank and Feeley [12] argued that training should be on lies relevant to the trainees. We agree, but in a recent publication [6] we refined this argument. It may be even more important that the lie scenario used for training contains the kinds of behaviors, both verbal and non-verbal, that provide clues to deception than that the lie superficially looks like a lie of interest. This distinction is what test psychologists call face validity versus construct validity and what experimental psychologists term mundane realism versus experimental realism. A lie scenario may seem relevant to a law enforcement lie detection situation because it shows a felon being interviewed by a police officer (face validity, mundane realism). But if the lie is about a topic of no importance to the felon, the emotional and cognitive aspects of a high stakes lie will not be present. Conversely, a college student discussing a strongly held belief, who will receive substantial rewards if he tells the truth successfully or lies successfully and who will be punished if he is unsuccessful, may better simulate the behaviors seen in a law enforcement interview (construct validity, experimental realism). So while the construct validity or experimental realism of a scenario is the more important variable, the relevance or interest of the lie to the lie catcher (its face validity or mundane realism) must also be considered. In screening expert lie detectors from several different professional groups including law enforcement personnel and therapists, O'Sullivan [5] found that about one-third of the experts were at least 80% accurate on each of three different lie detection tasks. The remaining two-thirds of the experts obtained 80% on two of the three tests. For this second group, their lowest score was either on a test in which young men lied about

**TABLE 1 Lie Detection Accuracy Training Studies, 2000–2007**

| Group | Study | n | Sample Trained | Accuracy Pre/Post | Relevance of Test | High Stakes of Test | Training Adequacy | Testing Adequacy | Situational Generality | Time Generality |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Akehurst [14] | 26 | Police | Ns | No | No | Yes | Yes | No | No |
| 2 | Akehurst [14] | 14 | Social workers | Ns | No | No | Yes | Yes | No | No |
| 3 | Akehurst [14] | 18 | College | Ns | No | No | Yes | Yes | No | No |
| 4 | Crews [15] | 29 | College | 42/69 | Yes | No | Yes | Yes | No | No |
| 5 | Crews [15] | | College | 44/64 | Yes | No | Yes | Yes | No | No |
| 6 | George [16] | 177 | Air Force | 54/60 | Unknown | Unknown | Yes | Unknown | No | No |
| 7 | George [16] | | Air Force | 47/61 | Unknown | Unknown | Yes | Unknown | No | No |
| 8 | Hartwig [17] | 164 | Police trainees | 56/85[a] | Yes | Perhaps | Yes | Yes | No | No |
| 9 | Levine [18] | 256 | College | Ns | Yes | No | No | No | No | No |
| 10 | Levine [18] | 90 | College | Ns | Yes | No | No | No | No | No |
| 11 | Levine [18] | 96 | College | Ns | Yes | No | No | No | No | No |
| 12 | Levine [18] | 158 | College | 56/58[a] | Yes | No | Yes | No | No | No |
| 13 | O'Sullivan [19] | 78 | College | 57/61 | Yes | Yes | Yes | No | No | No |
| 14 | Porter [20] | 151 | College | Ns | Yes | Yes | No | Yes | No | No |
| 15 | Porter [21] | 20 | Parole officers | 40/77 | No | Yes | Yes | Yes | No | Perhaps |
| 16 | Santarcangelo [22] | 97 | College | 65/69 | Yes | No | Perhaps | Yes | No | No |

*Note*: College: college students; Accuracy: pretest accuracy/post-test accuracy scores for same individuals.
[a]Accuracy for post-test only design: untrained accuracy/trained accuracy scores.

stealing a significant amount of money or a test in which young women lied or told the truth about whether they were watching a gruesome surgical film or a pleasant nature film. Not surprisingly, the lowest of the three scores for therapists was on the crime test; for law enforcement personnel, their lowest score was on the emotion test. This finding was highly significant.

Among recently published lie detection accuracy studies, several meet the criterion of relevance, whether this term is used to refer to importance to the trainees (mundane realism, face validity) or actual validity for the lies that lie catchers need to be accurate on (experimental realism, construct validity). Hartwig [17] tested police officers using a mock theft scenario and allowed the trainees to interview the experimental suspects. Akehurst [14], on the other hand, used test stimuli in which children lied or told the truth about an adult taking a photograph. Since it is unlikely that much arousal happened, whether this scenario had either mundane or experimental realism for the subjects is doubtful. All of the other studies used college students as target liars and truth tellers. Insofar as the trainees were students or therapists, who work with clients in that age group, such materials are probably relevant to them.

## 5 HIGH STAKES LIES

Among the nine training studies published between 2000 and 2007, four used what we consider to be high stakes lies. Porter [20, 21] used a scenario in which targets lied or told the truth about highly emotional events in their personal lives. We consider lies with a strong self-identity aspect to be high stakes. O'Sullivan [19] used a scenario in which both personal identity and a large cash reward were involved. Although the Hartwig study [17] used a sanctioned mock theft scenario which reduces the stakes for the liars and truth tellers, the targets also received a lawyer's letter which may have "bumped up" the stress of the situation. (Three of these four studies achieved a significant learning effect.) The other studies included scenarios in which college students told social lies about friends or lied about whether they had headphones hidden in their pockets. (They had been directed to do so by the experimenter, so little emotional arousal could be expected.)

## 6 TRAINING

Outstanding expertise in lie detection is likely the result of a host of individual difference variables such as interest, extensive and varied life experience, motivation, practice, and feedback with professionally relevant lies that most expert lie detectors seem to share. In addition, there are probably particular kinds of skills such as visual or auditory acuity, pattern recognition and social or emotional memory that vary from expert to expert and that will cause them to be more or less expert on different kinds of lies, depending on their particular subset of skills. So while expert lie detection employs a host of skills, training for lie detection accuracy in a particular course or a particular study might more efficiently proceed by training in a focused skill or set of skills known to be related to lie detection. Many of the recent lie detection studies used this approach, narrowing their focus and evaluating the effectiveness of training with a particular kind of knowledge or subset of cues.

Santarcangelo [22] found that informing trainees about either (i) verbal content cues (plausibility, concreteness, consistency, and clarity which are included in the more extensive Criteria-Based Content Analysis (CBCA) protocol); (ii) nonverbal cues (adaptors, hand gestures, foot and leg movements, and postural shifts) or (iii) vocal cues (response duration, pauses, speech errors, and response latency) resulted in lie detection accuracy greater than a no-cues control group.

Levine [18] conducted a series of studies on how to increase lie detection accuracy that also used mere verbal description of cues. In three of the studies, a lecture describing general behavioral cues comprised one condition. A second condition was a bogus training group in which *incorrect* information about lie detection clues was given to the subjects. The control group received no information about lie detection clues. None of the three studies obtained significant results in the predicted direction. In the fourth study, behavioral cues actually occurring in the stimulus materials were used for the lecture condition. In this condition, a significant result was found between the training lecture (58%) and the control condition (50%). However, the bogus training also resulted in significantly increased training (56%) which was not significantly different from the authentic training condition. Interpretation of this study is complicated by the use of only two different stimulus persons as the target liars and truth tellers. Other researchers are also designing training studies which teach those behavioral cues actually existing in the training and testing materials [15, 23]. For studies using this training method, situational generality (testing on other lie detection tests as well) is particularly important.

Hartwig [17] took a novel approach by training police trainees to adjust the timing of their questions. Rather than assessing the nonverbal behaviors of the liars and truth tellers, actual evidence (eyewitness testimony, fingerprints, etc.) was available and the liars and truth tellers were informed of this during the interview. The Hartwig study found that if interviewers held back knowledge of the evidence until later in the interview, liars were more likely to make inconsistent statements which increased detection accuracy for the interviewers. This training is much more like the kind of interview situation in which law enforcement officers decide the honesty of suspects. Such training, however, may not generalize to interview situations in which no evidence is available.

An unusual feature of deception research, although certainly not new in other kinds of training, is the use of computer programs in lieu of instructor presentation or printed materials. Crews [15] and George [16] demonstrated that there was no difference between a computer-based training program and the same material presented by a human instructor. In both cases, significantly increased accuracy was achieved.

Although most of the studies provided examples of honest and deceptive behaviors for trainees, some did not. Subjects in the Levine [18] and Santarcangelo [22] studies, for example, only received a written sheet of cue information that could be read rather quickly. It is interesting that these studies found a significant, albeit small (4%) increase in accuracy, whereas studies using more lengthy training procedures [15, 17] reported gains in excess of 20%.

## 7 TESTING

(a) *Randomization.* Trainees were randomly assigned in all of the studies. Most of the studies used a pre—post design except those of Hartwig [17] and Levine [18] which utilized a random assignment, post-group comparison design. Random assignment in a post-group-only design assumes that all assigned interviewers or judges are

alike prior to training and that differences afterwards are due to the training alone. A post-test-only design does not completely rule out the possibility that trained and untrained interviewers or judges, even if randomly assigned, were different before the experiment.

(b) *Independence of items in the stimulus materials.* Although most of the lie detection materials used different liars or truth tellers for each "item" some did not. Levine [18], for example, used only two targets, who both lied and told the truth about items on a test. When "items" are not independent, the effect of biases, personal likes and dislikes with particular kinds of people, familiarity with particular kinds of people or particular kinds of behavioral styles can all affect the final scores. These biases may reflect factors other than lie detection accuracy.

(c) *Independence of targets in pre—post designs.* All of the pre- and post studies, except O'Sullivan's [19], used different liars and truth tellers for their pre- and post-tests. Although a control group ameliorates the effect of mere familiarity on increased lie detection accuracy, it is preferable to have different individuals as targets in the pre- and post-test measures and to ensure that the tests are of equivalent difficulty. The Crews study [15] did an especially careful job of determining that their pre- and post tests were equivalent in difficulty, establishing their norms in a pilot study. None of the other studies did this, or if they did, they did not mention it.

(d) *Numbers of targets.* Except for Levine [18] who used only two test subjects, most of the studies used 6 to 12 subjects for the pre-test and/or post-test measures.

## 8 SITUATIONAL GENERALITY

All of the studies used a single kind of lie so the generalizability of training for lie detection accuracy is unknown. Given that some of the studies with the greatest increase in accuracy taught and emphasized the cues that were actually contained in the materials [15, 16], the issue of situational or lie generality is an important one.

## 9 TIME GENERALITY

None of the studies reviewed examined the temporal stability of any gain in lie detection accuracy, so we have no way of knowing whether gains in lie detection accuracy survive the time span of the training course. Researchers are aware of this issue, however. Porter [21] spread the training over five weeks, and found a highly significant increase in detection accuracy. Whether this gain would last longer than five weeks, however, is unknown. Marett [24] was specifically interested in the effect of lie detection history (training over time) on final accuracy, but the small number of subjects and items did not allow them to reach any conclusions. (This study is not reviewed since no accuracy means were reported.)

## 10 INDIVIDUAL DIFFERENCES RELATED TO LIE DETECTION ACCURACY

In training to increase lie detection accuracy, a variety of individual difference abilities need to be considered. The already existing ability of the trainees is one that has

often been overlooked. It seems reasonable, however, that training which provides new information to mediocre lie detectors, may be superfluous to expert ones. And providing specialized training, in verbal content analysis or facial expression recognition or other nonverbal cues, might be more advantageous for those already at an average or above average lie detection accuracy level. No research exists which examines the role of pre-existing lie detection accuracy on the efficacy of different lie detection training paradigms.

In our work with expert lie detectors who have been trained in facial expression recognition, several of them have reported a disruption of their ability to assess truthfulness in the months immediately following the training. With practice, however, according to their self-reports, they were able to incorporate the new information into their skill set. Kohnken [25] and Akehurst [14] also described reports from police trainees that they needed more time to incorporate the new information provided. (In these studies it was verbal content training rather than facial expression recognition.) A difficulty in examining this hypothesis (that more expert lie detectors may have an initial disruption effect, resulting in a decrement in lie detection accuracy) may occur due to the ceiling effect or regression to the mean for the lucky guessers in the first testing. If trainees are already highly accurate prior to training (70% or better), there is little room for improvement as measured by most existing lie detection accuracy measures. Many lie detection accuracy tests are relatively brief; the median number of items is ten. Clearly, new tests containing more items of greater difficulty are necessary. The issue of item difficulty is also an important one. Many items in existing lie detection measures are difficult because the lies are trivial and there are no emotional and/or cognitive clues to discern. Item difficulty should be based on subtle cues that are present although, difficult to distinguish, or should reflect the kinds of personality types (outgoing, friendly) that are particularly difficult for American judges to perceive as liars.

Other individual difference variables that have been largely overlooked in studies of lie detection accuracy training are the intelligence and cognitive abilities of the lie detector. O'Sullivan [26] demonstrated that the fundamental attribution error was negatively related with accurate detection of liars. Whether such cognitive biases can be corrected through training has not been examined. Although many people seem to believe that lie detection is a natural ability unrelated to education or training, O'Sullivan noted [27] that more than half of her 50 expert lie detectors have advanced degrees and all have at least a two year associates degree. The interpretation of the many cognitive and emotional cues that occur while lying and telling the truth may take a superior baseline level of intelligence to decipher. This hypothesis has also not been examined. On the other hand, Ask and Granhag [28] found no relationship between cognitive or personality variables such as need for closure, attributional complexity, and absorption. The lie scenarios they used, however, may not have provided sufficient score variance to examine their hypotheses adequately.

Many expert lie detectors seem to have an ongoing life commitment to seeking the truth [5]. This kind of commitment and practice cannot be taught in a single training program, which suggests that selecting already accurate lie detectors might be a more sensible approach to use when staffing personnel to perform lie detection interviews. This option, however, may be difficult to implement given the relative rarity of expert lie detectors (from 1 per thousand in some professional groups to 20% in others [5]) and the personnel restrictions in some agencies.

In addition to individual differences in lie detection accuracy as a factor to be considered in designing and implementing lie detection accuracy training courses, the role of other individual difference factors needs to be considered. Deception researchers [9] have noted the extraordinary motivation of expert lie detectors to know the truth. Porter [29] attempted to examine motivation by randomly assigning subjects to one of two levels of motivation to succeed at a lie detection task. This motivation manipulation had no impact on consequent lie detection accuracy. An experimentally manipulated motivation to detect deception, however, may not be a sufficient analog for the life-long commitment to discern the truth in one's profession and one's life that some expert lie detectors show.

To date there is mounting evidence that certain law enforcement personnel groups [6, 30, 31] and individuals [5, 7] are accurate at least with certain kinds of lies. There is replicated evidence that groups of forensic specialists (psychologists and psychiatrists), federal judges [31], and dispute mediators [5] are also significantly above chance in their ability to discern the truth. In all of these studies, comparison groups, usually of college students, have average accuracies at the chance level on the tests used. This provides some support for the view that the lie detection tests are not easy, which rules out one explanation for their high accuracy.

While commitment to lie detection is an aspect of some expert lie catcher's professional lives, O'Sullivan [19] found that even among college students, concern for honesty was significantly related to lie detection accuracy. Students who reported rarely lying to friends obtained higher accuracy on a lie detection measure than students who lied to friends frequently. In this same study, a high rating for honesty as a value when compared with other values (such as a comfortable life) also distinguished more and less accurate lie detectors.

Given the importance of emotional clues in detecting deception, it is not surprising that a number of studies have reported significant correlations between emotional recognition ability and lie detection accuracy. Warren, Schertler, and Bull [32], for example, demonstrated that accuracy at recognizing subtle facial expressions using the SETT (Subtle Expression Training Tool [33]) was positively related to accuracy in detecting emotional lies, but not nonemotional ones. (This study underscores the need for situational generality of lie scenarios as discussed earlier.) Ekman and O'Sullivan [30], Frank and Ekman [34], and Frank and Hurley [10] all found a significant relationship between micro-expression detection accuracy and lie detection accuracy using precursors of the Micro-Expression Training Tool (METT) [35]. Frank [36] also found that being trained on micro-expressions significantly improved detecting emotions that occurred while lying.

Many IQ tests are highly saturated with verbal content, so it is likely that the ability to apply one type of verbal system (e.g., CBCA) in improving lie detection accuracy may be related to verbal intelligence. Vrij [37] found individual differences in the ability to learn CBCA in order to lie or tell the truth more effectively. While the ability to learn CBCA may have a cognitive component, the study also found that ability to use CBCA in truth and lie performance was related to social anxiety.

Porter's [29] report of a significant correlation between handedness and lie detection accuracy (left-handed lie catchers being superior) also suggests a biologically based individual difference that should be considered in lie detection accuracy programs. Etcoff and her colleagues [38] also reported a similar right brain advantage in lie detection.

Other individual difference variables of interest have included gender and personality variables such as social skill and Machiavellianism. For all of these variables, conclusions are difficult to draw because of the widely varying adequacy of the lie detection scenarios used, or the lack of variance in lie detection accuracy of some of the subjects. For example, in one study [39] which reported an interaction effect between gender and increased accuracy with training, the differing mean accuracies of the two genders at the start of the study compromises this conclusion. Before training, average accuracy for males was 47% which increased to 70% after training. For females, pretraining accuracy was 68% which decreased to 62% after training. Pretraining performance for females was significantly higher than for males, giving females less headroom for improvement. Even though the males' accuracy increased significantly while the females did not, the difference in their final accuracy levels was not significant. This effect might reflect a room-for-improvement phenomenon rather than a gender one. Some low-scoring females might have shown some improvement. The confounding of base accuracy level and gender would need to be clarified before conclusions can be drawn about gender effects. Over all, no consistent gender superiority in lie detection accuracy or in training effectiveness has been demonstrated.

Training studies with relevant tasks, focused training programs, and reliable test materials known to contain behavioral clues or other evidence relevant to lie detection, have resulted in a growing body of research demonstrating that lie detection is difficult for most people, but that improvement is possible with well-honed training programs.

Selecting the best detectors within an organization may be more cost-effective, but it too is fraught with problems. The tasks used to determine who goes forward need to mirror the structural features of the scenarios to which these personnel will apply their skills. And, ideally it would be useful to develop some metric as to how well they do in the real world, compared to those not selected. For example, we can consider criteria such as how much contraband is confiscated, or how many cases go to trial and result in a conviction, or other goals specific to the agency may be useful. This would require a new way of thinking about security, but it may violate assumptions about equal treatment for all agency personnel.

## 11 CONCLUSION

We end on an optimistic note. Increasingly, researchers are identifying highly accurate lie catchers. This increased range of lie detection accuracy can provide a proving ground for developing lie-specific training. Research on how expert lie detectors do what they do can suggest materials to be included in lie detection courses. Researchers have also become increasingly sophisticated about the need for experimental validity in their work. They have also become more sophisticated about the value of training on one particular skill or clue domain at a time (e.g., CBCA, METT). We believe the tools of the scientist can be successfully applied to real-world security settings. But more work is needed in order to calibrate the cost/benefit ratio because so much of the science is not directly relevant to security personnel. We see this as a call for increased cooperation between scientists who are sympathetic to the pressures on security personnel and practitioners who desire scientific help in their professions. Once we achieve that combination of forces, we can move this issue forward to identify the optimal way to deploy people in the lie detection process.

## REFERENCES


1. Ekman, P. (2001). *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*. W. W. Norton & Co, New York.
2. O'Sullivan, M. (2005). Emotional intelligence and detecting deception. Why most people can't "read" others, but a few can. In *Applications of Nonverbal Communication*, R. E. Riggio, and R. S. Feldman, Eds. Erlbaum, Mahwah, NJ, pp. 215–253.
3. Bond, C. F. Jr., and DePaulo, B. M. (2008). Individual differences in judging deception: accuracy and bias. *Psychol. Bull.* **134**(4), 501–503. DOI: 10.1037/0033-2909.134.4.477.
4. Pigott, T. D., and Wu, M. (2008). Methodological issues in meta-analyzing standard deviations: comment on Bond and DePaulo (2008). *Psychol. Bull.* **134**(4), 498–500. DOI: 10.1037/0033-2909.134.4.498.
5. O'Sullivan, M. (2008). Home runs and humbugs: comment on Bond and DePaulo (2008). *Psychol. Bull.* **134**(4), 493–497. DOI: 10.1037/0033-2909.134.4.493.
6. O'Sullivan, M., Frank, M. G., Hurley, C. M., and Tiwana, J. Police lie detection accuracy: the effect of lie scenario. *Law Hum. Behav.*, In press.
7. Bond, G. A. (2008). Deception detection expertise. *Law Hum. Behav.* **32**(4), 339–351. DOI: 10.1007/s10979-007-9110-z.
8. O'Sullivan, M. (2007). Unicorns or Tiger Woods: are lie detection experts myths or rarities? A response to On lie detection 'Wizards' by Bond and Uysal. *Law Hum. Behav.* **31**(1), 117–123. DOI: 10.1007/s10979-006-9058-4.
9. O'Sullivan, M., and Ekman, P. (2004). The wizards of deception detection. In *The Detection of Deception in Forensic Contexts*, P. A. Granhag, and L. Stromwell, Eds. Cambridge University Press, Cambridge, pp. 269–286.
10. Frank, M. G., and Hurley, C. M. (2009). *Detection Deception and Emotion by Police Officers*. Manuscript in preparation.
11. O'Sullivan, M. (2008). Lie detection and aging. *Annual Conference Society for Personality and Social Psychology. Albuquerque, NM*.
12. Frank, M. G., and Feeley, T. H. (2003). To catch a liar: challenges for research in lie detection training. *J. Appl. Commun. Res.* **31**(1), 58–75.
13. Frank, M. G. (2005). Research methods in detecting deception research. In *Handbook of Nonverbal Behavior Research*, J. A. Harrigan, K. R. Scherer, and R. Rosenthal, Eds. Oxford University Press, New York, pp. 341–368.
14. Akehurst, L., Bull, R., Vrij, A., and Kohnken, G. (2004). The effects of training professional groups and lay persons to use criteria-based content analysis to detect deception. *Appl. Cogn. Psychol.* **18**(7), 877–891. DOI: 10.1002/acp.1057.
15. Crews, J. M., Cao, J., Lin, M., Nunamaker, J. F. Jr., and Burgoon, J. K. (2007). A comparison of instructor-led vs. web-based training for detecting deception. *J. STEM Educ.* **8**(1/2), 31–40.
16. George, J. F., Biros, D. P., Adkins, M., Burgoon, J. K., and Nunamaker, J. F. Jr. (2004). Testing various modes of computer-based training for deception detection. *Proc. Conf. ISI.* **3073**, 411–417.
17. Hartwig, M., Granhag, P. A., Stromwall, L. A., and Kronkvist, O. (2006). Strategic use of evidence during police interviews: when training to detect deception works. *Law Hum. Behav.* **30**(5), 603–619. DOI: 10.1007/s10979-006-9053-9.
18. Levine, T. R., Feeley, T. H., McCornack, S. A., Hughes, M., and Harms, C. M. (2005). Testing the effects of nonverbal behavior training on accuracy in deception detection with the inclusion of a bogus training control group. *West. J. Commun.* **69**(3), 203–217. DOI: 10.1080/10570310500202355.

19. O'Sullivan, M. (2003). Learning to detect deception. *Annual Conference of the Western Psychological Association. Vancouver, BC*.
20. Porter, S., McCabe, S., Woodworth, M., and Peace, K. A. (2007). 'Genius is 1% inspiration and 99% perspiration' ... or is it? An investigation of the impact of motivation and feedback on deception detection. *Leg. Criminol. Psychol.* **12**(2), 297–309. DOI: 10.1348/135532506X143958.
21. Porter, S., Woodworth, M., and Birt, A. R. (2000). Truth, lies, and videotape: an investigation of the ability of federal parole officers to detect deception. *Law Hum. Behav.* **24**(6), 643–658. DOI: 10.1023/A:1005500219657.
22. Santarcangelo, M., Cribbie, R. A., and Hubbard, A. S. (2004). Improving accuracy of veracity judgment through cue training. *Percept. Motor Skill.* **98**(3), 1039–1048.
23. Cao, J., Lin, M., Deokar, A., Burgoon, J. K., Crews, J. M., and Adkins, M. (2004). Computer-based training for deception detection: What users want? *Proc. Conf. ISI.* **3073**, 163–175.
24. Marett, K., Biros, D. P., and Knode, M. L. (2004). Self-efficacy, training effectiveness, and deception detection: a longitudinal study of lie detection training. *Proc. Conf. ISI.* **3073**, 187–200.
25. Kohnken, G. (1987). Training police officers to detect deceptive eyewitness statements: Does it work? *Soc. Behav.* **2**(1), 1–17.
26. O'Sullivan, M. (2003). The fundamental attribution error in detecting deception: the boy-who-cried-wolf effect. *Pers. Soc. Psychol. Bull.* **29**(10), 1316–1327. DOI: 10.1177/0146167203254610.
27. O'Sullivan, M. (2009). Are there any "natural" lie detectors? *Psychol. Today.* Available at http://blogs.psychologytoday.com/blog/deception/200903/are-there-any-natural-lie-detec1tors.
28. Ask, K., and Granhag, P. A. (2003). Individual determinants of deception detection performance: Need for closure, attribution complexity and absorption. *Goteborg Psychol. Rep.* **1**(33), 1–13.
29. Porter, S., Campbell, M. A., Stapleton, J., and Birt, A. R. (2002). The influence of judge, target, and stimulus characteristics on the accuracy of detecting deceit. *Can. J. Behav. Sci.* **34**(3), 172–185. DOI: 10.1037/h0087170.
30. Ekman, P., and O'Sullivan, M. (1991). Who can catch a liar? *Am. Psychol.* **46**(9), 189–204.
31. Ekman, P., O'Sullivan, M., and Frank, M. G. (1999). A few can catch a liar. *Psychol. Sci.* **10**(3), 263–266.
32. Warren, G., Schertler, E., and Bull, P. (2009). Detecting deception from emotional and unemotional cues. *J. Nonverbal Behav.* **33**(1), 59–69. DOI: 10.1007/s10919-008-0057-7.
33. Ekman, P., and Matsumoto, D. (2003). *Subtle Expression Training Tool*.
34. Frank, M. G., and Ekman, P. (1997). The ability to detect deceit generalizes across different types of high-stake lies. *J. Pers. Soc. Psychol.* **72**(6), 1429–1439.
35. Ekman, P., Matsumoto, D. M., and Frank, M. G. (2003). *Micro Expression Training Tool v1*.
36. Frank, M. G., Matsumoto, D. M., Ekman, P., Kang, S., and Kurylo, A. (2009). *Improving the Ability to Recognize Micro-expressions of Emotion*. Manuscript in preparation.
37. Vrij, A., Akehurst, L., Soukara, S., and Bull, R. (2002). Will the truth come out? The effect of deception, age, status, coaching, and social skills on CBCA scores. *Law Hum. Behav.* **26**(3), 261–283. DOI: 10.1023/A:1015313120905.
38. Etcoff, N. L., Ekman, P., Magee, J. J., and Frank, M. G. (2000). Lie detection and language comprehension. *Nature* **405**(6783), 139. DOI: 10.1038/35012129.
39. deTurck, M. A. (1991). Training observers to detect spontaneous deception: the effects of gender. *Commun. Rep.* **4**(2), 79–89.

**FURTHER READING**

Ekman, P. (2003). *Emotions Revealed*. Henry Holt, New York.

Harrington, B., Ed. (2009). *Deception: From Ancient Empires to Internet Dating*. Stanford University Press, Stanford, CA.

Lindsay, R. C. L., Ross, D. F., Read, J. D., and Toglia, M. P., Eds. (2007). *The Handbook of Eyewitness Psychology Vol I Memory for People*. Lawrence Erlbaum, Mahwah, NJ.

Toglia, M. P., Read, J. D., Ross, D. F, and Lindsay, R. C. L., Eds. (2007). *The Handbook of Eyewitness Psychology Vol I Memory for Events*. Lawrence Erlbaum, Mahwah, NJ.

# DETERRENCE: AN EMPIRICAL PSYCHOLOGICAL MODEL

ROBERT W. ANTHONY

*Institute for Defense Analyses, Alexandria, Virginia*

## 1 INTRODUCTION

Although deterrence has not led to a strategic victory to date against the entire loosely knit network of cocaine traffickers. However, it has shut down nearly all direct smuggler flights into the United States [1, 2], eliminated Peru as a major cocaine producing country [2, 3], and recently closed down nearly all Caribbean go-fast boat traffic. Section 3 recounts how data obtained from these various success stories facilitated the derivation and calibration of an unexpectedly simple mathematical function representing the psychology of deterrence [1, 3]. It goes on to explain how these tactical victories teach several practical lessons and reveal operational dilemmas. To apply these results to terrorism, Section 4 summarizes an analysis of terrorist preparations for the 9/11 attacks. This analysis suggests that "deterrence" influences decision making for terrorists perpetrating complex plots. The section also explains the methods for estimating the deterrent effect of a mixture of several possible consequences and methods for estimating the deterrence contribution of multilayer defenses. Section 5 introduces several testable hypotheses concerning the generality of these findings and possible explanations for the willingness function. It also emphasizes the importance of interdisciplinary, integrated research to focus all available knowledge on understanding the risk judgments of criminals, insurgents, and terrorists.

## 2 DEFINITIONS AND SOURCES

A great deal of deterrence research addresses the prisoner's dilemma gaming of the cold war standoff, rate of loss models of military attrition, or guidance to law enforcement in various situations, often with the underlying assumption of a linear relationship between effort and effect. By contrast, this work focuses on the psychology of perpetrators represented as a fraction of a pool willing to act. Therefore, this approach does not discriminate between individual behavior and distributions across a perpetrator population.

The US military has formally defined both deterrence and strategic deterrence; the first applies to thwarting terrorists in general, while the second applies to complex plots that could damage the vital interests of the United States. Remarkably, these definitions include a psychological interpretation of deterrence.

Primary data sources in the public domain are cited at the end of this section. Unfortunately, many organizations applying deterrence in their operations cannot publicly release their classified data, and others with fewer restrictions are reluctant to do so. Moreover, these organizations also do not see their mission as one of justifying support for sustained applied research or any basic science.

### 2.1 Definition of Deterrence

The US Department of Defense (DoD) defines deterrence as "the prevention from action by fear of consequences—deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction" [4]. Even suicide terrorists must fear some consequences, especially risks that undermine their motives for taking such drastic action. For example, some terrorists might fear failure, arrest, or loss of life without completing their mission; dishonoring or bringing retribution upon their families; embarrassing their cause and supporters of their cause; or revealing a larger scheme or its supporting network.

### 2.2 Definition of Strategic Deterrence

Recently, the DoD introduced a related concept: "*strategic deterrence* is defined as the prevention of adversary aggression or coercion threatening vital interests of the United States and/or our national survival; strategic deterrence convinces adversaries not to take grievous courses of action by means of decisive influence over their decision making" [5]. This definition should exclude individuals who are mentally ill, act impulsively, or act alone. Strategic deterrence primarily applies to complex plots and networks with sufficient resources to threaten national vital interests. Although the empirical quantitative model reveals that deterrence will not thwart everyone, its cumulative and systemic impact on complex plots or networks should be capable of debilitating virtually all of them.

### 2.3 Information from Operational Sources

Operational organizations provided an interview report summarizing the responses of a very diverse population of 109 imprisoned drug smugglers. Analyses of these data led to the development of a simple mathematical expression representing the psychology of deterrence [1, 3]. Two reports provide more details on the interviews and operational data from major countercocaine operations [3, 6] used to verify and calibrate the deterrence model. Unfortunately, other data sets are not available for public release.

## 3 PRINCIPAL FINDINGS

Deterrence is essential for amplifying limited interdiction capabilities to thwart hostile activity. For example, lethal consequences can amplify interdiction effort by more than a factor of 10. The following quantitative representation of the psychology of deterrence and associated tactical lessons has been used to size forces, guide operations, and assess operational effectiveness in counterdrug and counterterrorism operations. Although the references provide more detail, one case is summarized: the air interdiction operations against smugglers flying cocaine from Peru to Colombia. This case illustrates the effectiveness of deterrence, verifies essential features of the mathematical form of the willingness function, and provides calibration for lethal consequences.

### 3.1 Willingness Function

The "willingness function" expresses the psychological aspects of deterrence in mathematical terms. It facilitates an estimate of the fraction of all would-be perpetrators willing to challenge the risks of interdiction. It has one independent variable, the probability of interdiction, $P_I$, and one constant parameter, the threshold of deterrence, $P_0$, calibrated to the specific perceived consequences of interdiction. Figure 1 plots the willingness functions for three different values of the deterrence threshold. The vertical axis represents the fraction of perpetrators and the horizontal axis represents the probability of interdiction.

To interpret a willingness function, consider the light curve. As the interdiction probability increases from zero, all would-be perpetrators remain willing to continue until their perception of the interdiction probability reaches the deterrence threshold at a probability of interdiction of 0.13. Beyond the deterrence threshold, the fraction of the perpetrators still willing to perpetrate, $W(P_I)$, declines in proportion to the inverse of the perceived

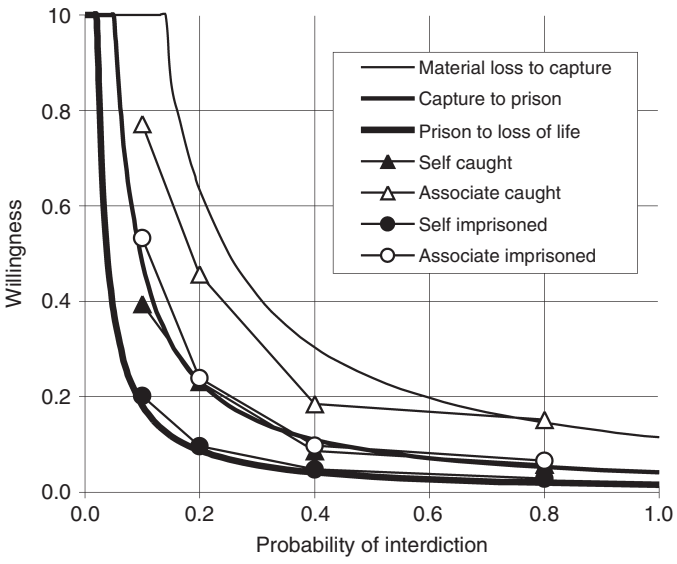



**FIGURE 1** The willingness function.

probability of interdiction:

$$W = \frac{P_0}{P_I}. \tag{1}$$

As the interdiction probability approaches 1.0, however, a small fraction, $P_0$, of the perpetrators persist, even expecting certain interdiction. In interviews with imprisoned drug smugglers, some commented that they would continue smuggling knowing they would be imprisoned since one fee, given in advance, would more than compensate for their prison time [3]. Scofflaw fishermen violating restrictions that protect living marine resources also behave according to the deterrence model and show no indication of quitting out to an 80% probability of interdiction [1].

Heavy, medium, and light curves in Figure 1 illustrate willingness functions bounding the ranges of four different types of consequences. The heavy curve represents the boundary between "lethal" consequences and "imprisonment" and is determined by a threshold of deterrence of 0.02. The medium weight curve separates "imprisonment" from "capture followed by release" and has a threshold of 0.05. The light curve separates "capture and release" from "loss of material assets" and has a threshold of 0.13.

Figure 1 also shows four sets of data obtained from voluntary interviews of imprisoned smugglers. Each was asked whether he or she would be willing to continue to smuggle if the chance of interdiction equaled successively higher values as indicated by data symbols along the trend lines. The same willingness questions were asked for different consequences, for example, being caught then released or being imprisoned, and for two different perceptual orientations, answering for themselves and answering as if they were a former associate smuggler. As the researchers anticipated, the interviewees estimated their associates would be more willing to continue smuggling than they would be now that they have experienced incarceration. These cumulative trends illustrate how well the willingness function boundaries parallel and bracket the interview responses.

In such very high-risk activities, perpetrators appear to decide whether the risks are acceptable before even considering the adequacy of the rewards. For example, all inmates stated their willingness to smuggle without any reference to wages. On separate questions exploring the sensitivity of willingness to wage levels, significantly higher wage offers did not increase the previously declared fraction of the smugglers willing to face the risks. However, if risks do increase, the wage necessary to sustain smuggler willingness at their previously declared levels increases quadratically relative to the increased risk.

### 3.2 Surge Operations

Surge operations typically consist of doubling or more the interdiction pressure and sustains it long enough to convince perpetrators that they cannot simply outwait the interdictors (typically 2–5 months for counterdrug operations). Surges have effectively communicated risks to perpetrators and caused lasting deterrence, even as interdiction efforts substantially relax from surge levels [1, 3].

A surge operation can provide valuable intelligence since it can induce perpetrators to react, thereby revealing their clandestine activity and the level of their deterrence threshold. Focusing surges on criminal hot spots should amplify the visibility of criminal reaction to deterrence, and has proven capable of doing so in urban areas [7]. However, if perpetrators can change their mode of operation or shift their location, the interview

data suggests they will change whenever interdiction risk reaches only approximately one-half of the deterrence threshold [1, 3]. Thus, operators must take this possibility into account in their subsequent planning.

### 3.3 Breakouts from Deterrence

A mathematical property of the willingness function shows that deterrence, once established, is at risk of instability. After deterrence has suppressed attempts, the estimated fraction of perpetrators actually interdicted tends to remain constant at a magnitude equal to the deterrence threshold:

$$W \cdot P_I = \left(\frac{P_0}{P_I}\right) \cdot P_I = P_0. \tag{2}$$

Under normal conditions, defenders need only interdict this constant fraction to deter. However, any diversion of interdiction effort elsewhere or additional recruitment expanding the pool of potential perpetrators, possibly as the result of an external event, could cause the fraction interdicted to drop below the deterrence threshold. This would most likely trigger a burst of perpetrator attempts, threatening a breakout from deterrence. Interdictors, therefore, need to maintain a reserve capacity, or other overwhelming threat of counteraction, to prevent breakout or reestablish deterrence.

### 3.4 Deterrence Model

The deterrence model estimates the fraction of all perpetrators thwarted by interdictors, $P_t$, that is, those who are either interdicted or deterred.

$$P_t = 1 - (1 - P_I) \cdot W(P_I^*) \tag{3}$$

where $P_I^*$ is the perceived probability of interdiction. Under steady conditions with well-informed perpetrators, the willingness function represents the subjective aspects of perceived risk, and $P_I^*$ equals $P_I$. During surges or other transition periods, however, there might be a diversity of perceptions with many misunderstandings of the real situation. Since the probability of thwarting an attempt equals the probability of unsuccessful attempts, it is one minus the probability of those willing and able to avoid interdiction.

### 3.5 Example—Peruvian Drug Flights

A series of operations to interdict and deter air traffickers flying cocaine base from Peru to Colombia provided an estimate of the deterrence threshold for lethal consequences [1, 3]. These operations also demonstrated the impact of an initial surge and proved that perpetrators will ignore even lethal consequences under some conditions.

The US detection and monitoring support to the Peruvians provided nearly perfect coverage of trafficker flights, and the combined capacities of those flights closely matched satellite estimates of the coca crop during periods without deterrence. This enabled an estimate of those willing, while complete and verified interdiction records gave probability of interdiction.

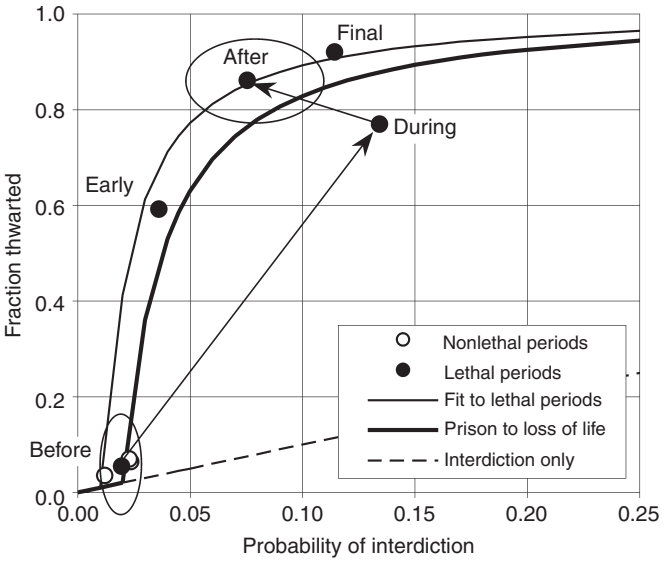



**FIGURE 2** Deterrence model for lethal interdiction showing operational periods intended to stop smuggler flights from Peru to Colombia.

Figure 2 shows the principal operational periods plotted over two deterrence model curves. The vertical axis is the fraction of flights thwarted and the horizontal axis shows the probability of interdiction. Each operational period lasted from 7 to 11 months, identified 100–500 smuggler flights, and involved 6–17 interdictions. Ovals represent conservative estimates of the asymmetric uncertainty ranges from both statistical and systematic sources. Open circles represent periods of nonlethal consequences during which air traffickers carried all cocaine base destined for Colombia. Filled circles represent periods with lethal consequences.

Three periods of lethal interdiction illustrate the transition from no deterrence to full deterrence, after passing through an intervening surge. Figure 2 labels these as "before," "during," and "after." In the 10-month "before" period, there is no evidence for deterrence; smugglers simply ignored lethal consequences. Since the Peruvians did not have US detection and monitoring support, they only shot down seven smugglers. This is well within the statistical uncertainty range of the deterrence threshold for lethal interdiction indicated by the heavy curve.

To aid the Peruvians in protecting their national security against an ongoing insurgency, the US Presidential Directive resumed intelligence support to their air force. This initiated the surge period "during" the transition. In the first month, Peruvian interceptors interdicted eight trafficker flights. Unusually high levels of lethal interdiction continued, and smuggling flights plummeted as trafficker pilots communicated and adjusted their perception of the risks. Full deterrence had set in by the period labeled "after." Since the probability of interdiction in the transition period exceeded the trafficker pilots' perceptions of that probability, the point labeled "during" is out of equilibrium and does not lie on the deterrence model curves.

In the first month of the "after" period, interdictors relaxed their pressure, and smuggler flights increased fourfold. Interdiction support resumed the next month, and once again,

traffickers were deterred. Thereafter, intelligence reports indicating depressed coca prices sustained the support for interdiction. Illicit Peruvian coca cultivation eventually declined to less than one-third of its previous levels.

The best-fit value for the deterrence threshold for lethal consequences, excluding the "during" period, is 1.2 ± 0.2%. Since the distribution of interdictions by month is a Poisson distribution, the operational variation about the threshold is comparable to the threshold itself. Consequently, operational planners adopt a conservative value of 2.0% for the lethal threshold to cover this variation.

### 3.6 Interdictor's Dilemma

The Peruvian experience illustrates the interdictor's dilemma: is deterrence working or are perpetrators avoiding detection? In the general case, the only resolution to this dilemma is convincing corroborating intelligence proving damage to the illicit activity. Often this is supplemented by intelligence indicating perpetrator intent, consequences perpetrators fear, and clandestine attempts.

### 3.7 Defender's Dilemma

Defense can be a thankless task. If there are no explicit hostile acts, why do we need to continue operations? If deterrence fails and there are attacks, who do we hold accountable? Defensive operations driven by concerns over accountability promote routine activities that become vulnerable to terrorist probes.

Two potential sources of information can transform passive and reactive defenses into dynamic ones taking the initiative. First, deterrence operations can be augmented with intelligence collection on perpetrator attempts to probe or defeat our defenses, and, second, red teams, exercises, and gaming can be employed to continually introduce new and adaptive elements into our defenses. These activities could also provide credible information for evaluating effectiveness and justifying resources.

## 4 IMPORTANT APPLICATIONS

Do lessons learned from criminals transfer to insurgents and terrorists? Analysis of the preparations for the 9/11 attacks indicates consistency between the drug smugglers' deterrence threshold for lethal consequences of 0.012 and the inferred subjective criterion used by Mohamed Atta to initiate the attack. Although factors other than psychological ones might also have applied, there was evidence of deterrence further up the leadership hierarchy. The 9/11 Commission Report stated on page 247, "According to [Ramzi] Binalshibh, had Bin Laden and [Khalid Sheikh Mohammed] KSM learned prior to 9/11 that Moussaoui had been detained, they might have canceled the operation." A second application of the willingness function extends it to estimate the deterrence effect of combinations of consequences. A third application extends the deterrence model to estimate the contribution of deterrence to multiple layers of defense.

### 4.1 Deterrence of 9/11 Terrorists

Although dedicated suicide terrorists perpetrated the 9/11 attacks, analysis reveals that they were probably deterred from hasty action until they developed confidence in their

plan [8]. Terrorists must exercise extreme caution day-to-day while preparing for a complex attack, and risk aversion provides a basis for deterrence. Their cautious preparations and practice flights were analyzed as a system reliability problem: for a plot consisting of *all four hijacked flights reaching their targets*, how many unchallenged "practice" flights would be necessary to reduce their perceived risk of failure to a level comparable to the deterrence threshold for lethal interdiction derived from studies of drug smugglers? By this criterion, in addition to the flights necessary to assemble the team in the United States, the 9/11 plot leaders would have had to practice 20–40 more times to be confident of the success of the attack. After this analysis was published, Chapter 7 of the 9/11 Commission Report mentions at least 80 flights, half of which are domestic, and 8 of those use the hijacking routes, box cutters and all. This analysis illustrates how our imperfect deterrence of individuals could have compounded to undermine their complex plot.

### 4.2 Deterrence through Combining Consequences

Interdictors need a means of estimating the deterrence effect of a combination of risks, especially for anticipating the effect of multiple layers of defense. A logically consistent method for doing this is obtained by drawing an analogy with expressions for expected utility and related models from the psychology of decision making under risk:

$$\sum_{i=1}^{N} \frac{P_{I,i}}{P_{0,i}} = P_I \cdot \sum_{i=1}^{N} \frac{(P_{I,i}/P_I)}{P_{0,i}} = \frac{P_I}{P_0} = \frac{1}{W} \text{ where } P_I = \sum_{i=1}^{N} P_{I,i}. \tag{4}$$

This represents a combination of $N$ risks, each with probability of interdiction, $P_{I,i}$, and deterrence threshold, $P_{0,i}$. The combination also recovers the mathematical form of an inverse willingness function by identifying the following expression as a deterrence threshold:

$$P_0 = \left[ \sum_{i=1}^{N} \frac{(P_{I,i}/P_I)}{P_{0,i}} \right]^{-1}. \tag{5}$$

Since $W \leq 1.0$ implies deterrence, the corresponding condition is $1/W \geq 1.0$. Note that the individual risks, $P_{I,i}/P_{0,i}$, all can be below their respective thresholds, yet their combination can deter.

Since the consequences represent losses, the inverse willingness, $1/W$, can be interpreted as a measure of risk. Those familiar with economics of choice among lotteries or the psychology of judgment under uncertainty will recognize the left-hand expression in Eq. (4) as similar to that for estimating risk, with $1/P_{0,i}$ corresponding to the utility function or more generally the subjective utility.

Other than the Peru–Colombia flights, all of the operations, for which there are data, involved a combination of consequences [1, 3], and these followed the willingness function. As an example of mixed consequences, consider the wide range of consequences faced by cocaine smugglers at each of the five transactional steps required to breakdown multiton loads from Colombia into gram-sized purchases by millions of users in the United States. Remarkably, traffickers at all levels share the risk since traffickers lose

on average 12% of their loads at each step [2]. The following equation illustrates how a plausible mixture of consequences could result in a 12% deterrence threshold:

$$\frac{P_I}{P_0} = \frac{0.12}{0.12} = 1.0 = \frac{P_{I,lethal}}{P_{0,lethal}} + \frac{P_{I,\mathrm{Pr}ison}}{P_{0,\mathrm{Pr}ison}} + \frac{P_{I,Drugs}}{P_{0,Drugs}} = \frac{0.004}{0.02} + \frac{0.022}{0.05} + \frac{0.094}{0.25} \quad (6)$$

Here, a 0.4% chance of death, a 2.2% chance of being imprisoned, and a 9.4% chance of losing the drugs and most likely the smuggling vehicle could combine to yield the 12% threshold. Note that each of the individual contributions is below its respective deterrence threshold.

Although the logical consistency and plausibility of this method for combining consequences can be verified, in general, one must exercise caution and plan to verify the estimated combination since the research on descriptive risk judgments describes many deviations from the simple prescriptive form of the expected utility [9–11]. Mathematical simplicity is an overriding practical consideration for counterterrorism operations, and the simplicity of the willingness function is remarkably relative to other models from the literature that require several parameters to represent subject responses. A fundamental difference, however, between the willingness function and expressions found in the literature is that acceptance or attractiveness of a gamble is generally interpreted as the *negative of risk* rather than its *reciprocal* [12]. Why the willingness function fits the available data so well remains a mystery. Possibly perpetrator preoccupation with extreme risk reduces the complex general case to a simpler asymptotic form.

### 4.3 Defense in Depth

Estimating the ability of several layers of defense to thwart terrorists requires an understanding of how terrorists might perceive those defenses. Some circumstances might cause terrorists to perceive all of the layers as one barrier (e.g. if penetrating the first layer required penetrating all layers, as with passengers on a ship, or if terrorist planners required several members of a cell to be able to penetrate all of the layers). By contrast, other situations would allow perpetrators to attempt penetrations one layer at a time.

If all layers are perceived as one barrier, each layer becomes a separate risk, and all layers a combination of those risks. Again, for such a combination, individual layers might not pose sufficient risk to exceed the deterrence threshold, yet together they could. This advantage of layers perceived as one barrier is offset by the high rate of undeterrables, numerically equivalent to the deterrence threshold for only one barrier.

If, however, the layers are viewed as independent risks, some or all must pose a risk above the deterrence threshold if deterrence is to contribute. Since the layers each thwart a fraction of the perpetrators, their effects compound multiplicatively to suppress residual leakage. This also assumes that undeterrables at one layer might be deterred by a risk at a subsequent layer. If it were otherwise, terrorist planners employing a team of less cautious undeterrables for a complex plot would risk revealing it before it could be executed.

Figure 3 shows the deterrence model for two-layer defenses plotted against the probability of interdiction for one layer that is assumed representative of both layers. A large deterrence threshold of 0.2 expands the graphic scale to ease visualization. With two layers perceived as one barrier, deterrence begins at approximately one-half the deterrence thresholds of the individual layers. (With very large thresholds at each layer, the

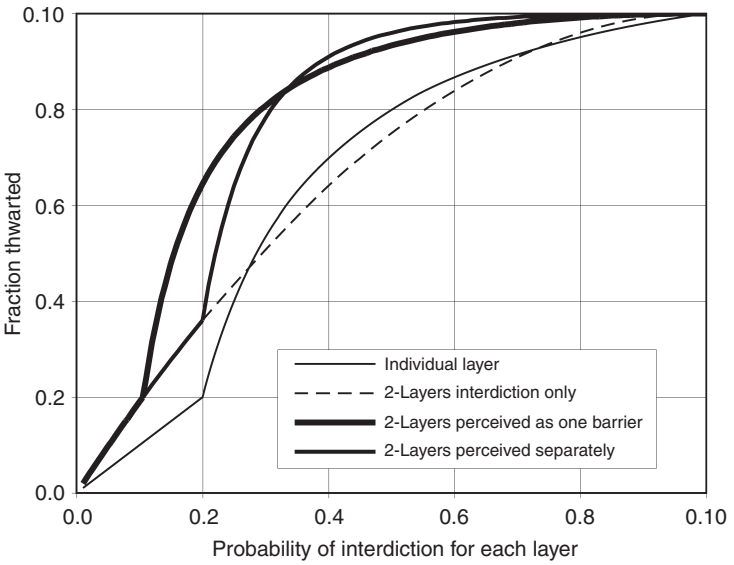



**FIGURE 3** Comparison of deterrence models for two-layered defenses.

probability of confronting deeper layers would be discounted by the chances of being interdicted at earlier ones.) Also, in Figure 3, the two layers acting separately compound to thwart relatively more perpetrators beyond an interdiction rate of approximately 0.33.

Correlations among layers could undermine or enhance deterrence relative to these baseline cases. Perpetrators might view both layers as equivalent—after crossing one, the other is an assured passage—hence undermining deterrence. Alternatively, the first layer could alert interdictors at subsequent layers to suspicious individuals for a more in-depth examination or perpetrators falsifying statements at one layer might increase the consequences if interdicted at a subsequent layer; both of these possibilities would enhance deterrence if they were known to would-be perpetrators.

## 5 RESEARCH DIRECTIONS

How broadly does the willingness function apply? How might the willingness function be knit into the body of established psychological and behavioral findings? Future research should integrate these findings and other work on deterrence into a unified area of study so that lessons transfer and deeper understanding informs our ongoing counterterrorism efforts.

### 5.1 General Result

Several testable hypotheses suggest that the understanding of deterrence presented here applies to those taking extreme risks, including drug traffickers, insurgents, and terrorists:

- People can judge risk directly [1, 3, 9–11], and with simple mathematical regularity in extreme situations.

- Underlying motives are more common than different. Even drug traffickers seek respect from their reference group, need to maintain a lifestyle, pursue the thrill of risk taking, and, in some cases, fund insurgencies and terrorism.
- The mathematical simplicity of the willingness function is difficult to explain without appealing to some overriding principle, given the intricacies of the psychological theories and models as well as the diversity of subjects and situations covered by the willingness function.

### 5.2 Explaining the Willingness Function

Future research might examine two alternative explanations of the willingness function and connect them with the study of decision under uncertainty:

- In the psychology of persuasion, the persuasiveness of a communication is a sum over salient novel arguments; thus, the constant fraction interdicted might represent a constant rate of persuasive argumentation against perpetrating acts [13].
- If the decline of those willing represents the distribution of those with greater needs than the likely consequences of deterrence, then the decline might parallel the Pareto distribution that extends toward lower incomes [14].

Extensive research into the psychology of judgment under risk should be applicable to deterrence, yet the models and methods address acceptance as the negative rather than the reciprocal of risk. Might there be a universal asymptotic distribution converging on an inverse power law?

### 5.3 Integrating the Research Community

Understanding the psychology of deterrence as it applies to terrorists requires information on, among other things, terrorist perspectives, intentions, perceptions of risk, and behavior. Results presented here indicate that it appears possible to relate deterrence of terrorists and insurgents to criminals and extreme risk takers. A national research effort to understand deterrence would have to integrate intelligence sources, operational experience, and various social science research communities. Today, the barriers between these three communities are formidable. Hopefully, this handbook will raise awareness of the value of, and need for, a synthesis across these institutional barriers, and catalyze efforts toward that end.

## REFERENCES

1. Anthony, R.W. United Nations Office on Drugs and Crime. (2004). A calibrated model of the psychology of deterrence. *Bull. Narc.: Illicit Drug Markets* **LVI**(1 and 2), 49–64.
2. Anthony, R.W., and Fries, A. United Nations Office on Drugs and Crime. (2004). Empirical modeling of narcotics trafficking from farm gate to street. *Bull. Narc.: Illicit Drug Markets* **LVI**(1 and 2), 1–48.
3. Anthony, R.W., Crane, B.D., and Hanson, S.F. (2000). *Deterrence Effects and Peru's Force-Down / Shoot-Down Policy: Lessons Learned for Counter-Cocaine Interdiction Operations*. Institute for Defense Analyses, p. 252. IDA Paper P-3472.

4. *Department of Defense Dictionary of Military and Associated Terms*. (2000). *JCS Pub 1–02*, Joint Chiefs of Staff Publication.
5. U.S. Strategic Command. (2004). *Strategic Deterrence Joint Operating Concept*, Director, Policy, Resources and Requirements, Offutt AFB, NE, p. 77.
6. Crane, B.D. (1999). *Deterrence Effects of Operation Frontier Shield*, Institute for Defense Analyses, IDA Paper P-3460, (25) March 1999.
7. Sherman, L.W., and Weisburd, D. (1995). General deterrent effects of police patrol in crime "Hot Spots": a randomized, controlled trial. *Justice Q.* **12**(4), 625–648.
8. Anthony, R.W. (2002). *Deterrence of the 9-11 Terrorists*, Institute for Defense Analyses, Document D-2802, (15) December 2002.
9. Kahneman, D., and Tversky, A. (1979). Prospect theory: an analysis of decision under risk. *Econometrica* **47**(2), 263–291.
10. Weber, E.U. (1997). The utility of measuring and modeling perceived risk. In *Choice Decision and Measurement: Essays in Honor of R. Duncan Luce*, A.A.J. Marley, Ed. Lawrence Erlbaum Associates, pp. 45–56, 472.
11. Jia, J., Dyer, J.S., and Butler, J.C. (1999). Measures of perceived risk. *Manage. Sci.* **45**(4), 519–532.
12. Weber, E.U., Anderson, C.J., and Birnbaum, M.H. (1992). A theory of perceived risk and attractiveness. *Organ. Behav. Hum. Decis. Process.* **52**, 492–523.
13. Perloff, R.M. (2003). *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*. 2nd ed., Lawrence Erlbaum Associates, New Jersey and London, p. 392.
14. Reed, W.J. (2001). The Pareto, Zipf and other power laws. *Econ. Lett.* **74**, 15–19.

## FURTHER READING

The references to the psychological literature and "Research Directions" section provide a starting point on further reading.

# DECISION SUPPORT SYSTEMS

# TECHNOLOGIES FOR REAL-TIME DATA ACQUISITION, INTEGRATION, AND TRANSMISSION

CHARLES K. HUYCK AND PAUL R. AMYX
*Imagecat, Inc., Long Beach, California*

## 1 INTRODUCTION

Real-time sources typically stream raw data for a given hazard tied to collection of specific locations. This data is useful not only for engineers and scientists studying natural phenomena, but when the data is processed correctly, it can aid in emergency management decisions. Real-time data can be used in a planning capacity to determine the likelihood of disaster striking a specific area, as with the monitoring of hurricanes tracks, or fault slip rates. Real-time data is essential in tracking events which are slow to evolve and provide ample time to respond, such as tracking hurricanes and flood stages. In some cases, real-time sensors provide immediate access to warning data, such as *in situ* hazardous material sensors or earthquake early warning systems. Immediately after an event, when the extent of damage is unclear, raw data from accelerometers and anemometers provide data to estimate the spatial extent of damage, and can be used to provide responders with a road map for response. During response, real-time data allows managers to monitor the public, asses traffic congestion, assess damage, and monitor progress. The following section provides a description of select real-time data sources in the United States.

## 2 AVAILABILITY OF REAL-TIME DATA

Real-time data acquisition should include data from the proliferation of mobile phone devices that can be used to record images, video, and send text, and data sent to a general repository from the general public. Increasingly, information and communication sources are becoming far more prevalent in the form of distributed GPS, video, mobile phones, and humans as sensors. This direction is sure to continue as wireless Internet devices and MEMS are integrated into commercial off-the-shelf (COTS) products. The communication and security equipment available on 11 September 2001 did not prevent United Airlines Flight 93 from being hijacked, but mobile phones played a crucial role in

preventing the ultimate goal of the hijacking. Successful real-time data integration should consider both *in situ* sensors sponsored by the government and informal multimodal real-time and near real-time data streams, including humans as sensors. This is particularly important in developing countries and when coordinating international response, where formal real-time data may not be available.

Real-time data can be critical in triggering decisions such as whether to evacuate, deploy personnel, and stage resources. With proper preparation, real-time data can be combined with modeling programs to estimate projected impact of a disaster in near real time. The next section explores how real-time data can be integrated into decision support systems (DSS) where they can effectively be used to make decisions.

## 3 UTILIZING REAL-TIME DATA FOR DECISION-MAKING

Typically it is not effective to stream raw hazard data directly to emergency managers. Although these data are critical to measuring the magnitude and spatial extent of an event, first responders and government officials generally lack the expertise to interpret raw numbers indicating contamination levels, wind speeds, and ground motions [1]. Raw data need to be interpreted by experts and converted into meaningful metrics, such as projected losses and casualties. In many cases, utilizing this data (Table 1 and Table 2) requires manually gleaning real-time data from web sites, FTP sites, or RSS feeds. The data must then be verified, processed, and massaged before it can be loaded into DSS. Real-time data is most effective when it is automatically processed, run through a DSS, and verified before dissemination. The knowledge required to massage raw data can be time-consuming, when timing is critical, and the expertise required to process data may be known by a limited number of people, who may not be available when disaster strikes. Table 3 presents several modeling platforms, highlighting the availability of real-time data.

The Federal Emergency Management Agency's (FEMA's) loss estimation tool, *haz*ards United States (HAZUS), does not incorporate real-time data feeds, but is capable of importing data derived from real-time sources [2]. Processing this data requires careful consideration, and can be problematic. HAZUS supported HurrEvac data in MR 1 and supports alerts in MR 3, but the functionality was not included in MR 2. Engineers adjusted the program in MR 3 to adjust wind speeds for the overly conservative assumptions from direct interpretation of broad maximum wind speeds, without interpolation. For the flood model real-time data must be heavily processed before it is suitable for analysis. The "Quick Look" feature enabling calculations from a polygon with a single depth of flooding is difficult to produce, and can generate highly inaccurate results. With the "Enhanced Quick Look" feature, a user is able to generate a depth of flooding grid from a DEM and an inundation boundary. However, this provides only a "quick look" and should not be mistaken for a full hydrologic analysis. Expert users, if not software developers, should be on call to assure real-time data is used correctly within HAZUS.

Prompt Assessment of Global Earthquakes for Response (PAGER) is an example of a system developed to work directly with real-time data and provides notification of population exposure to significant groundshaking directly after an event. PAGER does not provide loss estimates, largely because it is designed to work internationally where building exposure and vulnerability may be unknown, although this is the ultimate goal

**TABLE 1 Real-Time Data Feeds from US Government Sources**

| Real-Time Data Source | Agency | Description | Use | Web Site |
|---|---|---|---|---|
| Water Watch | United States Geological Survey | Stream gauge data providing water levels on major streams | Early warning for flooding | http://water.usgs.gov/ waterwatch/ |
| ShakeCast | United States Geological Survey | Accelerometer network | Real-time ground motion following an earthquake | http://earthquake.usgs.gov/ resources/software/shakecast/ |
| Deep-ocean Assessment and Reporting of Tsunamis (DART) | National Oceanic and Atmospheric Administration | Network of buoys | Early warning for tsunamis | http://www.ndbc.noaa.gov/ dart/dart.shtml |
| SeaWinds QuikSCAT | National Aeronautics and Space Administration | Scatterometer | Track hurricane wind speeds and direction | http://winds.jpl.nasa.gov/missions/ quikscat/index.cfm |
| National Climatic Data Center—extreme wind speed data sets | National Oceanic and Atmospheric Administration | Peak gust wind speeds from a network of anemometers | Hurricane advisories | http://www.ncdc.noaa.gov/oa/ land.html |
| National Weather Service—Doppler radar | National Oceanic and Atmospheric Administration | Weather radar | Probable weather for extreme weather hazards | http://radar.weather.gov/ |

of the program. The information provided by PAGER allows emergency managers to deduce whether they are facing a large event with significant exposure or a small event, which would not be possible based on earthquake magnitude alone.

INLET (INternet-based Loss Estimation Tool) is a technology testing tool developed for the National Science Foundation, based on exposure databases for Los Angeles and Orange counties [3, 4]. Damage and casualties are produced after ShakeCast pushes a ShakeMap onto the hard drive of the server. A ShakeMap is an array of ground motion data easily converted into a GIS file. ShakeCast supports automatic determination of ground motion levels for a collection of locations, and can be configured to trigger a Perl script when data arrives at the computer [5]. In Inlet, ShakeCast determines ground motion for a collection of census tract centroids. When completed, a Perl script feeds these data into the INLET database and triggers INLET loss estimation routines. Because the ground motion recordings are more accurate than the ground motions that would be calculated from the attenuation functions, INLET is able to produce better results. The estimated distribution of damaged structures and casualties allows emergency responders to immediately understand the potential ramifications of the event [6, 7].

When results from programs like HAZUS and INLET are ported to an on-line environment, they can be merged with disaster portals that integrate spatial data. Ideally, this data will be linked with technologies presented in Table 2, where the general public provides text, messages, photos, and videos that enable emergency managers to rapidly verify loss estimates. Table 2 provides a list of COTS products that can supplement sensor networks to monitor an event and coordinate response. Some, such as radio frequency identification (RFID), have not been extensively used for emergency response but hold great promise if the preparatory measures are taken to integrate the data into emergency response. Internet and cell phone use have provided tremendous amounts of information through Internet blogs, video posting on You Tube, and the media. The use of this data can be highly problematic due to verifiability and unstructured formats, but avoiding the use of these sources of data because they are problematic, is a mistake. These sources will continue to provide damage assessment data for events as they unfold, and devising clever strategies to harness humans as sensors can potentially yield much greater information than sensors alone. The United States Geological Survey (USGS) "Can you feel it" program allows the general public to provide feedback in the form of a short questionnaire. When combined with geo-referencing, observations from the general

**TABLE 2 Real-Time Data Feeds from Public and Private Sources**

| Source | Description | Potential Use |
|---|---|---|
| Mobile phones and wireless Internet devices | Voice, SMS text messages, photos, video, and location | Monitoring traffic flow, situational awareness, damage assessment |
| Closed-circuit television (CCTV) | Video stream for security and crowd control | Monitoring traffic flow, situational awareness, damage assessment |
| Internet | Webcams, blogs, chats, emails | Situational awareness at the local level |
| Radio frequency identification (RFID) | Product inventories | Emergency resource allocation |

**TABLE 3 Software Programs Utilizing Real-Time Data to Support Decision-Making**

| Tool | Description | Hazard | Real-Time Data Link |
|---|---|---|---|
| HAZUS-MH™ (HAZards United States, Multi-Hazard) | Multihazard loss estimation software developed for FEMA by National Institute of Building Sciences (NIBS) | Earthquake | No real-time link, USGS ShakeMap import |
| | | Hurricane | No real-time link, National Hurricane Center forecast/advisory data download from HurrEvac FTP site |
| | | Flood | No real-time link, inundation boundary import |
| INLET (INternet-based Loss Estimation Tool) | Earthquake loss estimation tool to test integration of technologies into emergency response. For NSF | Earthquake | ShakeCast |
| CATS (Consequence Assessment Toolkit) | Loss estimation program. Developed for FEMA. Currently supported by Defense Threat Reduction Agency (DTRA) | Multihazard | Global Disaster Alert and Coordination System (http://www.gdacs.org/), uses National Earthquake Information Center (NEIC) RSS for earthquakes |
| ShakeCast | USGS RSS extended to generates custom reports of ground shaking by facility in real time | Earthquake | ShakeCast RSS feed |
| PAGER (USGS Prompt Assessment of Global Earthquakes for Response) | GIS intersection between ground shaking and global population databases | Earthquake | NEIC |
| MIDAS (Metrological Information and Dose Assessment System) | Plume modeling software for commercial, military, and civil government applications | Plume modeling | Meteorological data, plant effluent monitor data, National Oceanic and Atmospheric Administration (NOAA) data, and other RSS feeds |
| HPAC (Hazard Prediction and Assessment Capability) | DTRA plume modeling software military, and civil government applications | Plume modeling | Wind speed from National Weather Service (NWS) |
| CWMS (Corps Water Management System) | United States Army Corps of Engineers (USACE) real-time data management system for the HEC-RAS hydrologic modeling platform | Reservoir management | Various NWS, USGS, and USACE readings of river stage, reservoir elevation, gauge precipitation, and other hydrological data sets |

public are used to adjust and verify ground motions where accelerograms are sparse. Real-time data feeds benefit substantially when merged spatially with real-time observed data utilizing humans as sensors. Although the estimates still need to be verified and accurate inventory data is critical, the availability of this data, directly after an event when no other information is available, has the potential to optimize the use of resources and reduce the likelihood that lack of information will lead to an inappropriate level of response [8].

Real-time data is routinely used in transportation, and this could possibly be extended to disasters. Before an event makes landfall, real-time data can be used to trigger evacuation and monitor evacuation routes [9]. Real-time data can be used to reverse the evacuation process. Before Hurricane Rita made landfall in 2005, the National Hurricane Center (NHC) posted data confirming that it was highly unlikely that Houston would be affected, but the evacuation continued. When there is advance notice to an impending disaster, such as an earthquake or tsunami, warnings could be disseminated through ITS and text messaging systems. Directly after an event, real-time data can be used to confirm the state of critical transportation infrastructure. Bridge-health monitoring can be used not only to monitor safety, but to prioritize restoration, such as through incentives programs rewarding the early completion of construction [10]. Given a widespread disaster, real-time data can be an essential component in data dissemination for situational awareness. Locations of roads that are obstructed or destroyed can be disseminated through a variety of handheld and Internet resources. Mobile phones and portable devices are routinely equipped with mapping applications. These applications could be modified to adapt instructions based on collapsed bridges and blocked roadways. These alternate routes would be available to first responders, many of which may be from out of town. Under rapidly evolving conditions, situation awareness could be disseminated to the public on the roadways through text messaging and reverse 911. Additionally, text messages from the public can be used to inform emergency responders about the extent of damage.

## 4 IMPLEMENTATION ROAD-BLOCKS

Even under normal driving conditions, integration of real-time data into transportation is problematic. Although ITS message boards placed on freeways provide estimated drive times so that drivers can plan for delays, drivers must rely on their own experience to determine alternate routes, and since information is not provided for local roadways, their decisions are not well-informed. The key to resolving this problem may be cell phones and wireless Internet devices. As these devices begin to track congestion on the roadways, they will be capable of relaying this information back to a centralized system that can combine information from other commuters to suggest alternative routes. It is not clear, however, that this information will reduce congestion. When drivers receive information, they attempt to assess: (i) the status of an event; (ii) the expected duration of disruption; and (iii) the best action to take. With more accurate information, drivers are expected to behave in a more predictable manner. However, a transportation system with no information may be more efficient than a transportation system which advises an inordinate number of users to take a specific alternate route. Transportation models suitable for routing traffic optimally in real time will be required to optimize the use of real-time traffic data. This basic research is required before the models can be extended to address homeland security, where the models will need to be informed by research

into how drivers will react to routing instructions in the face of conflicting priorities, such as their perceived safety and the safety of their children.

With the surge in wireless bandwidth and the advent of low-cost sensors, it is very likely that managers will face a torrent of data for making critical decisions. Transforming raw, multimodal data streams into meaningful information will require new tools for analyzing and finding patterns in information; it will require algorithms that not only fuse disparate data sources, but proactively seek patterns in the data. These patterns must be presented through intuitive visual interfaces with analytical capabilities so that urban planners and other decision-makers can monitor events as they unfold. Data mining and data fusion algorithms need to be brought into the emergency management arena to address the potential flood of real-time data available from the proliferation of wireless and embedded devices.

In many instances, there are legal implications complicating the application of real-time data [11]. Emergency responders are in new territory with advanced technologies that allow very rapid response, live tracking, or even prediction of events. Emergency managers need clear legal and legislative support to empower decisions to pursue or reject advanced technologies. Without this support, it is very difficult for emergency managers to integrate advanced technologies with confidence.

The risk of false alarms, missing alerts, and sensor error needs to be addressed thoroughly before systems are developed to work in conjunction with real-time data [11]. There should always be a backup method to verify records. This may be from *in situ* videos, security personnel, or volunteers from the public.

Technology is evolving rapidly and best practices have a short window of opportunity to arise, before the next innovation occurs. Open Internet mapping applications such as Virtual Earth and Google Earth greatly simplify the process of disseminating real-time information gleaned from a variety of web sites [12]. The Southern California fires of 2007 revealed a very high level of sophistication of the media in geocoding burnt structures and displaying them with on-line maps. But given the limited spatial accuracy and conservative approach of delineating burn areas, maps depicted many more burnt structures than detailed surveys could confirm. Given the amount of data verification and interpretation required to correctly use real-time data for loss estimation, the emergency response community needs to establish the best way to use these data sets so that they are not misinterpreted. This requires not only building the IT infrastructure to process real-time data, but funding development in areas such as transportation, where the optimal use of real-time data is not clear.

Real-time data combined with DSS and Internet support systems can give emergency managers the tools they need to make informed decisions if data are effectively collected, verified, processed, and disseminated. Automation of these tasks assures that the data are available when they are needed. If real-time data is processed using well-known standards it can disseminate results and DSS routines, allowing calculations to occur and maps to be produced in the first half hour following an event, when they are most useful. DSS results need to be combined with data supplied from the general public using mobile phones and other devices. These data sources will continue to provide damage assessment data for events as they unfold, and devise clever strategies to harness humans as sensors, since they can potentially yield much greater information than sensors alone. Further research into multimodal data collection and information dissemination is needed to guide the use of real-time data in emergency response, particularly in the field of transportation.

## 5 WEB SITES

http://www.fema.gov/plan/prevent/hazus/index.shtm
http://www.nibs.org/hazusweb/
http://rescue-ibm.calit2.uci.edu/inlet/default.asp
http://cats.saic.com
http://earthquake.usgs.gov/resources/software/shakecast/
http://earthquake.usgs.gov/eqcenter/pager/
http://www.absconsulting.com/midas/index.html
http://www.dtra.mil/rd/programs/acec/hpac.cfm
http://nereids.jpl.nasa.gov/cgi-bin/nereids.cgi
http://radar.weather.gov/GIS.html
http://podaac.jpl.nasa.gov/DATA_PRODUCT/OVW/index.html

## ACKNOWLEDGMENTS

This study is supported by National Science Foundation (NSF) Grants through the University of California, Irvine. (NSF Award Number IIS-0331707).

Thanks to Paul Earle and Frank Lavelle for information regarding HAZUS and PAGER.

## REFERENCES

1. Huyck, C. K., and Adams, B. J. (2002). *Emergency Response in the Wake of the World Trade Center Attack: The Remote Sensing Perspective, MCEER Special Report Series on Engineering and Organizational Issues Related to the World Trade Center Terrorist Attack*, Vol. 3. Multidisciplinary Center for Earthquake Engineering Research, Buffalo, NY.
2. Seligson, H., Huyck, C. K., Ghosh, S., and Bortugno, E. (2004). *Data Standardization Guidelines for Loss Estimation–Populating Inventory Databases for HAZUS®99*. California Governor's Office of Emergency Services, Sacramento, CA.
3. Chung, H., Huyck, C. K., Cho, S., Mio, M. Z., Eguchi, R. T., Shinozuka, M., and Mehrotra, S. (2005). A centralized web-based loss estimation and transportation simulation platform for disaster response. *Proceedings of the 9th International Conferences on Structural Safety and Reliability (ICOSSAR'05)*.
4. Huyck, C. K., Chung, H., Cho, S., Mio, M. Z., Ghosh, S., and Eguchi, R. T. (2006). Centralized web-based loss estimation tool. *Proceedings of SPIE*.
5. Huyck, C. K., Chung, H., Cho, S., Mio, M. Z., Ghosh, S., Eguchi, R. T., and Mehrotra, S. (2006). Loss estimation on-line using INLET (Internet-based Loss Estimation Tool). *Proceedings of the Eighth National Conference on Earthquake Engineering (8NCEE)*.
6. Eguchi, R. T., Goltz, J. D., Seligson, H. A., Flores, P. J., Blais, N. C., Heaton, T. H., and Bortugno, E. (1997). Real-time loss estimation as an emergency response decision support system: the early post-earthquake damage assessment tool (EPEDAT). *Earthquake Spectra*, **13**(4), 815–833.
7. Eguchi, R. T., Goltz, J. D., Seligson, H. A., and Heaton, T. H. (1994). Real-time earthquake Hazard assessment in California: the early post-earthquake damage assessment tool and the Caltech-USGS broadcast of earthquakes. *Proceedings, Fifth US National Conference on Earthquake Engineering*, Vol. 1, 55–63.

8. Chung, H., Adams, B. J., Huyck, C. K., Ghosh, S., and Eguchi, R. T. (2004). Remote sensing for building inventory update and improved loss estimation in HAZUS99. *Proceedings of the 2nd International Workshop on Remote Sensing for Post-Disaster Response*.
9. Cho, S., Huyck, C. K., Ghosh, S., and Eguchi, R. T. (2006). Development of a web-based transportation modeling platform for emergency response. *Proceedings of the Eighth National Conference on Earthquake Engineering (8NCEE)*.
10. Werner, S. D., Lavoie, J. P., Eitzel, C., Cho, S., Huyck, C. K., Ghosh, S., Eguchi, R. T., Taylor, C. E., and Moore, J. E. II. (2003). *REDARS 1: Demonstration Software for Seismic Risk Analysis of Highway Systems. Research Progress and Accomplishment 2002-2003*. Multidisciplinary Center for Earthquake Engineering Research, Buffalo, NY.
11. Tierney, K. J. (2000). *Implementing a Seismic Computerized Alert System (SCAN) for Southern California: Lessons and Guidance from the Literature on Warning Response and Warning Systems*. Disaster Research Center, University of Delaware.
12. Huyck, C. K. (2005). Suggestions for the effective use of remote sensing data in emergency management. *NRC Planning for Catastrophe Study Workshop on Geospatial Information for Disaster Management*. National Academy of Sciences.

## FURTHER READING

ABS Consulting/EQE International, Inc. (2001, 2002). *TriNet Studies and Planning Activities in Real-time Earthquake Early Warning V1-4*, Irvine, California.

Shoaf, K. I., and Bourque, L. B. (2001). *Survey of Potential Early Warning System Users*. Center for Public Health and Disasters, University of California, Los Angeles, CA.

# MULTI-OBJECTIVE DECISION ANALYSIS

GREGORY S. PARNELL
*Department of Systems Engineering, United States Military Academy, West Point, New York*
*Innovative Decisions Inc., Vienna, Virginia*

## 1 INTRODUCTION

Multiobjective decision analysis (MODA) is an appropriate operations research technique to determine the best alternative when we have complex alternatives, multiple conflicting objectives, and significant uncertainties. Other names for this type of technique are multiple attribute utility theory, multiple attribute value theory, multiple attribute preference theory, and multiple criteria decision analysis. Keeney and Raiffa published the seminal

book in 1976 [1]. Kirkwood wrote an excellent contemporary textbook [2]. Value-focused thinking (VFT) is a philosophy to guide decision makers to create higher value alternatives [3]. It has three major ideas: start with values, use values to generate better alternatives, and use values to evaluate those alternatives. VFT is usually implemented using the mathematics of MODA. Since MODA requires an understanding of theory and the art of modeling, experienced decision analysts are required to effectively use the technique.

## 2 TYPES OF DECISION PROBLEMS

A decision is an irrevocable allocation of resources [4]. It is useful to distinguish two types of decision problems: a single decision and a portfolio of decisions. In a single-decision problem, we select the best alternative from a group of potential alternatives. An example is selecting the best vaccine for a bioagent that could be used by terrorists. In portfolio decision making, we select the best group of decisions. Examples include selecting the best set of vaccines to develop and protect the nation against the most likely bioagents that terrorists might use in the United States, selecting the best portfolio of research and development (R&D) projects to fund from a large set of projects, annually allocating an organization's budget to the best projects (or programs) from a large set of potential projects, and systems design using multiple subsystems and components.

In this article, we illustrate the first type of decision. Kirkwood [2] describes how to use MODA for resource allocation decision making and Parnell et al. [5] describe how to use MODA for systems design.

## 3 DEFINITIONS

Analysts should use precise technical language to define key MODA terms. Here are the terms used in this article in logical order.

- *Fundamental objective.* The most basic objective we are trying to achieve. Example: select the best vaccine for a bioagent.
- *Functions.* A function is a verb–object combination, for example, detect bioagents. When multiple decisions are involved, you may want to identify functions before identifying the objectives. An alternative term is missions or tasks.
- *Objective.* A preference statement that expands on the fundamental objective. Example: maximize effectiveness of the vaccine.
- *Value measure.* Scale to assess how well we attain an objective. For example, we may measure the time to detect the dispersal of a bioagent. Alternative terms are evaluation measures, measures of effectiveness, measure of performance, measures of merit, and metrics.
- *Range of a value measure.* The possible variation of the scores of a value measure, such as probability of detection in 24 h after dispersal may range from 0.0 to 1.0.
- *Score (level).* A specific numerical rating of the value measure, such as a time to detect a bioagent dispersal. A score may be on a natural or a constructed scale. (We avoid using the term value for scores because the value function uses that term.)

- *Qualitative value model.* The complete description of our qualitative values, including the fundamental objective, functions (if used), objectives, and value measures.
- *Value hierarchy (value tree).* Pictorial representation of the qualitative value model.
- *Tier (layer).* Levels in the value hierarchy.
- *Weights.* The weight assigns a value measure depending on the measure's importance and the range of the value measure. Weights are our relative preference for value measures. They must sum to one.
- *Value function.* A function that assigns value to a value measure's score. Quantitatively, value is defined as *returns to scale on the value measure* [2].
- *Quantitative value model.* The value functions, weights, and mathematical equation (such as the additive value model) to evaluate the alternatives.
- *Value model.* The qualitative and quantitative values models.
- *Utility.* Utility is different from value. It includes returns to scale and risk preference. Kirkwood [2] covers methods for assessing utility functions.
- *Utility function.* A function that assigns utility to a value-measure score. We assess utility functions using lotteries [2].

We should modify our lexicon to use terms that are familiar to our decision makers and stakeholders. For example, the problem domain may use criteria and performance measures instead of objectives and value measures.

## 4 QUALITATIVE VALUE MODELING

Qualitative value modeling is critical to the success of an analysis. If we do not get the decision makers' and stakeholders' values qualitatively right, they will not (and should not) care about our quantitative analysis. The key to successful value modeling is to determine whose values to model. In analyzing commercial decisions, the decision makers usually want to produce the highest shareholder value or net present value. When customers buy the product or service, future shareholder value will increase. Similarly, for many homeland security decisions, the values may be the future values of national, state, and local decision makers; private companies; and our citizens.

Value models usually include several key aspects of value:

- Why we are making this decision (fundamental objective)
- What we value (functions and objectives)
- Where we achieve an objective (location)
- When we achieve an objective (time preference)
- How well we attain an objective (value measures and value functions)
- How important is the objective (weights)

Notice that value models do not include *how* one does an activity. Instead, we care about how well the alternative works. For example, a vaccine could be a pill, a shot, or an aerosol. We do not score directly how it is used, but we might have a value measure that scores ease of use. Structured techniques based on clear criteria are the key to credible and defensible qualitative value modeling.

### 4.1 Criteria for Developing a Successful Value Model

Qualitative value models must satisfy four criteria by being collectively exhaustive, mutually exclusive, operable, and as small as possible—though Kirkwood describes the first two criteria differently [2]. By collectively exhaustive, it means that value models must consider all essential types of evaluation. Their criteria are mutually exclusive if they do not overlap. Further, the value measures must be operable, which means the data is available and everyone interprets them in the same way. Finally, we should use as few value measures as possible to limit the model's size. Only include those values that can be affected by the decision and those values that are essential to the decision.

Parnell [6] provides four structured techniques for value modeling. The amount of effort to develop a value model corresponds directly to the number of measures. Each value measure must have a defined scale and a value function. Thus, more value measures result in more time for model development and scoring.

### 4.2 Developing a Qualitative Value Model

It is useful to distinguish between models that use functions and objectives, and models that use only objectives. For portfolio decisions, it is useful to identify the functions first and then the objectives.

*Step 1: Identify the fundamental objective.* Identifying the fundamental objective is the essential first step that guides how we develop the value model. It must be a clear, concise statement of the most basic reason for the decision. In practice, we take time and apply thought to properly specify the fundamental objective. Once we understand it, we can determine if we have single or multiple functions. If we have a single function, we can skip step 2 and start to identify the objectives.

*Step 2: Identify functions that provide value.* We can get functions from documents or develop them using functional analysis [5]. Affinity diagramming is an excellent technique for identifying functions [7]. We use research and brainstorming to discover action verb–object combinations (e.g. detect attack and provide warning) that describe potential future functions. Then, we group verb–object combinations by affinity (similarity). Sometimes, it is useful to establish functions and subfunctions before identifying the objectives.

Affinity diagramming has two major benefits for value-model development. First, affinity groups are mutually exclusive (each function different) and collectively exhaustive (all necessary functions identified). Secondly, affinity diagramming usually identifies new functions required for our fundamental objective.

*Step 3: Identify the objectives that define value.* For each function, we need to identify the objectives that define value. Objectives can come from documents, interviews with senior leaders, or workshops with stakeholders (or stakeholders' representatives). Again, affinity diagrams are excellent for developing mutually exclusive and collectively exhaustive objectives.

*Step 4: Identify the value measures.* We can identify value measures by research and interviews with decision makers, stakeholders, and subject-matter experts. Access to stakeholders and subject-matter experts is the key to developing good value measures. Kirkwood [2] identifies two useful dimensions for value measures: alignment with the objective and type of measure. Alignment with the objective can be direct or by

**TABLE 1 Preference for Types of Value Measure**

| Type | Direct Alignment | Proxy Alignment |
|---|---|---|
| Natural | 1 | 3 |
| Constructed | 2 | 4 |

proxy. A direct measure focuses on attaining the objective, for example, efficacy of the vaccine against the bioagent. A proxy measure focuses on attaining an associated objective, for example, the number of casualties is a proxy for the consequences of a bioagent attack. The type of measure can be natural or constructed. A natural measure is in general use and commonly interpreted, such as cost in dollars. We develop a constructed measure (such as homeland security advisory system classifications [8]) when natural measures do not exist.

Table 1 reflects the author's preferences for types of value measures. Priorities 1 and 4 are obvious. Direct and constructed measures to proxy and natural for two reasons are preferred. First, alignment with the objective is more important than the type of scale. Secondly, one direct and constructed measure can replace many natural and proxy measures. Keeney and Raiffa [1], Kirkwood [2], and Keeney [3] provide useful information on how to develop value measures.

*Step 5: Vet the qualitative value model with key decision makers and stakeholders.* We must ensure that our model has captured the values of the decision makers and stakeholders. Vetting the qualitative value model and incorporating their comments is critical to ensuring that they will accept the analysis results.

Figure 1 provides a terrorist value hierarchy. The terrorist organization's fundamental objective is to remove US presence in the Middle East. The three objectives of a terrorist attack are to maximize economic impact (measured in dollars), maximize people killed (measured in number of deaths), and maximize citizen fear (measured in a constructed citizen fear scale).

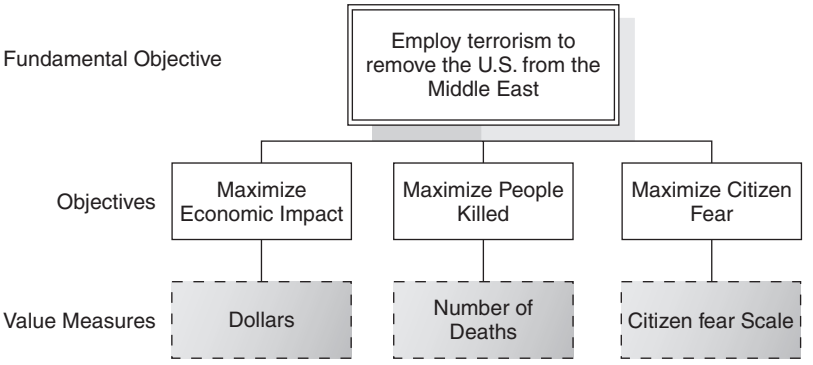



**FIGURE 1** Terrorist value hierarchy.

## 5 QUANTITATIVE VALUE MODELING

Once we have vetted the qualitative value model with our decision makers and key stakeholders, we are ready to develop the quantitative value model. It includes the mathematical model, value functions, and weights.

### 5.1 Mathematical Model

MODA uses many mathematical equations to evaluate alternatives [1]. The simplest and most commonly used model is the additive value model [2]. This model uses the following equation to calculate each alternative's value:

$$v(x) = \sum_{i=1}^{n} w_i v_i(x_i)$$

where $v(x)$ is the alternative's value, $i = 1$ to $n$ is the number of the value measure, $x_i$ is the alternative's score on the $i$th value measure, $v_i\ (x_i)$ is the single-dimensional value function that converts a score of $x_i$ to a normalized value, $w_i$ is the weight of the $i$th value measure, and $\sum_{i=1}^{n} w_i = 1$ (all weights sum to one).

The additive value model has no index for the alternatives because our values do not depend on the alternative since we do not put "how" in the model. We use the same equations to evaluate every alternative.

### 5.2 Value Functions Measure Returns to Scale

Value functions measure returns to scale on the value measures [2]. They have four basic shapes: linear, concave, convex, and an S curve (Fig. 2). The linear value function has constant returns to scale: each increment of the measure is equally valuable. The concave value function has decreasing returns to scale: each increment is worth less than the preceding increment. The convex value function has increasing returns to scale: each

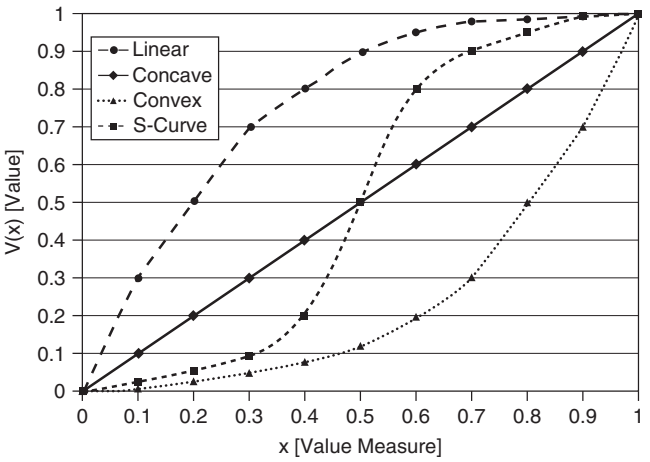



**FIGURE 2** Four types of value functions.

increment of the measure is worth more than the preceding increment. The S curve has increasing, then decreasing, returns to scale on the measure.

We have several techniques to develop value curves from subject-matter experts [2]. Our first step is to have the experts determine the shape of the value curve: linear, concave, convex, or S curve. Next, we use value increments to identify several points on the curve—asking experts the relative value of increments in the value-measure scale. Kirkwood [2] provides Excel macros that can be used to easily implement value functions.

### 5.3 Weights Depend on Importance and Range of the Value-Measure Scales

Weights play a key role in the additive value model. MODA quantitatively assesses the trade-offs between conflicting objectives by evaluating the alternative's contribution to the value measures (a score converted to value by single-dimensional value functions) and the importance of each value measure (weight). The weights depend on the measure scales' importance and range. If we hold constant all other measure ranges and reduce the range of one of the measure scales, the measure's relative weight decreases, and the weight assigned to the others increases since the weights add to 1.0. The only mathematically correct way to do weights is bottom-up using the variation of the value measures. A very effective weighting technique is the swing weight matrix [9].

## 6 ALTERNATIVE SCORING USING VALUE-FOCUSED THINKING

Once we have vetted the quantitative value model and developed alternatives, we must score the alternatives on the value measures. VFT [3] has three major ideas: start with your values, use your values to evaluate alternatives, and use your values to generate better alternatives. VFT is a tool to foster creativity. Since we use values to develop the value hierarchy, alternative scoring has two purposes: evaluating alternatives and generating better ones. The second purpose is most important. When we begin to score our alternatives, we will identify value gaps—chances to improve the alternatives (create better scores) to achieve higher value.

It is prudent to consider who will score the alternatives and how we will resolve scoring disagreements. Three scoring approaches have been successful: alternative champions, a scoring panel, and alternative champions reviewed by a scoring panel.

- *Scoring by alternative champions.* This approach is useful because it provides information about values from the value model directly to "champions" as they do the scoring. A disadvantage is the perception that a champion of an alternative may bias a score to unduly favor it or that scores from different champions will be inconsistent.
- *Scoring by a scoring panel.* To avoid the perception of scoring bias and potential scoring inconsistencies, subject-matter experts can convene as a panel to assign scores and improve the alternatives. Champions of alternatives can present scoring recommendations to the panel, but the panel assigns the score.
- *Scoring by alternative champions reviewed by a scoring panel.* Having the idea champion score the alternative and modify it to create more value is the essence of VFT. A scoring review panel can then ensure that the scores are unbiased and consistent.

Once we have the scores, we can start evaluating the alternatives—typically through deterministic analysis and probabilistic (or uncertainty) analysis.

## 7 ANALYSIS OF ALTERNATIVES

Analysis of alternatives using MODA involves deterministic and probabilistic analysis. In deterministic analysis, all the parameters are known for certain. In probabilistic analysis some of the parameters can be uncertain. Probabilistic analysis can provide insights about deterministic and stochastic domination [10].

### 7.1 Deterministic Analysis of Alternatives

In deterministic analysis, uncertainty is not a factor. We can determine the dominant alternatives and their values without probabilities. See Parnell [6] for deterministic analysis of portfolio decisions.

In addition to scoring our alternatives, we should always include the current (or baseline) alternative and the ideal (or perfect) alternative. Several types of analysis are useful to obtain insights about the alternatives, and many software packages have built-in features that "automate" do sensitivity analysis.

- *Stacked bar.* Stacked bar graphs are a useful way to compare alternatives. The "stacks" show the contribution for one level in the hierarchy. We can plot the stacked bar graphs for any level in the hierarchy. Analysis usually begins top down to identify insights.
- *Value gaps.* Value gaps are one of the key insights that we can extract from stacked bar graphs. Values gaps are the differences between the best alternative and the ideal alternative. We can examine them at all levels in the value hierarchy, so they "shine a light" on areas for VFT.
- *Value versus cost.* It is always find it useful to separate cost and benefits (value) typically by plotting the value versus the cost of the alternatives. This chart helps to quickly identify the dominant alternatives and enables decision makers to see the value added for the additional cost.
- *Sensitivity analysis.* Sensitivity analysis is useful for key parameters, including some weights and scores.

### 7.2 Probabilistic Analysis of Alternatives

The additive value model allows for three sources of uncertainty—alternative scores, value functions, and weights. Risk is the probability of a low value (utility). We can model our uncertainty about alternative scores using probability distributions. We can sequence the decisions and uncertainties using decision trees. Using distributions, the additive value model gives us the probability distribution of value (utility), from which decision makers can directly assess the alternative's risk. We also can do sensitivity analysis to weights or value functions that might change depending on the future scenario [6].

The usual approach to uncertainty analysis is to put probability distributions on the scores (or variables affecting the scores) that reflect our uncertainty about the alternative's future score on the value measures. The additive value model can then assess how uncertainty affects value (or utility). Two approaches are common: MODA with decision trees and Monte Carlo simulation.

- *MODA with decision trees.* We can add the uncertain variables (exogenous variables or alternative scores) as nodes in a decision tree. Then, we use the additive value model to assess value (utility) at the end of the tree. The best alternative comes from the decision tree's "average out/fold back" algorithm [10]. This method works equally well for independent and dependent uncertain variables.
- *Monte Carlo simulation.* Monte Carlo simulation is useful to assess how uncertainty affects alternative value (or utility). It has four main steps: develop probability distributions for uncertain variables, draw a random number for each uncertain variable and for each distribution, calculate the value (or utility) using all simulated scores, and do numerous runs and plot a value (utility) distribution to assess the alternative's risk. This method works for independent and dependent uncertain variables, but we must express the dependent variables as functions of the independent variables.

Parnell [6] provides additional techniques for probabilistic analysis.

## 8 USES OF MODA FOR HOMELAND SECURITY

Decision analysis using MODA/VFT has been used in many problem domains [11, 12]. Parnell et al. [5] describe a systems decision-making framework that can be applied to homeland security challenges. Recent applications include the following homeland security capabilities [13]: ports and harbors [14], information assurance [15–17], commercial airlines [18], and general terrorist attacks [19].

In this section, we briefly describe a probabilistic decision analysis application of an adversary threat scenario for bioterrorism to illustrate how MODA, using decision trees, can be applied to homeland security challenges. Usually, we are the decision makers and we use our assessment of our values and our uncertainties. However, since terrorists are intelligent adversaries, it may be useful to consider their values and uncertainties. The terrorist's influence diagram [20] is shown in Figure 3. Squares are decisions, circles are uncertain nodes, rounded squares are deterministic nodes, and terrorist value is the multiobjective value node used to solve the diagram. In this very simplified model, the terrorist has three decisions: the target, the agent, and the acquisition decisions. The terrorist has three major uncertainties: does he obtain the agent, is he detected before attack, and is the attack successful. The decision alternatives and the sequence of the decisions and events are shown in the decision tree in Figure 4. The probabilities are conditioned on the assumption that the terrorist has decided to attack. In addition, the probability of an event can depend on the terrorist's decisions and other uncertain events. For example, the probability that he obtains the agent depends on the type of agent and how he acquires the agent. In this simplified model, the migration effectiveness depends on the target and the agent. Finally, the terrorist has two objectives: maximize deaths and maximize economic impact. An additive value model with linear value functions and equal weights is assumed.

Using the DPL software [20], we can solve for the preferred terrorist decision. The highest value strategy for the terrorist is shown in Figure 5. On the basis of this (notional) data, the terrorist prefers to produce agent C to attack location Y. In addition to the decision, we can use decision analysis tools to learn significant additional information. For example, location Y is twice as good as location X; location Y stochastically dominates [10] locations X, and his probability of obtaining the agent is higher (0.42) than his probability of being detected before the attack (0.4).

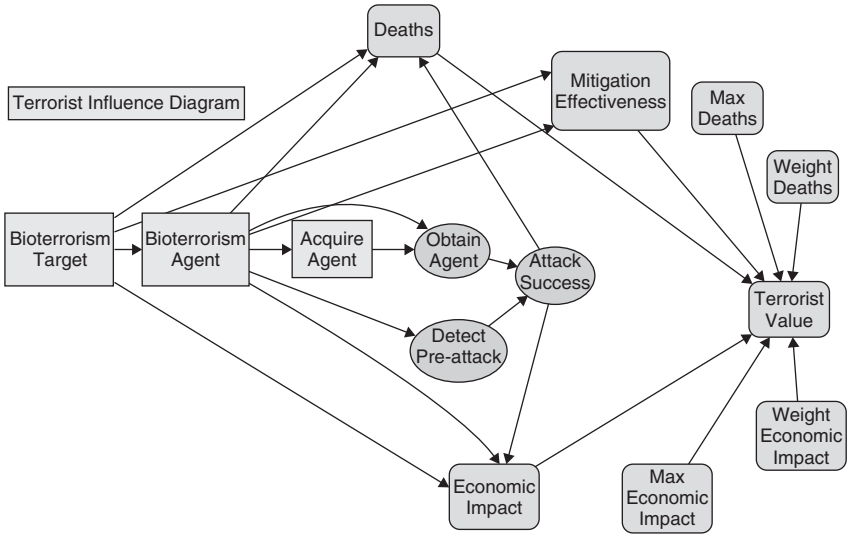



**FIGURE 3** Terrorist influence diagram.

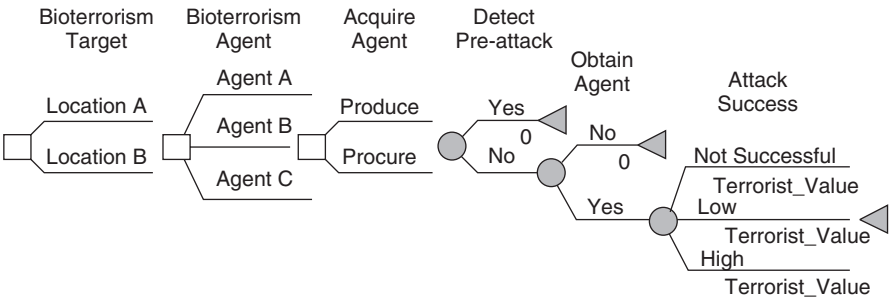



**FIGURE 4** Terrorist decision tree.

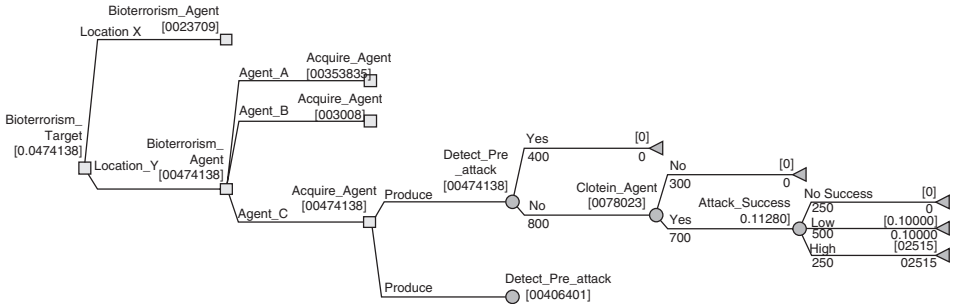



**FIGURE 5** Terrorist's highest value strategy.

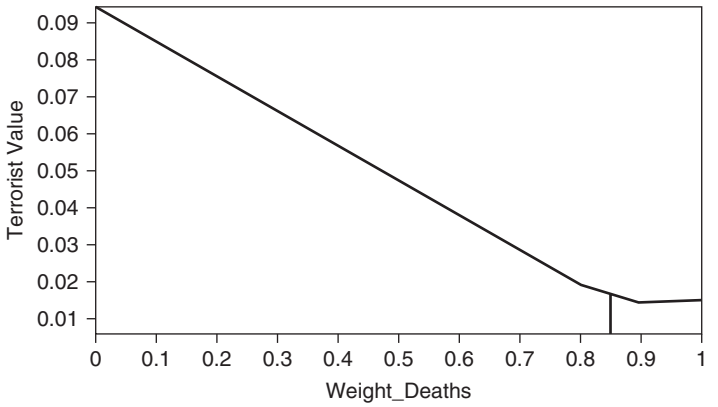



**FIGURE 6** Location sensitivity to weight assigned to deaths.

Decision analysis also provides useful tools for sensitivity analysis. Figure 6 shows the sensitivity of the target location decision to the assumption about weights. If the terrorist assigns a weight of less than 0.85 to deaths, he would prefer location Y. If the weight is greater than 0.85, he would prefer X. If we had considered multiple locations, some may never be preferred. In addition, two-way sensitivity plots and tornado diagrams can also be used to assess the sensitivity to assumptions.

## 9 SUMMARY

In this article, we have introduced and illustrated MODA. MODA is an appropriate operations research technique to determine the best alternative when we have complex alternatives, multiple conflicting objectives, and significant uncertainties. MODA asks the right questions: what we can value, what are the major uncertainties, and what can we do to achieve our values? We have seen that MODA can be used to analyze complex homeland security alternatives using value models (our values or our adversaries' values) of conflicting objectives, probability models of uncertainty, and decision trees to determine the best alternative. MODA provides a logically consistent, credible, and defensible methodology to provide analysis insights for decision makers.

## ACKNOWLEDGMENT

The anonymous reviewers provided useful suggestions to improve the clarity of this article.

## REFERENCES

1. Keeney, R. L., and Raiffa, H. (1976). *Decision Making with Multiple Objectives: Preferences and Value Tradeoffs*, John Wiley & Sons, New York.
2. Kirkwood, C. W. (1997). *Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets*, Duxbury Press, Pacific Grove, CA,

3. Keeney, R. L. (1992). *Value-Focused Thinking: A Path to Creative Decisionmaking*, Harvard University Press, Cambridge, MA.
4. Howard, R. (1983). *Decision Analysis Class Notes*, Stanford University, California, CA.
5. Parnell, G. S., Driscoll, P. J., and Henderson, D. L., eds. (2008). *Systems Decision Making for Systems Engineering and Management*. John Wiley & Sons, Inc.
6. Parnell, G. S. (2007). Chapter 19. *Value-Focused Thinking Using Multiple Objective Decision Analysis in Methods for Conducting Military Operational Analysis: Best Practices in use Throughout the Department of Defense*, R., Larry, and A. Loerch, Eds. Military Operations Research Society. Washington, DC.
7. (2006). *Affinity Diagrams, Basic Tools for Process Improvement*, accessed June 1, 2006. http://www.saferpak.com/affinity_articles/howto_affinity.pdf.
8. Homeland Security Advisory System. (2006). www.dhs.gov, accessed September 3, 2006.
9. Ewing, P. L., Tarantino, W. J., and Parnell, G. S. (2006). Use of decision analysis in the army base realignment and closure (BRAC) 2005 military value analysis. *Decision Anal.* **3**(1), 33–49.
10. Clemen, R. T., and Reilly, T. (2001). *Making Hard Decisions with Decision Tools Suite update 2004 Edition*, Duxbury Press, Pacific Grove, CA.
11. Corner, J. L., and Kirkwood, C. W. (1991). Decision analysis applications in the operations research literature, 1970–1989. *Oper. Res.* **39**, 206–219.
12. Keefer, D. L., Corner, J. L., and Kirkwood, C. W. (2004). Perspectives on decision analysis applications, 1990–2001. *Decision Anal.* **1**(1), 4–22.
13. Pruitt, K. A., Deckro, R. F., and Chambal, S. P. (2004). Modeling homeland security. *J. Def. Model. Simulat.* **1**(4), 187–200.
14. Parnell, G. S., Figueira, J. R., and Bennett, S. (2007). *Decision analysis tools for safety, security, and sustainability of ports and harbors in NATO workshop: risk management tools for port security, critical infrastructure, and sustainability*, Springer, Netherlands.
15. Buckshaw, D. L., Parnell, G. S., Unkenholz, W. L., Parks, D. L., Wallner, J. M., and Saydjari, O. S. (2005). Mission oriented risk and design analysis of critical information systems. *Mil. Oper. Res.* **10**(2), 19–38.
16. Hamill, J. T., Deckro, R. F., and Kloeber, J. M. (2005). Evaluating information assurance strategies. *Decis. Support. Syst.* **39**(3), 463–484.
17. Hamill, J. T., Deckro, R. F., Kloeber, J. M., and Kelso, T. S. (2002). Risk management and the value of information in a defense computer system. *Mil. Oper. Res.* **7**(2), 61–81.
18. Von Winterfeldt, D., and O'Sullivan, T. M. (2006). Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? *Decision Anal.* **3**(2), 63–75.
19. Paté-Cornell, M. E.. Guikema, S. D.. (2002). Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. *Mil. Oper. Res.*, **7**(4), 5–20.
20. Syncopation Software.(2006).*DPL Decision Analysis Software*,http://www.syncopationsoftware.com/, accessed November 9, 2006.

## FURTHER READING

Parnell, G.S., Dillon-Merrill, R.L., and Bresnick, T.A. (2005). Integrating risk management with homeland security and antiterrorism resource allocation decision-making. in *The McGraw-Hill Handbook of Homeland Security*, D. Kamien, ed. McGraw-Hill, New York, pp. 431–461.

Watson, S. R.. Buede, D. M. (1987). *Decision Synthesis: the Principles and Practice of Decision Analysis*, Cambridge University Press, Cambridge.

# NATURALISTIC DECISION MAKING, EXPERTISE, AND HOMELAND SECURITY

EDUARDO SALAS AND MICHAEL A. ROSEN
*Department of Psychology, Institute for Simulation and Training, University of Central Florida, Orlando, Florida*

## 1 INTRODUCTION

Homeland Security (HS) is a "people business". It is fundamentally about the interaction of people with other people and understanding the intent of other people. It is about psychology, communication, deception, recognition, coordination, teamwork, situation assessment, and decision making. This is completely evident on the frontlines of HS where police officers, transportation security administration (TSA) agents, and border patrol agents come face to face with possible threats to security. However, it is equally the case in complex intelligence analysis where agents may be working behind several layers of sophisticated technology. No matter how elaborate a system of information collection, analysis, and representation may be, as long as there remains a human in the loop, the expertise of that human will play a role in HS. The decision-making effectiveness of people from the frontline law enforcers to intelligence analysts will impact these national goals. Therefore, understanding how people perceive, integrate, process, disseminate, communicate, and execute decision making in these types of complex environments is of critical importance. This knowledge can be used to train better decision makers and to design systems that support the way experts make decisions to further boost performance and safety.

So, if HS is about people, about interactions, decision making, and expertise, what are the means available to ensure the highest possible levels of safety and security? What should be the scientific basis of efforts to build and maintain safeguards against threats to the nation? This article is dedicated to reviewing the naturalistic decision making (NDM) approach and, more generally, the present understanding of the role of expertise in organizations. Also, we propose that the NDM approach and the scientific understanding of human expertise make valuable contributions to HS efforts. The substantial and continually growing scientific literature concerning how people develop, maintain, and leverage expertise in complex and stress-filled environments can provide information on the design and analysis of sociotechnical systems supporting HS. To this end, we pursue three main goals in this article: (i) provide a definition and general overview of NDM, (ii) review current methodological approaches and tools in NDM, and (iii) briefly highlight findings from the NDM literature that describe expert individual and team decision making. Before addressing these goals, we provide some illustrative examples of NDM applications to HS.

## 2 WHAT DO EXPERTISE AND NDM HAVE TO DO WITH HOMELAND SECURITY?

One of the defining features of NDM is a commitment to improving decision-making performance. This begs the question: how can NDM help HS efforts? In general, the NDM approach contributes to organizational effectiveness by providing an understanding of how expert decision makers perform effectively (i.e. What processes and knowledge does the expert use? What coordination strategies are used?). This understanding can be leveraged into better training programs [1] to create more expert decision makers at a faster rate as well as better system design [2] to facilitate the performance of experts. Specific applications of the NDM approach to HS are numerous. Two brief examples are provided below: information analysis and baggage screening.

The task of intelligence analysis is extremely complex. The analyst must "sort through enormous volumes of data and combine seemingly unrelated events to construct an accurate interpretation of a situation, and make predictions about complex dynamic events" [3, pp. 281–282]. During this process, a multitude of decisions must be made concerning the validity, reliability, and significance of various pieces of information, as well as how information may fit complex patterns extended over time [4]. To further complicate matters, this task is conducted in an environment where uncertainty and deception are pervasive, time is frequently scarce, and there are costly consequences for failing to detect (or misinterpreting) patterns in the data and draw faulty inferences and predictions [5]. All of these factors produce an "unfriendly" environment for decision making; however, human decision makers are robust and manage to do well in such circumstances. In fact, information analysts have developed numerous methods for accomplishing their task, and the process has been characterized as highly idiosyncratic [6]. No doubt, some analysts' processes are better than others, and the NDM approach can be used to identify methods that are more effective. This can serve as the foundation for the development of a set of formalized methods and processes (as called for by Johnston [6]). This would be a monumental contribution that would expedite the development of experts within the domain. Additionally, Hutchinson et al. [7] applied NDM methods to the information analysts' task and found that the use of analysis tools that forced analysts to make decisions without a context for information was a major source of poor performance. This finding, along with the specifications of the contextual information that is necessary, can be used to develop tools that facilitate rather than encumber decision-making processes.

Like information analysis, baggage screening is a vital component to defenses against terrorist attacks. Though in many senses, baggage screening does not involve the "cognitive complexity" of intelligence analysis, there is a great deal of perceptual expertise involved in effective baggage screening. Detecting a pattern indicating a threat, in a long sequence of patterns containing primarily innocuous items, requires not only sustained attention, but the capacity to detect subtle visual cues [8]. Understanding what cues are used by expert baggage screeners can facilitate tools (e.g. augmented displays that emphasize critical information) as well as training programs to build perceptual expertise.

The two types of tasks discussed above are different in many critical ways. However, they share a commonality in that success depends on the expertise of human decision makers. Consequently, the nature of expertise and decision making can serve as a valuable scientific knowledge base to build and maintain effective HS sociotechnical systems.

## 3 WHAT IS NATURALISTIC DECISION MAKING?

In 1988, the USS Vincennes, a US Navy-guided missile cruiser, mistook a commercial Iranian flight for an attacking military jet. The crew of the Vincennes fired two missiles at what they thought was an imminent threat to their safety. The immediate result of this decision by the Vincennes crew was the tragic death of the 290 innocent passengers and crew members aboard the Iranian flight. However, this event was to have an enormous impact on the study of human decision making as well. A major research project called the Tactical Decision Making Under Stress (TADMUS) program, was launched with the aim of better understanding how decisions are made in high-stress, high-stake military environments. This project [see Ref. 9], in conjunction with preexisting research efforts [10] helped to advance what has come to be known as the *NDM community*, a group of researchers working to understand decision making in contexts where traditional decision-making research is not applicable. In the following sections, we provide an overview of this field and related work in the study of expertise. There are many parallels between the situation experienced by the Vincennes crew and those encountered by HS personnel: intense time pressure, high stakes outcomes, and uncertain information. NDM seeks to understand and support decision making in these types of environments and is therefore well suited to contribute to the scientific basis of HS.

### 3.1 NDM and Traditional Decision-Making Research

Spurred by the practical implications of the topic, decision making has been an subject of scientific inquiry for centuries. The prolonged attention given to decision making has produced an extensive theoretical and empirical literature base, which can generally be understood through one of the three paradigms: the formal-empiricist, the rationalist, and the naturalistic [11]. The formal-empiricist paradigm is typified by the classical decision making (CDM) approach and the rationale paradigm by the judgment and decision making (JDM), and behavioral decision theory (BDT) threads of research. Although each of these research traditions have made unique contributions, they all share fatal flaws that have rendered them ineffectual at explaining "real-world" decision performance in high-stress, high-stake environments like the Vincennes incident and many others common to HS [12]. First, the rationalist and formal-empiricist traditions both viewed decision making as selection of an alternative from a set of concurrently available options, which were all evaluated by the decision maker. Essentially, this amounted to imposing an idealized structure (i.e. exhaustive search and evaluation of decision alternatives) on the decision-making process. Most people do not actually use this approach when given ample time, and it is impossible to use while making decisions under time pressure and other stressors. Second, the rationalist and formal-empiricist traditions do not account for the expertise of the decision maker nor do they address complex multicomponent decisions [13]. Decisions were viewed as isolated from one another, and the past experience of the decision maker was viewed as irrelevant. In contrast to these two prescriptive traditions, which are both based upon an unrealistic ideal decision-making process, the naturalistic paradigm seeks to describe how effective decisions are made by professionals working in complex situations, where time is scarce and information incomplete or uncertain. The naturalistic paradigm is typified by NDM and organizational decision making (ODM) traditions, both of which are based on observational and descriptive research,

focus on what real decision makers actually do (cf. artificial laboratory tasks), and reject a view of decision making as choice from an exhaustive set of decision alternatives [14].

### 3.2 Defining the NDM Approach

The NDM approach can be defined most succinctly as an investigation of "the way people use their experience to make decisions in field settings" Zsambok [15], p. 4. There are two important implications of this definition that form the basis of the NDM approach. First, the expertise of the decision maker is fundamental to the decision-making process. An understanding of how decisions are made within a particular domain cannot be divorced from an understanding of the expertise of the decision maker [16]. Second, the NDM approach emphasizes the real-world context of decision making. NDM research happens "in the field" because decision making and expertise are tightly bound to the context of work [17]. Providing guidance on how to improve HS effectiveness involves generating an understanding of how effective HS personnel do their jobs and make good decisions.

Because of this focus on the context of work, descriptions of environmental factors that define NDM research have been proposed. These include the presence of ill-structured problems, uncertain and dynamic environments, shifting and ill-defined or competing goals, action/feedback loops, time stress, high stakes for decision outcomes, multiple players, and the influence of organizational goals and norms [12]. Although not all of these factors are present in all NDM research, several usually play an important role. To further illustrate the nature of the NDM approach, Lipshitz et al. [18] provide five essential characteristics of NDM research: (i) an emphasis on proficient decision makers, (ii) an orientation toward the *process* of decision making (not just outcomes), (iii) the development of situation–action matching decision rules, (iv) context-bound informal modeling, and (v) empirical-based prescription. As previously noted, the expertise of the decision maker is at the center of inquiry [19]. NDM emphasizes the processes of decision making [20] and developing descriptions of these processes that are practically useful. As reflected in the recognition-primed decision (RPD) model described below, emphasizing expertise and describing the process leads to an understanding of decision making as a process of matching features of a situation to past experience to retrieve rules and possible courses of action. Similarly, the importance of context becomes salient; experts use features of a particular situation that are causally or correlationally related to the problem at hand. Ultimately, NDM is concerned with improving a decision-making performance. To this end, all prescriptions resulting from NDM research focus on realistic actions and strategies that are feasible to apply in the real world.

### 3.3 Defining Expertise

By this point, it should be clear that human expertise is the center of the NDM approach and the primary tool of decision makers in complex environments. But what is expertise? In general, expertise is thought of as high levels of skill or knowledge in a specific area. This conceptualization is apparently simple, but a scientific explanation of expertise has undergone a long evolution. Initially, expertise was considered to be the result of the application of superior general reasoning strategies [21]; however, this was found to be a flawed approach for reasons similar to those which rendered rationalist and formal-empiricist approaches ineffectual to decision making. Specific domain knowledge, and not general reasoning strategies, was found to play a major role in expert performance

[22]. This finding shifted expertise research into the knowledge-based phase; it is the novice's performance that is best characterized by the use of general reasoning strategies, not the expert's. However, it is not just the amount of knowledge (or even organization) that determines expert performance. Expertise has come to be viewed as the result of the many adaptations (e.g. skilled memory, automaticity, specialized reasoning strategies) to the constraints of a domain and set of tasks [23]. Consequently, experts use different performance processes from those of novices, and do not just reach higher levels of performance outcomes by being better at using the same processes.

### 3.4 Exemplar NDM Theoretical Models

Nothing is more practical than a good theory. This section provides a brief description of several theoretical models and approaches discussed in the NDM literature.

***3.4.1 Recognition-Primed Decision Making.*** The RPD model is grounded in the scientific understanding of expertise and developed through extensive field observations of fireground commanders [17]. This model was developed to explain these fireground commanders' ability to make effective and extremely rapid decisions without performing an exhaustive analysis of the situation. The RPD provides a two-process description of expert decision making: (i) pattern recognition and (ii) mental simulation. In the pattern matching process, decision makers scan the environment to build an understanding of the present situation. This situation representation is used to match cues in the environment to a past experience. When a match is found, the course of action associated with that past experience can be retrieved. This represents a course of action that was successful in the past and hence may be effective in the current situation. In addition to a course of action, the decision maker retrieves expectancies associated with the situation, information about cues that are most critical to attend to, and goals for the situation. If a successful match is not found, the decision maker searches for more information to build a better representation of the situation. Once a course of action has been retrieved through this pattern recognition process, the decision maker evaluates the likely effectiveness of the retrieved course of action considering the unique aspects of the present situation. This is accomplished through mental simulation wherein the decision maker does a "cognitive walkthrough" of the implementation of the course of action and considers how the unique features of the present situation will impact the effectiveness of the course of action. Mental simulation results in either the adoption of the retrieved course of action unchanged or modified to the new situation, or rejection of the course of action. If the option is rejected, the decision maker returns to pattern recognition activities.

***3.4.2 Heuristics and Bounded Rationality.*** A complimentary yet distinct line of research has produced an explanation of decision-making performance in terms of fast and frugal heuristics [24]. This approach is known as the *study of bounded rationality* [25] and is the analysis of heuristics used by people, the structure of the decision-making environment, and the fit between these two things (called *ecological rationality*; [24]). By using adaptive heuristics with high levels of "ecological rationality", decision makers can engage in satisficing (i.e. taking the first acceptable solution) in complex environments where optimization is unobtainable [26]. From this perspective, an expert decision maker is one who possesses an "adaptive toolbox" [27], a set of heuristics well suited to the information structure of the environment. NDM and the bounded rationality

approach share much in common [28]. However, whereas the RPD (and other NDM models) relies on informal and descriptive models, the bounded rationality approach focuses on the formal modeling of the rules that decision makers actually use [29].

***3.4.3 Shared Mental Models.*** The preceding two theoretical approaches deal with individual decision making. Shared mental model theory is a dominant explanation of how expert teams make decisions effectively [30]. A shared mental model is an organized knowledge structure that enables the coordination of interdependent teamwork processes [31]. On the individual level, mental models are knowledge structures involved in the integration and comprehension of information. On the team level, a shared mental model is a knowledge structure that is partially shared and partially distributed throughout a team. By sharing and distributing these knowledge structures, team members are able to interpret incoming information in a similar or compatible manner. This, in turn, facilitates effective coordination; team members develop similar causal explanations of information and inferences about possible future states of the environment. Additionally, shared mental models enable the implicit communication patterns characteristic of expert teams [32]. HS security operations frequently require the coordination of multiple individuals and possibly even multiple teams (e.g. maritime interdictions). Shared mental model theory is an important theoretical perspective to understanding and subsequently boosting the effectiveness of performance in these types of situations.

## 4 WHAT METHODS ARE USED IN NDM RESEARCH?

Methods in the NDM approach require tools and techniques for eliciting, analyzing, and representing the knowledge and cognitive processes involved in task performance. Fortunately, many methods rooted in the theory and methods of cognitive psychology and the other cognitive sciences have been developed to this end. Broadly, these methods have been grouped under the label cognitive task analysis (CTA). Table 1 provides a summary of the primary types of methods used in NDM research (for comprehensive reviews of these techniques, see Rosen et al. [33] and [2, 34]). CTA is a loose set of methods and tools and not a codified and unitary "one-size-fits-all" method. Any one specific CTA approach must be developed considering the purpose of the CTA, practical constraints (e.g. time and access to experts), and the relative strengths and weaknesses of each specific method and tool.

A comprehensive review of the methods used by NDM researchers is outside the scope of this article. However, these methods fall into one of the four general categories. First, *process tracing techniques* involve capturing the external processes of task performance in a way that enables inferences to be made about the internal cognitive processes of the person performing the task [36]. Protocol analysis, information monitoring (i.e. capturing keystroke data), and eye tracking are examples of process tracing techniques. These methods provide a very robust and rich data set, but frequently require substantial time and effort to analyze. Second, *interview and observation techniques* provide direct access to the full range of social, organizational, and physical factors influencing cognitive work; however, field observations can be difficult to arrange due to security, safety, or logistical reasons. Interview approaches include the critical decision method [37], and techniques from ethnography and cognitive anthropology have been adapted to facilitate field observations [38]. Third, there are several *indirect and conceptual methods* available that, in

**TABLE 1 Overview of Methods Used in NDM Research**

| Category of Methods | Examples | General Strengths | General Weaknesses |
|---|---|---|---|
| Process tracing techniques | Protocol analysis | Rich quantity and quality of information | Data collection and analysis can be time consuming for many of the methods |
| | Decision analysis | Readily applicable to "real-world" settings | Some methods used concurrently with task performance may alter performance processes (e.g. verbalizing aspects of performance not generally verbalized) |
| | Information sampling | Methods are process-oriented; they focus on the sequences of activity | |
| | Verbal reports | | |
| | Nonverbal reports | | |
| Interview and observation | Critical decision method | Rich data | Time consuming to analyze |
| | Critical incident technique | Techniques have face validity to experts; they are familiar with them | Retrospective techniques produce data with uncertain reliability due to memory degradation |
| | Structured/semistructured/ unstructured interviews | Techniques are highly flexible and applicable in most contexts | Gaining access to field observations can be difficult |
| | Field observations | Focusing on critical incidents is highly efficient | Access to time with experts is generally limited |
| | | Gives "real-world" perspective on work processes | Observation can be reactive |
| | | Effectively identifies individual differences in performance | |
| Indirect/Conceptual methods | Concept maps | Can be very efficient (especially when combined with interview techniques) | Methods do not have high "face validity" for most domain experts |

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| Category of Methods | Examples | General Strengths | General Weaknesses |
|---|---|---|---|
| | Pairwise relatedness ratings | Helps experts make "tacit" knowledge explicit | |
| | Abstraction hierarchies | Knowledge elicitation and analysis are combined for concept mapping | |
| | Repertory grid technique | | |
| | Sorting techniques | | |
| | Multidimensional scaling, network scaling, and cluster analysis | | |
| Simulations and contrived tasks | Simulated task environment (ranging from high to low fidelity) | Allows for merger of experimental control and real-world task complexity | Risk of collecting data that is not valid in real context of performance |
| | Tasks that deviate from real-world task (hypotheticals) | Allows for observation of performance for tasks that occur at a low frequency on the job | Construction and validation of simulation takes time, effort, and money |
| | | Allows for observation of performance during events that would be unsafe in the real world | |

Adapted from Ref. 35.

general, attempt to assess the structure or organization of expert knowledge. Examples include concept mapping and paired comparison ratings [39]. These methods are very efficient and effective; however, they tend to lack face validity for domain experts. Fourth, the *simulations and contrived tasks* can be used to "bring the real world into the lab." Simulations offer a compromise between the complexity of the real world and experimental control and afford the ability to observe low-frequency events (e.g. observing how an expert flight crew handles a critical failure during a flight is not feasible in the real world but is possible and practical using simulations; [40]). However, simulations can be costly to develop and no matter how much effort is dedicated to replicating critical aspects of the real world, there will be some differences between the real world and the simulation that may influence a decision-making performance. Each of the types of methods has general strengths and weaknesses and any specific method will have its own trade-offs. Any one NDM investigation will likely use a combination of these methods in order to generate a robust understanding of the decision maker's expertise through triangulation while working within the practical constraints.

## 5 WHAT HAVE WE LEARNED FROM NDM AND EXPERTISE RESEARCH?

The NDM approach is solidly rooted in field research, and as such has been criticized for generating results with low levels of generalizability. The nature of expertise is domain specific; therefore, an understanding of one type of expert is not directly applicable to experts in other domains. However, a consistent pattern of findings has emerged from studies in many domains. These patterns represent a "prototype" of expert decision making; they are a set of mechanisms that individuals and teams use to make effective decisions. The importance of any one of the mechanisms will vary depending on the features of the decision-making task and environment. These mechanisms can be used as a framework for understanding expert decision making across domains, but must be contextualized to the specific task features of any one domain. We briefly review these patterns for expert individual and team decision making below. The mechanisms of expert individual and team decision making are listed in Tables 2 and 3, respectively.

**TABLE 2 Mechanisms of Expertise and Individual Decision Making**

| Expert Decision Makers . . . |
|---|
| Are tightly coupled to cues and contextual features of the environment . . . |
| They develop psychological and physiological adaptations to the task environment |
| They are sensitive to and leverage contextual patterns of cues in decision making |
| Have a larger knowledge base and organize it different than nonexperts . . . |
| They have a more conceptually organized knowledge base |
| They have more robust connections between aspects of their knowledge |
| They have a more abstracted and functional knowledge base |
| Engage in pattern recognition . . . |
| They perceive larger and more meaningful patterns in the environment |
| They are able to detect subtle cue configurations |
| They are able to retrieve courses of action based on situation/action matching rules |
| Have better situation assessment and problem representations . . . |
| They spend more time evaluating the situation |
| They create deeper, more conceptual, more functional, and more abstracted situation Representations |
| Have specialized memory skills . . . |
| They functionally increase their ability to handle large amounts of information |
| They anticipate what information will be needed in the decision making |
| Automate the small steps . . . |
| They quickly and effortlessly do what requires large amounts of attention for nonexperts |
| They have more cognitive resources available for dealing with more complex aspects of decision making |
| Self-regulate and monitor their processes . . . |
| They evaluate their own understanding of a situation |
| They judge the consistency, reliability and completeness of their information |
| They make good decisions about when to stop evaluating the situation |

Adapted from Ref. 33.

**TABLE 3 Prototypical Mechanisms of Expert Team Performance and Decision Making**

| Members of Expert Teams |
|---|
| They develop shared mental models |
| They anticipate each other's needs and actions |
| They can communicate implicitly |
| They interpret cues in a complimentary manner |
| Learn and adapt |
| They self-correct |
| They learn from past decision-making episodes |
| They adapt coordinating processes to dynamic environments |
| They compensate for each other |
| Maintain clear roles and responsibilities |
| They mange expectations. |
| They understand each others' roles and how they fit together |
| They maintain clarity of roles while maintaining flexibility |
| Possess clear, valued, and shared vision |
| They develop their goals with a shared sense of purpose |
| They guide their decisions with a common set of values |
| Develop a cycle of prebrief → performance → debrief |
| They regularly provide individual and team level feedback to one another |
| They establish and revise team goals and plans |
| They dynamically set priorities |
| They anticipate and review issues/problems of members |
| They periodically diagnose team decision making "effectiveness", including its results, and its processes |
| Are lead by strong team leaders |
| They are led by someone with good leadership skills and not just technical competence |
| They believe the leaders care about them |
| Leaders of expert teams provide situation updates |
| Leaders of expert teams foster teamwork, coordination and cooperation |
| Leaders of expert teams self-correct first |
| **Have a strong sense of "collective," trust, teamness, and confidence** |
| They manage conflict well; they confront each other effectively |
| They have a strong sense of team orientation |
| They trust other team members' "intentions" |
| They strongly believe in the team's collective ability to succeed |
| Cooperate and coordinate |
| They identify teamwork and task work requirements |
| They ensure that, through staffing and/or development, the team possesses the right mix of competencies |
| They consciously integrate new team members |
| They distribute and assign work thoughtfully |
| They examine and adjust the team's physical workplace to optimize communication and coordination |

Adapted from Ref. 41.

### 5.1 Individuals

With experience, decision makers adapt their psychological processes to fit the decision-making task and environmental constraints [42]. The ability to leverage contextual structure into decision-making processes [43] and a larger and more organized knowledge base [22] enables the expert decision maker's pattern recognition ability—the primary means of making effective decisions without exhaustive search and evaluation of options. As previously discussed, pattern recognition is critical in a broad range of HS tasks, including baggage screening and information analysis. The expert decision maker realizes the importance of having a good representation of the current situation and uses self-monitoring and metacognitive processes to ensure their representations are complete and accurate [44, 45]. For example, expert information analysts are able to assess their understanding of the situation and know the quality of the situation representation they are dealing with. This will prompt them to search for more information or know when they have an understanding that can be used to make a good decision. Expert decision makers manage overwhelming amounts of information by developing automaticity of low level task components as well as specialized memory skills [46, 47]. For a detailed review of the mechanisms of individual expert decision making, see Rosen et al. [33], Ross et al. [48], Phillips et al. [49], and Klein [17].

### 5.2 Teams

Having individual expertise is necessary, but frequently insufficient to ensure high levels of performance in modern organizations and HS. Few decisions are made in isolation from other individuals, and consequently decision making has become a team effort for most people. Just as there are general mechanisms that enable expert individual decision making, teams too develop a set of mechanisms to achieve high levels of effectiveness. Expert teams are defined as "a set of interdependent team members, each of whom possesses a unique and expert level knowledge, skills, and experience related to task performance, and who adapt, coordinate, and cooperate as a team, thereby producing sustainable and repeatable team functioning at superior or at least near-optimal levels of performance" [41, p. 440]. In order to achieve these high levels of performance, members of expert teams develop shared mental models [50]. Shared mental models allow team members to anticipate the needs of their fellow team members and interpret environmental cues in a compatible manner. Expert teams continuously learn from past experiences and adapt their coordination processes to meet changing task demands [51, 52]. To this end, they develop cycles of prebrief $\rightarrow$ performance $\rightarrow$ debrief, wherein team members establish and revise team goals and plans as well as provide developmental feedback to one another [53]. Expert teams have clear roles and responsibilities; everyone knows the part they play and how it fits together with their fellow team members' roles [54]. For example, TSA agents responding to an immediate and high-level threat in an airport terminal should all know what they are responsible for doing and what their fellow team members will be doing. This facilitates coordination of efforts and adaptation to unique situations. Definition of these roles and responsibilities is clear, but they are not rigid. They change, shift, and adapt as necessary; this process is guided by a shared vision and a sense of the team's purpose [55]. Leadership plays a major role in establishing this vision and other critical aspects of expert team decision making, such as providing situation updates, fostering coordination, and self-correcting and modeling a good decision-making performance [56].

## 6 CONCLUDING REMARKS

The NDM approach has already contributed to the understanding of the role of human expertise in HS; hopefully, this is just the beginning with more to come. From baggage screening, to maritime interdictions, to border patrol and intelligence analysis, human expertise and decision making drive the effectiveness of HS operations. The emergent science of NDM and expertise are poised to contribute scientifically based and practically relevant guidance for maximizing performance on HS tasks.

## ACKNOWLEDGMENTS

The views herein are those of the authors and do not necessarily reflect those of the organizations with which they are affiliated or their sponsoring agencies. Research and writing of this article was partially supported by grant number SBE0350345 from the National Science Foundation awarded to Eduardo Salas and Stephen M. Fiore, and by grant number SES0527675 from the National Science Foundation awarded to Glenn Harrison, Stephen M. Fiore, Charlie Hughes, and Eduardo Salas.

## REFERENCES

1. Ross, K. G., Lussier, J. W., and Klein, G. (2005). From the recognition primed decision model to training. In *The Routines of Decision Making*, T. Betsch and S. Haberstroh, Eds. Erlbaum, Mahwah, NJ, pp. 327–341.
2. Crandall, B., Klein, G., and Hoffman, R. R. (2006). *Working Minds: A Practitioner's Guide to Cognitive Task Analysis*. MIT Press, Cambridge, MA.
3. Hutchins, S. G., Pirolli, P. L., and Card, S. K. (2007). What makes intelligence analysis difficult?: A cognitive task analysis. In *Expertise Out of Context*. R. R. Hoffman, Ed. Erlbaum, New York, pp. 281–316.
4. Hoffman, R. R. and Fiore, S. M. (2007). Perceptual (Re)learning: a leverage point for human-centered computing. *IEEE Intell. Syst.* **22**(3), 79–83.
5. Cook, M., Adams, C., and Angus, C. (2007). Intelligence, uncertainty, interpretations and prediction failure. In *Decision Making in Complex Environments*, M. Cooke, J. Noyes, and Y. Masakowski, Eds. Ashgate, Burlington, VT, pp. 389–409.
6. Johnston, R. (2005). *Analytic Culture in the United States Intelligence Community: An Ethnographic Study*. U.S. Government Printing Office, Washington, DC.
7. Hutchins, S. G., Pirolli, P. L., and Card, S. K. (2007). What makes intelligence analysis difficult?: A cognitive task analysis. In *Expertise out of context*, R. R. Hoffman, Ed. Erlbaum, New York, pp. 281–316.
8. Fiore, S. M., Scielzo, S., and Jentsch, F. (2004). Stimulus competition during perceptual learning: training and aptitude considerations in the X-ray security screening process. *Int. J. Cogn. Technol.* **9**(2), 34–39.
9. Cannon-Bowers, J. A. and Salas, E., Eds. (1998). *Making Decisions Under Stress*. American Psychological Association, Washington, DC.
10. Klein, G., Orasanu, J., Calderwood, R., and Zsambok, C. E., Eds. (1993). *Decision Making in Action*. Ablex, Norwood, NJ.

11. Cohen, M. S. (1993). Three paradigms for viewing decision biases. In *Decision Making in Action: Models and Methods*, G. Klein, J. Orasanu, R. Calderwood, and C. E. Zsambok, Eds. Ablex, Norwood, NJ, pp. 36–50.
12. Orasanu, J. and Connolly, T. (1993). The reinvention of decision making. In *Decision Making in Action: Models and Methods*, G. Klein, J. Orasanu, R. Calderwood,and C. E. Zsambok, Eds. Ablex, Norwood, CT, pp. 3–20.
13. Cannon-Bowers, J. A., Salas, E., and Pruitt, J. S. (1996). Establishing the boundaries of a paradigm for decision-making research. *Hum. Factors* **38**(2), 193–205.
14. Lipshitz, R., Klein, G., and Carroll, J. S. (2006). Naturalistic decision making and organizational decision making: exploring the intersections. *Organ. Stud.* **27**(7), 917–923.
15. Zsambok, C. E. (1997). Naturalistic decision making: where are we now? In *Naturalistic Decision Making*, C. E. Zsambok and G. Klein, Eds. Erlbaum, Mahwah, NJ, pp. 3–16.
16. Salas, E. and Klein, G., Eds. (2001). *Linking Expertise and Naturalistic Decision Making*. Erlbaum, Mahwah, NJ.
17. Klein, G. (1998). *Sources of Power: How People Make Decisions*. MIT Press, Cambridge, MA.
18. Lipshitz, R., Klein, G., Orasanu, J., and Salas, E. (2001). Taking stock of naturalistic decision making. *J. Behav. Decis. Making* **14**(5), 331–352.
19. Pruitt, J. S., Cannon-Bowers, J. A., and Salas, E. (1997). In search of naturalistic decisions. In *Decision Making Under Stress: Emerging Themes and Applications*, R. Flin, E. Salas, M. Strub, and L. Martin, Eds. Ashgate, Aldershot, pp. 29–42.
20. Pliske, R. and Klein, G. (2003). The naturalistic decision-making perspective. In *Emerging Perspectives on Judgment and Decision Research*, S. L. Schneider and J. Shanteau, Eds. Cambridge University Press, New York, pp. 559–585.
21. Newell, A. and Simon, H. A. (1972). *Human Problem Solving*. Prentice-Hall, Englewood Cliffs, NJ.
22. Chase, W. G., and Simon, H. A. (1973). Perception in chess. *Cognit. Psychol.* **4**, 55–81.
23. Ericsson, K. A., and Lehmann, A. C. (1996). Expert and exceptional performance: evidence of maximal adaptation to task constraints. *Annu. Rev. Psychol.* **47**, 273–305.
24. Gigerenzer, G., Todd, P. M., and ABC Research Group. (1999). *Simple Heuristics that Make us Smart*. Oxford University Press, Oxford.
25. Simon, H. A. (1996). *The Sciences of the Artificial*, 3rd ed., The MIT Press, Cambridge, MA.
26. Klein, G. (2001). The fiction of optimization. In *Bounded rationality: The Adaptive Toolbox*, G. Gigerenzer and R. Selten Eds. The MIT Press, Cambridge, MA. pp. 103–121.
27. Gigerenzer, G. and Selten, R., Eds. (2001). *Bounded Rationality: the Adaptive Toolbox*. The MIT Press, Cambridge, MA.
28. Todd, P. M., and Gigerenzer, G. (2000). Precis of simple heuristics that make us smart. *Behav. Brain Sci.* **23**, 727–780.
29. Todd, P. M., and Gigerenzer, G. (2001). Putting naturalistic decision making into the adaptive toolbox. *J. Behav. Decis. Mak.* **14**, 353–384.
30. Cannon-Bowers, J. A., Salas, E., and Converse, S. (1993). Shared mental models in expert team decision making. In *Individual and Group Decision Making*, N. J. Castellan Jr., Ed. Erlbaum, Hillsdale, NJ, pp. 221–246.
31. Klimoski, R., and Mohammed, S. (1994). Team mental model: construct or metaphor? *J. Manage.* **20**(2), 403–437.
32. Mohammed, S., and Dummville, B. C. (2001). Team mental models in a team knowledge framework: expanding theory and measure across disciplinary boundaries. *J. Organ. Behav.* **22**(2), 89–103.

33. Rosen, M. A., Salas, E., Lyons, R., and Fiore, S. M. (2008). Expertise and naturalistic decision making in organizations: mechanisms of effective decision making. In *The Oxford Handbook of Organizational Decision Making: Psychological and Management Perspectives*, G. P. Hodgkinson and W. H. Starbuck, Eds. Oxford University Press, Oxford.
34. Schraagen, J. M., Chipman, S. F., and Shalin, V. L., Eds. (2000). *Cognitive Task Analysis*. Erlbaum, Mahwah, NJ.
35. Rosen, M. A., Salas, E., Lazzara, E. H., and Lyons, R. (2007). Cognitive task analysis: methods for capturing and leveraging expertise in the workplace. In *Job Analysis: Studying the World of Work in the 21st Century*, W. Bennett Jr., G. M. Alliger, W. J. Strickland, and J. L. Mitchell, Eds. (under review).
36. Ford, J. K., Schmitt, N., Schechtman, S. L., Hults, B. M., and Doherty, M. L. (1989). Process tracing methods: contributions, problems, and neglected research questions. *Organ. Behav. Hum. Decis. Process.* **43**(1), 75.
37. Klein, G. A., Calderwood, R., and MacGregor, D. (1989). Critical decision method for eliciting knowledge. *IEEE Trans. Syst. Man Cybern.* **19**(3), 462–472.
38. Hutchins, E. (1995). *Cognition in the Wild*. The MIT Press, Cambridge, MA.
39. Hoffman, R. R. and Lintern, G. (2006). Eliciting and representing the knowledge of experts. In *The Cambridge Handbook of Expertise and Expert Performance*, K. A. Ericsson, N. Charness, P. J. Feltovich, and R. R. Hoffman, Eds. Cambridge University Press, Cambridge, pp. 203–222.
40. Ward, P., Williams, A. M., and Hancock, P. A. (2006). Simulation for performance and training. In *The Cambridge Handbook of Expertise and Expert Performance*, K. A. Ericsson, N. Charness, P. J. Feltovich, R. R. Hoffman, Eds. Cambridge University Press, Cambridge, pp. 243–262.
41. Salas, E., Rosen, M. A., Burke, C. S., Goodwin, G. F., and Fiore, S. (2006). The making of a dream team: when expert teams do best. In *The Cambridge Handbook of Expertise and Expert Performance*, K. A. Ericsson, N. Charness, P. J. Feltovich, and R. R. Hoffman, Eds. Cambridge University Press, New York, pp. 439–453.
42. Chi, M. T. H. (2006). Two approaches to the study of experts' characteristics. In *The Cambridge Handbook of Expertise and Expert Performance*, K. A. Ericsson, N. Charness, R. R. Hoffman, P. J. Fletovich, Eds. Cambridge University Press, New York, pp. 21–30.
43. Shanteau, J. (1992). Competence in experts: the role of task characteristics. *Organ. Behav. Hum. Decis. Process.* **53**, 252–266.
44. Randel, J. M., Pugh, H. L., and Reed, S. K. (1996). Differences in expert and novice situation awareness in naturalistic decision making. *Int. J. Hum. Comput. Stud.* **45**(5), 579–597.
45. Orasanu, J. (1990). *Shared Mental Models and Crew Decision Making*, Vol. 46. Cognitive Sciences Laboratory, Princeton University, Princeton, NJ.
46. Ericsson, K. A., and Kintsch, W. (1995). Long-term working memory. *Psychol. Rev.* **102**(2), 211–245.
47. Moors, A., and De Houwer, J. (2006). Automaticity: a theoretical and conceptual analysis. *Psychol. Bull.* **132**(2), 297–326.
48. Ross, K. G., Shafer, J. L., and Klein, G. (2006). Professional judgement and naturalistic decision making. In *The Cambridge Handbook of Expertise and Expert Performance*, K. A. Ericsson, N. Charness, P. J. Feltovich, and R. R. Hoffman, Eds. Cambridge University Press, Cambridge, pp. 403–419.
49. Phillips, J. K., Klein, G., and Sieck, W. R. (2004). Expertise in judgment and decision making: A case for training intuitive decision skills. In *Blackwell Handbook of Judgement and Decision Making*, D. J. Koehler and N. Harvey, Eds. Blackwell Publishing, Victoria, pp. 297–315.

50. Orasanu, J. and Salas, E. (1993). Team decision making in complex environments. In *Decision Making in Action: Models and Methods*, G. A. Klein and J. Oarsaun,Eds. Ablex Publishing, Westport, CT.

51. Edmondson, A. C., Bohmer, R. M., and Pisano, G. P. (2001). Disrupted routines: team learning and new technology implementation in hospitals. *Adm. Sci. Q.* **46**, 685–716.

52. Burke, C. S., Stagl, K., Salas, E., Pierce, L., and Kendall, D. (2006). Understanding team adaptation: a conceptual analysis and model. *J. Appl. Phycol.* **91**(6), 1189–1207.

53. Smith-Jentsch, K., Zeisig, R. L., Acton, B., and McPherson, J. A. (1998). Team dimensional training: a strategy for guided team self-correction. In *Making Decisions Under Stress: Implications for Individual and Team Training*, E. Salas and J. A. Cannon-Bowers, Eds. APA, Washington, DC, pp. 271–297.

54. LaPorte, T. R., and Consolini, P. M. (1991). Working in practice but not in theory: theoretical challenges of "High Reliability Organizations". *J. Public Adm.* **1**(1), 19–48.

55. Castka, P., Bamber, C., Sharp, J., and Belohoubek, P. (2001). Factors affecting successful implementation of high performance teams. *Team Perform. Manage* **7**(7/8), 123–134.

56. Salas, E., Burke, C. S., and Stagl, K. C. (2004). Developing teams and team leaders: strategies and principles. In *Leader development for transforming organizations: Growing Leaders for Tomorrow*, D. Day, S. J. Zaccaro, and S. M. Halpin, Eds. Lawrence Erlbaum Associates, Mahwah, NJ, pp. 325–355.

# CLASSIFICATION AND CLUSTERING FOR HOMELAND SECURITY APPLICATIONS

JIAWEI HAN AND XIAOLEI LI
*University of Illinois at Urbana-Champaign, Champaign, Illinois*

## 1 REPRESENTATION

Proper representation is the first step to utilize methods from classification and clustering [1]. To put it plainly, one has to take information from the real world, the analog world so-to-speak, and store them inside a computer, the digital world. Only after this, classification and clustering algorithms can operate on the real-world problem. This may seem like a simple step, but it can often be the most difficult part of the problem. A proper representation requires an accurate, concise, and static representation of something that can be dynamic and fluid in the real world. And without a good representation, the best algorithms will not be able to operate effectively.

| Color/type | Sedan | SUV | Truck | Motorcycle |
|---|---|---|---|---|
| Red | | | | |
| Green | | *x* | | |
| Blue | | | *y* | |
| Black | | | | |

**FIGURE 1** Feature space with "color" and "type".

To better explain, consider the example of a computer system observing vehicles at a border crossing. The goal of the system might be to automatically flag suspicious vehicles for the border agents to examine more closely. In order for this system to work, the first step is to *represent* the features of the vehicles inside the computer. This is not like how a border agent might describe a vehicle to his or her colleague. Some *features* he or she might use include the vehicle's brand, year, color, size, weight, and so on. The computer system uses a similar process.

Each vehicle is described by a set of features, which make up the so-called *feature space*. This space contains all possible vehicles that can be described by the set of associated features. Figure 1 shows a simple example where there are exactly two features: "color" and "type".

In this two-dimensional feature space shown in Figure 1, vehicles are distinguished only by color and type. Their combinations, which come up to 16, make up the feature space. Each vehicle in the real world can be described by a point in this feature space. A "green sport utility vehicle (SUV)" is point $x$ in Figure 1 and a "blue truck" is point $y$. Points in the feature space are sometimes called "feature vectors," because they can be written out as a vector. For example, $x$ can be written as <"green", "SUV">.

From this example, one might begin to get a sense of the importance of a proper feature space. The two-dimensional feature space in Figure 1 lacks much information valuable to border agents. The "year" and "make" are obvious misses. Without them, the agent will not be able to make an informed decision. At the same time, a feature space that includes everything under the sun is not a brilliant idea either. Suppose the feature space included information such as the fabric type of the seats or whether the vehicle has a CD player. These features are unlikely to have any impact on the decision-making process, but the inclusion of them in the feature might cause unnecessary confusion. To a computer algorithm, these extra features could reduce performance both in terms of accuracy and speed.

## 2 CLASSIFICATION

Classification or supervised learning is a problem from the field of machine learning that aims to learn a function (classifier) that maps a data point to a class label. For example, a data point could be a vehicle and the class label could either be "normal" or "suspicious." By using previously labeled data points, a classifier is able to tune its internal parameters such that in the future, it can correctly label previously unseen data points. Research in

classification mainly focuses on which classifiers to use and how to adjust the parameters inside the classifier.

### 2.1 Basic Concepts

Supervised learning entails the learning of a classifier from training data. The typical classification problem consists of the following components:

1. feature space
2. classification model
3. learning algorithm
4. training data
5. testing data.

The first item, feature space, has already been described in the previous section. To reiterate, it is the representation of the real-world data. The second item, the classification model, is described in detail later in this section. To put it bluntly, it is the brains in the computer that will automatically assign class labels to new objects. The third item, the learning algorithm, is in charge of "tuning" the classification model for optimal performance. Learning algorithms and classification models are often paired together. That is, each classification model has its own unique learning algorithm.

The fourth item, training data, is previously labeled data given to the learning algorithm. Training data consists of labeled data points in the given feature space. Each data point has assigned to it a class label. The set of class labels could either be binary (e.g. "normal" or "suspicious") or $n$-ary (e.g. "normal", "suspicious", "alarming", or "emergency"). With such data, the learning algorithm teaches the classification model how to recognize the features correlated with each different class label. Lastly, the testing data is a separate set of labeled data used to test the performance of the classification model after training. That is, after the classification model has been trained using the training data by the learning algorithm, it is tested using the testing data. The classification model will produce its own class labels for the data points in the testing data. These labels are compared with the true labels and the accuracy is reported back as the classification accuracy. Note that the training data and testing data are two different data sets. It is usually unwise to use the same data set for both training and testing. This leads to the undesirable result of the learning algorithm "over-fitting" the classification model just for the training data and not the general problem.

The training and testing process is similar to how human training occurs. Consider how a new border agent is trained to spot suspicious vehicles at a border crossing. The first few days on the job, he or she is probably trained by a more experienced agent, who teaches him or her the important skills in pinpointing suspicious vehicles. After a while, the new agent can proceed on his or her own after the supervisor is satisfied with his or her performance. The analogy to machine learning is something like the following. The new border agent is the classification model. Initially, it has a "blank" brain and does not really know how to identify suspicious behavior. The more experienced agent can be viewed as the learning algorithm since it teaches the new agent the knowledge required for the job. During the teaching process, the examples the experienced agent might use to teach the new agent are the training data. And finally, the supervisor might evaluate the new agent on some new cases, which are the testing data.

| Color/type | Sedan | SUV | Truck | Motorcycle |
|---|---|---|---|---|
| Red | | | | |
| Green | | *x* | | |
| Blue | | | *y* | |
| Black | | | | |

**FIGURE 2** Feature space with decision boundary for vehicles with four or more wheels versus vehicles with less than four wheels.

### 2.2 Classification Model

So far, the description of a classification model has largely been a black box. Somehow, it is able to put a class label on an object after some training. The exact method of how a model is able to do this depends on the classification model, but the general ideas are common across all models. A brief overview is given in this section.

At a high level, a classification model simply divides the feature space such that data points of different classes fall into separate regions. This division is sometimes called the *classification* or *decision boundary*. Figure 2 shows a classification boundary in the feature space of Figure 1 if the problems were to differentiate vehicles with four wheels or more versus vehicles with less than four wheels. The red decision boundary divides the feature space in a way such that all vehicles with four wheels or more are on the left-hand side of the boundary, while vehicles with less than four wheels are on the right-hand side. Points $x$ and $y$ fall on the left-hand side of the boundary. Given a decision boundary or possibly a set of them, classification on a new object is easy. One just has to find out which side of the boundary the object resides in and make the appropriate decision.

The role of the learning algorithm is to find the decision boundary for the given classification model and training data. Recall that points in the training data are labeled. Using these labels, the learning algorithm adjusts the decision boundary of the classification such that points of different class labels lie on different sides of the boundary. In practice, finding the perfect decision boundary is often impossible. There is usually no clear boundary that can clearly separate the data points of different classes. Because of noise or just the inherent difficulty of the problem, some training data will lie on the incorrect side. It is the duty of the learning algorithm to position the decision boundary such that this error is minimized.

### 2.3 Types of Classifiers

In the previous section, the classifier was discussed in general terms: it learns a decision boundary in the feature space. In practice, this could take shape in many forms. The "boundary" can be a line, a square, or any other shape. Different classifiers use different types of boundaries, and some boundaries might be more effective than others depending on the problem. There is no universal best. Furthermore, different classifiers use different learning algorithms to adjust its decision boundary. These algorithms have different characteristics as well. With respect to efficiency, some scale very nicely with the number of features and others scale very nicely with the number of points in the training data.

In the next few paragraphs, several popular classifiers are discussed.

***2.3.1 Decision Tree.*** Decision trees, one of the most basic and intuitive classifiers, are both accurate and easy to use. A decision tree's decision boundary is essentially a list of rules where each rule is a set of conditions. If a data object matches the conditions in the rule, then it is labeled according to the rule. For example, "Color = Black AND Type = SUV → Suspicious" could be a rule. In this case, all black SUVs would be labeled as suspicious. With these rules, the classifier can either make the decision automatically or the rules can be given to human agents for training [2].

Learning these rules is also relatively straightforward. The details are beyond the scope of this article but the intuitions are as follows. The classifier starts with a blank rule, that is, it applies to all data objects. Then, for every feature and its set of feature values, the classifier checks how useful it is with regard to classification. The measure of usefulness comes from information theory, and it essentially measures how discriminative it is alone at separating data points in the training set according to their class labels. The feature value that is most useful according to this measure is then added to the empty rule. At this point, this rule has split the training data, so the process continues recursively within each split.

There are many different decision tree algorithms but all of them basically work from the principles given above. Some of the more advanced techniques involve how to better measure the usefulness of a feature value and how to consolidate many rules together such that they are more accurate in the general case.

***2.3.2 Naïve Bayes.*** Bayes' rule is a basic equation from probability theory. Roughly speaking, it states that the probability of an event A conditional on another event B is related to event B conditional on A. If one lets A represent the event that an object is suspicious and B represent the event that feature $X$ is present, Bayes' rule would state the following: An object being suspicious conditional on feature $X$ is related to feature $X$ conditional on a suspicious object. From the training data, one can gather "evidence" on how often a suspicious object exhibits feature X. Then, through Bayes' rule, the same evidence can be used to guess how likely an object is suspicious given that it exhibits feature $X$ [2].

This describes how a single feature can be used to decide the class label. When there are multiple features, the same process is repeated independently and the final classification decision is a simple combination of them all. This independent feature assumption is often not true in the real world but it is used for the sake of simplifying the problem and making learning tractable.

***2.3.3 Support Vector Machine.*** In recent years, support vector machines (SVMs) have become the classifier of choice for many researchers. It has been shown to be more efficient and accurate when there are many features to consider (for example, text classification). It works by positioning its decision boundary in the feature space as close to the "middle" as possible. The intuition is that this boundary will work the best for future data points. In cases where a simple linear decision boundary cannot be found, SVMs can project the data points to a feature space with more dimensions such that it can be [3].

### 2.4 Applications of Classification in Homeland Security

The running example of labeling an object as being normal or suspicious is the most natural application of automated classification. The set of class labels does not have to be binary; there could be many classes. For instance, each class could be a different level of

alarm. Further, the object in question could be anything; the only question would be how to represent the object in a feature space. For example, if the object is a vehicle, some features would be the brand of the vehicle, the size of the vehicle, the license number, the year of the vehicle, the speed of travel, and so on. If the object is a person, some features would be age, height, hair color, and maybe other background information. If the object is a cargo container, some features would be the owner of the container, the source of the container, the destination, and so on.

The representation of a real-world problem as a classification problem is not difficult. Often, human beings already make these classification decisions; the only difference would be replacing a human by a classifier. However, there are two major issues that often prevent a classifier from being deployed. First and foremost, the exact representation and extraction of features of the object are difficult task. A person might look at a vehicle and say that it is a red truck; however, for an automated camera system to make that same decision is difficult. Any feature that requires the system to visually identify something is difficult. Although the most advanced vision algorithms can achieve a great degree of precision, 100% accuracy is still unreachable. Additionally, the "sixth sense" that humans have is simply impossible to represent in machine form.

Second, in order to train a classifier, training data must exist. A set of data points that have the correct class labels must be given to the classifier so that it can learn the right decision boundaries. In humans, this corresponds to experience one person might pass to another. In machines, this set of training data can be hard to obtain. Employee training programs might have case studies for training new hires, but they hardly cover the entire gambit of cases. Further, in many real-world "classification" problems, the answer is not always black-and-white. To translate such scenarios to a discrete world of machine learning is not always straightforward. All these problems make obtaining clean training data a tricky problem. And just like a new employee, without proper training, a classifier can never reach its full potential.

### 2.5 Semisupervised Learning

Supervised learning's paradigm is that there is a set of labeled data that is presented to the classifier for training. As mentioned, this is often difficult to achieve in practice. Labeled data might be very hard to obtain or simply may not exist. If there are too few training examples, the classifier will not be able to learn the correct decision boundary. However, there are many cases where unlabeled data exist in abundance. In these situations, semisupervised learning is more appropriate. In this new paradigm, the human user is involved in the training process of the classifier. For instance, the classifier might ask the user to classify a few data points that it finds difficult to process. The goal is for the classifier to maximize its learning while minimizing the number of interactions it must have with the human.

Semisupervised learning can often achieve better accuracy than supervised learning because it essentially has more training data. Further, these additional training data are selected based on their usefulness to the classifier. However, it does require more human intervention.

### 2.6 Incremental Learning

So far, the discussion has been focused on a classical learning system where all the training data are presented up front. Once the training is complete, the classifier is

"fixed." To borrow from the human learning analogy one more time, this learn-once paradigm is definitely untrue for humans. As new experiences and evidences become available, one would continuously readjust his or her thinking. For this paradigm, there are some classifiers that can do what is called *incremental learning* or *lifetime learning*. When new evidence becomes available, the classifier can consolidate it with its previous knowledge. This is more efficient than starting from scratch (that is, combine the new evidence with previous evidence and retrain from scratch).

## 3 CLUSTERING

Clustering or unsupervised learning is another problem from the field of machine learning. Compared to classification, the most obvious difference is that there are no longer training examples given. In other words, there is no supervision to guide the learning of parameters in the function. This is often the case in the real world where no labels are available. Clustering algorithms allow the user to see some natural groupings of data to gain some insight.

### 3.1 Basic Clustering Concepts

Much like classification, data points are first put into a feature space. Figure 3 shows a sample two-dimensional feature space with some points in it. The goal of clustering is to find natural groupings (clusters) of data points in this space. It is quite obvious in Figure 3 that there are two clusters. In fact, an automated clustering algorithm is likely to find them as well. In situations where the user knows very little about the data set, clustering can often reveal interesting information.

Just like classification, choosing of features is an important step. The same challenges there exist as here; however, there is one additional issue clustering has to consider. That is, how does one define similarity between two objects? This is known as the *similarity measure* in clustering. Theoretically, similar objects should be in the same cluster and dissimilar ones should be in different clusters. Therefore, the similarity measure is crucial in forming the right clustering. In Figure 3, the similarity function is the Euclidean distance between points. This is very natural in applications where data points represent physical locations. For example, if one wants to cluster all the gas stations in a city, Euclidean distance would be a good fit. However, in other situations, the similarity measure is tricky to choose. For example, suppose one is clustering the following three people: John, Jane, and Mary. If the similarity measure is the edit distance between the text string, John and Jane would likely be in one cluster and Mary be in another.

| Color/type | Sedan | SUV | Truck | Motorcycle |
|---|---|---|---|---|
| Red | $x_1$ | $x_2$ | | |
| Green | $x_3$ | $x_4$ | | |
| Blue | | | $y_1$ | $y_2$ |
| Black | | | $y_3$ | |

**FIGURE 3** Feature space with "color" and "type".

However, if the similarity measure is the gender of the person, Jane and Mary would be in one cluster (female) and John would be in his own cluster. Clearly, the similarity measure is highly application-specific and should be chosen with careful consideration.

With a similarity measure defined, one can then choose from a plethora of clustering algorithms. In other words, the choosing of the similarity measure and the clustering algorithm is somewhat independent. Both are important decisions and can affect the final outcome in many different ways.

### 3.2 Types of Clustering Algorithms

There are many types of clustering algorithms. Giving a single global taxonomy of all clustering algorithms would be impossible. There are, however, some properties that distinguish one from another.

Some of the basic clustering algorithms fall into the Partitioning group. The idea is to partition a data set into $k$ distinct groups. K-means and K-medoids are the classical examples in this. K-means is probably the most popular clustering algorithm [2]. It works as follows. Given a data set, it first randomly chooses $k$ points to be the centers of clusters, otherwise known as centroids. The value of $k$ is given in advance to the algorithm. Then, for all points in the data set, it is assigned to the closest centroid. This partitions the data into $k$ clusters, though it is rather random since the centroids are chosen randomly. Then, for each cluster, the algorithm recomputes a new centroid by taking the "average" or "mean" of all points that belong to that cluster. With these new centroids, all points in the data set are reassigned to their closest centroid. This process iterates until some stopping criterion, which could be when the recomputation of centroids does not alter their positions anymore. Though this process might seem rather random (the initial $k$ centroids are randomly chosen), it is guaranteed theoretically to converge.

The K-means algorithm and the similar K-medoids form the foundation of many clustering algorithms. It is relatively efficient and works quite well when the clusters are compact and isolated. It does, however, have several weaknesses. First and foremost, the value of $k$ is an input to the algorithm. The user must have some prior clue about the distribution of data. Although many works have focused on automatic selection of $k$, the results are still not perfect. Secondly, to compute the "average" of a cluster, numerical values are assumed. Many real-world data sets have categorical features that do not have an easy definition of average. Thirdly, outliers and noise can often confuse the algorithms to form unnatural clusters.

Another class of clustering algorithms is density-based clustering. As the name suggests, the density of data points at a local region dictate how clusters are formed. This has several advantages. First, clusters of arbitrary shapes can be formed. In partitioning algorithms, the distance metric or similarity measure often restricts the cluster shape. For example, using the Euclidean distance in K-means restricts cluster shapes to spheres. Secondly, density-based clustering is more robust with respect to noise. In it, the point in the upper-right corner is designated an outlier because its local region is sparse. A partitioning algorithm would either assign it to its own cluster or to a near-by cluster, thus stretching a cluster unnecessarily.

One of the first density-based clustering algorithms is DBSCAN [4]. It works as follows. Instead of defining the distance between two points in space as the Euclidean distance, it is defined as being "density-connected." Without going into the details, it roughly means that two points are either close to each other or connected via a sequence

of points that are also close to each other. While observing some other parameters, DBSCAN simply follows chains of density-connected points and mark each chain as being its own cluster. If a point is not density-connected to any other point, it is marked as an outlier.

Partitioning and density-based clustering algorithms produce "flat" clusters. That is, clusters are equal with respect to another. But in many real-world applications, a hierarchical structure to the clusters is more applicable. For example, shoes, socks, and boots might be clustered together in the "footwear" cluster, but the "footwear" cluster would belong to the apparel cluster, and so forth. This hierarchy makes organization easier and is often more natural. The very basic hierarchical clustering algorithm is called *hierarchical agglomerative clustering*. It starts by assigning each data point to its own cluster (or after some basic clustering). Then, the most similar pair of clusters is merged together. This process iterates until all original clusters are in the same cluster. The intermediate merge paths then form a binary hierarchy. One major issue in this algorithm is defining similarity between clusters. Two competing choices are single link and complete link. Single link uses the minimum of all similarity measures between a pairs of points between the two clusters and complete link uses the maximum. The choice between the two and possibly others is largely application dependent.

Lastly, we briefly examine one clustering algorithm that is particularly adept at dealing with large data sets. Algorithms like K-means or DBSCAN are only efficient up to a point. If there are millions or billions of data points, running K-means could require hours or days of computation. To this end, BIRCH was invented to handle very large data sets [4]. It works by the principle of "microclustering." That is, if a set of points is in a very tight cluster, they can essentially be treated as a single point or microcluster. The microclusters would then replace the original big data set and be presented to a clustering algorithm as input. The idea is that the number of microclusters is much smaller than the number of raw data points, and thus clustering can be completed in a reasonable time. Constructing microclusters is fairly straightforward. It relies basically on a user-defined maximum radius threshold. If the circle formed by a set of points has a radius smaller than the threshold, it is marked as a microcluster. Otherwise, points are redistributed to new microclusters such that the threshold value is not violated. After the microclusters are constructed, any other clustering algorithm can be run on top of it.

### 3.3 Outlier Detection

Related to clustering is outlier detection. One sometimes views it as a by-product of clustering. That is, if a cluster contains very few data points, it is regarded as an outlying cluster. This by-product can sometimes be gotten with no extra effort on the clustering algorithm; however, some assert that a dedicated outlier detection algorithm is better suited. One such algorithm is based on DBSCAN. Essentially, data points that are not density-connected to other points are marked as outliers.

### 3.4 Applications of Clustering to Homeland Security

Clustering is often applied to data about which little is known. It gives the user some preliminary ideas about some natural groupings in the data. The same case is true in homeland security. When there is so much data that one cannot make sense of it, clustering is helpful in shedding some light. For instance, clustering all vehicles at a busy border crossing can be helpful in dividing workload.

More applicable to homeland security is outlier detection. The majority of objects in question are normal and only a very subset is abnormal. In the border crossing example, the vast majority of vehicles are normal ones. The goal of the border agent is to seek out the small minority that is abnormal. This fits the model of outlier detection very well and is likely the common problem in homeland security.

## 4 FEATURE SELECTION

As mentioned previously, representation is just as important, if not more so, than the actual learning of the classifier. Consider the learning of a classifier for labeling the color of a vehicle. This is trivial if color is in the feature space; however, if it were not, the problem would be impossible regardless of the classifier. In this case, the feature space is not rich enough to capture the discriminating features. One might suggest to just throw all possible features to the classifier and might allow the classifier decide which ones are useful. This can also be problematic due to time constraints; a classifier could take an unrealistic amount of time to tune its parameters.

To this end, there is a field of research called *feature selection* that deals with this exact problem. Given a set of features, a feature selection algorithm chooses a subset, which can be just as good, if not better, than the full feature space with regard to classification accuracy. For instance, if the classifier is to label the color of a vehicle, the "number of wheels" feature can probably be dropped from the feature space. A properly pruned feature space can make the learning more efficient and also more accurate. A common approach is to rank the features according to some goodness measure and select the best features one-by-one until some stopping criteria is satisfied.

## REFERENCES

1. Russell, S. and Norvig, P. (2002). *Artificial Intelligence, A Modern Approach*, 2nd ed. Prentice Hall, NJ.
2. Mitchell, T. (1997). *Machine Learning*. McGraw-Hill, Columbus, OH.
3. Cristianini, N. and Shawe-Taylor, J. (2000). *An Introduction to Support Vector Machines and Other Kernel-based Learning Methods*. Cambridge University Press, Cambridge, UK.
4. Han, J. and Kamber, M. (2005). *Data Mining, Concepts and Techniques*, 2nd ed. Morgan Kaufmann, San Francisco.

## FURTHER READING

Bishop, C. M. (2007). *Pattern Recognition and Machine Learning*. Springer, New York, NY.

Duda, R. O., Hart, P. E., and Stork, D. G. (2000). *Pattern Classification*, 2nd ed. Wiley-Interscience; New York, NY.

Hastie, T., Tibshirani, R., and Friedman, J. H. (2003). *The Elements of Statistical Learning*. Springer, New York, NY.

Kearns, M. J. and Vazirani, U. V. (1994). *An Introduction to Computational Learning Theory*. MIT Press, Cambridge, MA.

Witten, I. H. and Frank, E. (2005). *Data Mining: Practical Machine Learning Tools And Techniques*, 2nd ed. Morgan Kaufmann, San Francisco.

# EXPERIENCE WITH EXPERT JUDGMENT: THE TU DELFT EXPERT JUDGMENT DATA

ROGER M. COOKE
*Department of Mathematics, Delft University of Technology, Delft, The Netherlands*
LOUIS L.H.J. GOOSSENS
*Department of Safety Science, Delft University of Technology, Delft, The Netherlands*

## 1 INTRODUCTION

The pros and cons of different weighting schemes remain a subject of research [1, 4]. The European Union (EU) contracted the TU Delft to review its applications both within EU projects, and elsewhere, in which experts assessed variables in their field of expertise for which the true values are known, in addition to variables of interest [3–6]. These are called *seed*, or *calibration*, variables. Since then, the TU Delft expert judgment database has nearly doubled. We now have studies involving over 67,000 experts' subjective probability distributions. The main sectors and summary information are given in Table 1.

The authors believe that this database represents a unique source from which much can be learned regarding the application of structured expert judgment in quantitative decision support. The entire data, appropriately anonymized, may be obtained from the

**TABLE 1 Summary of Applications per Sector**

| Sector | Number of Experts | Number of Variables | Number of Elicitations |
|---|---|---|---|
| Nuclear applications | 98 | 2,203 | 20,461 |
| Chemical and gas industry | 56 | 403 | 4,491 |
| Groundwater/water pollution/dike ring/barriers | 49 | 212 | 3,714 |
| Aerospace sector/space debris/aviation | 51 | 161 | 1,149 |
| Occupational sector: ladders/buildings (thermal physics) | 13 | 70 | 800 |
| Health: bovine/chicken (*Campylobacter*)/SARS | 46 | 240 | 2,979 |
| Banking: options/rent/operational risk | 24 | 119 | 4,328 |
| Volcanoes/dams | 231 | 673 | 29,079 |
| Rest group | 19 | 56 | 762 |
| *In total* | *521* | *3,688* | *67,001* |

first author. It is hoped that others will use this data to further develop methods for using structured expert judgment.

We assume that uncertainty is represented as subjective probability and concerns results of possible observations. For a discussion of foundational issues, the reader is referred to [7]. Section 2 discusses goals of a structured expert judgment study; Section 2 provides an explanation of the concepts and methods underlying the Delft expert judgment method. Section 3 gives an updated summary of the results, comparing equal weighting with performance-based weighting and with the best expert. Section 4 discusses seed variables and robustness, and Section 5 is devoted to lessons learned and anecdotal information, common pitfalls, and misconceptions. A concluding section identifies possible topics for future research.

## 2 STRUCTURED EXPERT JUDGMENT

Expert judgment is sought when substantial scientific uncertainty impacts a decision process. Because there is uncertainty, the experts themselves are not certain and hence will typically not agree. Informally soliciting expert's advice is not new. *Structured* expert judgment refers to an attempt to subject the decision process to transparent methodological rules, with the goal of treating expert judgments as scientific data in a formal decision process. The process by which experts come to agree is the scientific method itself. Structured expert judgment cannot preempt this role and therefore cannot have expert agreement as its goal. We may broadly distinguish three different goals to which a structured judgment method may aspire:

- Census
- Political consensus
- Rational consensus.

A study aiming at *census* will simply try to survey the distribution of views across an expert community. An illustration of this goal is found in the *Nuclear Regulatory Commission's Recommendations for Probabilistic Seismic Hazard Analysis: Guidance on Uncertainty and Use of Experts:*

> "To represent the overall community, if we wish to treat the outlier's opinion as equally credible to the other panelists, we might properly assign a weight (in a panel of 5 experts) of 1/100 to his or her position, not 1/5" (NUREG/CR-6372 [8], p. 36)

The goal of "representing the overall community" may in this view lead to a differential weighting of experts' views according to how representative they are of other experts. A similar goal is articulated in [9]. The philosophical underpinnings of this approach are elaborated in Budnitz et al. [10]. Expert agreement on the representation of the overall community is the weakest, and most accessible, type of consensus to which a study may aspire. Agreement on a "distribution to represent a group", agreement on a distribution, and agreement on a number are the other types of consensus, in decreasing accessibility.

*Political consensus* refers to a process in which experts are assigned weights according to the interests or stakeholders they represent. In practice, an equal number of experts

from different stakeholder groups would be placed and given equal weight in an expert panel. In this way the different groups are included equally in the resulting representation of uncertainty. This was the reasoning behind the selection of expert panels in the EU-USNRC accident consequence studies with equal weighting [11].

*Rational consensus* refers to a group decision process. The group agrees on a method according to which a representation of uncertainty will be generated for the purposes for which the panel was convened, without knowing the result of this method. It is not required that each individual member adopt this result as his/her personal degree of belief. This is a form of agreement on a distribution to represent a group. To be rational, this method must comply with necessary conditions devolving from the general scientific method. Cooke [1] formulated the necessary conditions or principles that any method warranting the predicate "science" should satisfy:

- *Scrutability/accountability.* All data, including experts' names and assessments, and all processing tools are open to peer review and results must be reproducible by competent reviewers.
- *Empirical control.* Quantitative expert assessments are subject to empirical quality controls.
- *Neutrality.* The method for combining/evaluating expert opinion should encourage experts to state their true opinions, and must not bias results.
- *Fairness.* Experts are not prejudged, before processing the results of their assessments.

Thus, a method which satisfies these conditions and to which the parties precommit is proposed. The method is applied and after the result of the method is obtained, parties wishing to withdraw from the consensus incur a burden of proof. They must demonstrate that some heretofore unmentioned necessary condition for rational consensus has been violated. If they fail to demonstrate, their dissent is "irrational". Of course any party may withdraw from the consensus because the result is hostile to his or her interests—this is not rational dissent and does not threaten rational consensus.

The requirement of empirical control will strike some as peculiar in this context. How can there be empirical control with regard to expert subjective probabilities? To answer this question, we must reflect on the question "when is a problem an expert judgment problem?" We would not have recourse to expert judgment to determine the speed of light in a vacuum. This is physically measurable and has been measured to everyone's satisfaction. Any experts we query would give the same answer. Nor do we consult expert judgment to determine the proclivities of a god. There are no experts in the operative sense of the word for this issue. A problem is susceptible for expert judgment only if there is relevant scientific expertise. This entails that there are theories *and* measurements relevant to the issues at hand, but that the quantities of interest themselves cannot be measured in practice. For example, toxicity of a substance for humans is measurable in principle, but is not measured for obvious reasons. However, there are toxicity measurements for other species, which might be relevant to the question of toxicity in humans. Other examples are given in Section 4. If a problem is an expert judgment problem, then necessarily there will be relevant experiments or measurements. Questions regarding such experiments can be used to implement empirical control. Studies indicate that performance on the so-called almanac questions does not predict performance on the variables in an expert's field of expertise [12]. The key question regarding seed variables is as follows: Is performance on

seed variables judged relevant to performance on the variables of interest? For example, should an expert who gave very overconfident off-mark assessments on the variables for which we know the true values be equally influential on the variables of interest as an expert who gave highly informative and statistically accurate assessments? That is indeed the choice that often confronts a problem owner after the results of an expert judgment study are in. If seed variables in this sense cannot be found, then rational consensus is not a feasible goal and the analyst should fall back on one of the other goals.

The above mentioned definition of "rational consensus" for group decision processes is evidently on a very high level of generality. Much work has gone into translating this into a workable procedure that gives good results in practice. This workable procedure is embodied in the "classical model" of Cooke [1] described in the following section.

Before going into details, it is appropriate to say something about Bayesian approaches. Since expert uncertainty concerns experts' subjective probabilities, many people believe that expert judgment should be approached from the Bayesian paradigm. This paradigm, recall, is based on the representation of preference of a rational individual in terms of maximal expected utility. If a Bayesian is given experts' assessments on variables of interest and on relevant seed variables, then (s)he may update themselves on the variables of interest by prior conditionalizing on the given information. This requires that the Bayesian formulates his/her joint distribution over

- the variables of interest;
- the seed variables;
- the experts' distributions over the seed variables and the variables of interest.

Issues that arise in building such a model are discussed in Cooke [1]. Suffice to say here that a group of rational individuals is not itself a rational individual, and group decision problems are notoriously resistant to the Bayesian paradigm.

## 3 THE CLASSICAL MODEL

The above principles have been operationalized in the so-called classical model, a performance-based linear pooling or weighted averaging model [1, 13]. The weights are derived from experts' calibration and information scores, as measured on seed variables. Seed variables serve a threefold purpose:

1. to quantify experts' performance as subjective probability assessors;
2. to enable performance-optimized combinations of expert distributions; and
3. to evaluate and hopefully validate the combination of expert judgments.

The name "classical model" is derived from an analogy between calibration measurement and classical statistical hypothesis testing. It contrasts with various Bayesian models.

The performance-based weights use two quantitative measures of performance, *calibration* and *information*. Loosely, calibration measures the statistical likelihood that a set of experimental results correspond, in a statistical sense, with the expert's assessments. Information measures the degree to which a distribution is concentrated.

These measures can be implemented for both discrete and quantile elicitation formats. In the discrete format, experts are presented with uncertain events and perform their elicitation by assigning each event to one of several predefined probability bins, typically 10, 20, . . . , 90%. In the quantile format, experts are presented with an uncertain quantity taking values in a continuous range, and they give predefined quantiles, or percentiles, of the subjective uncertainty distribution, typically 5, 50, and 95%. The quantile format has distinct advantages over the discrete format, and all the studies reported below use this format. In five studies, the 25 and 75% quantiles were also elicited. To simplify the exposition, we assume that the 5, 50, and 95% values were elicited.

### 3.1 Calibration

For each quantity, each expert divides the range into four interquantile intervals for which his/her probabilities are known, namely $p_1 = 0.05$: less than or equal to the 5% value, $p_2 = 0.45$: greater than the 5% value and less than or equal to the 50% value, and so on.

If $N$ quantities are assessed, each expert may be regarded as a statistical hypothesis, namely, that each realization falls in one of the four interquantile intervals with probability vector

$$p = (0.05, 0.45, 0.45, 0.05)$$

Suppose we have realizations $x_1, \ldots, x_N$ of these quantities. We may then form the sample distribution of the expert's interquantile intervals as

$$\begin{aligned} s_1(e) &= \#\{i | x_i \leq 5\% \text{ quantile}\}/N \\ s_2(e) &= \#\{i | 5\% \text{ quantile} < x_i \leq 50\% \text{ quantile}\}/N \\ s_3(e) &= \#\{i | 50\% \text{ quantile} < x_i \leq 95\% \text{ quantile}\}/N \\ s_4(e) &= \#\{i | 95\% \text{ quantile} < x_i\}/N \\ s(e) &= (s_1, \ldots, s_4) \end{aligned}$$

Note that the sample distribution depends on the expert $e$. If the realizations are indeed drawn independently from a distribution with quantiles as stated by the expert, then the quantity

$$2N I(s(e)|p) = 2N \Sigma_{i=1,\ldots,4}\ s_i \ln(s_i/p_i) \tag{1}$$

is asymptotically distributed as a chi-square variable with 3 degrees of freedom. This is the so-called likelihood ratio statistic and $I(s|p)$ is the relative information of distribution $s$ with respect to $p$. If we extract the leading term of the logarithm, we obtain the familiar chi-square test statistic for goodness of fit. There are advantages in using the form in Eq. (1) Cooke [1].

If after a few realizations the expert were to see that all realizations fell outside his 90% central confidence intervals, he/she might conclude that these intervals were too narrow and might broaden them on subsequent assessments. This means that for this expert the uncertainty distributions are not independent, and he/she learns from the realizations. Expert learning is not a goal of an expert judgment study and his/her joint distribution

is not elicited. Rather, the decision maker (DM) wants experts who do not need to learn from the elicitation. Hence, the DM scores expert $e$ as the statistical likelihood of the hypothesis. *$H_e$: the interquantile interval containing the true value for each variable is drawn independently from probability vector $p$.*

A simple test for this hypothesis uses the test statistic (Eq. (1)), and the likelihood, or $p$ value, or calibration score of this hypothesis, is

$$\text{Calibration score}(e) = p \text{ value} = \text{Prob}\{2NI(s(e)|p) \geq r|H_e\}$$

where $r$ is the value of Eq. (1) based on the observed values $x_1, \ldots, x_N$. It is the probability under hypothesis $H_e$ that a deviation at least as great as $r$ should be observed on $N$ realizations if $H_e$ were true. Calibration scores are absolute and can be compared across studies. However, before doing so, it is appropriate to equalize the power of the different hypothesis tests by equalizing the effective number of realizations. To compare scores on two data sets with $N$ and $N'$ *realizations*, we simply use the minimum of $N$ and $N'$ in Eq. (1), without changing the sample distribution $s$. In some cases involving multiple realizations of one and the same assessment, the effective number of seed variables is based on the number of assessments and not the number of realizations.

Although the calibration score uses the language of simple hypothesis testing, it must be emphasized that we are not rejecting expert hypotheses; rather we are using this language to measure the degree to which the data supports the hypothesis that the expert's probabilities are accurate. Low scores, near zero, mean that it is unlikely that the expert's probabilities are correct.

### 3.2 Information

The second scoring variable is information. Loosely, the information in a distribution is the degree to which the distribution is concentrated. Information cannot be measured absolutely, but only with respect to a background measure. Being concentrated or "spread out" is measured relative to some other distribution. Generally, the uniform and log-uniform background measures are used (other background measures are discussed in Yunusov et al. [14].

Measuring information requires associating a density with each quantile assessment of each expert. To do this, we use the unique density that complies with the experts' quantiles and is minimally informative with respect to the background measure. This density can easily be found with the method of Lagrange multipliers. For a uniform background measure, the density is constant between the assessed quantiles, and is such that the total mass between the quantiles agrees with $p$. The background measure is not elicited from experts as indeed it must be the same for all experts; instead it is chosen by the analyst.

The uniform and log-uniform background measures require an *intrinsic range* on which these measures are concentrated. The classical model implements the so-called $k\%$ overshoot rule: for each item we consider the smallest interval $I = [L, U]$ containing all the assessed quantiles of all experts and the realizations, if known. This interval is extended to

$$I^* = [L^*, U^*]; L^* = L - k(U - L)/100; U^* = U + k(U - L)/100$$

The value of $k$ is chosen by the analyst. A large value of $k$ tends to make all experts look quite informative, and tends to suppress the relative differences in information scores. The information score of expert $e$ on assessments for uncertain quantities $1, \ldots, N$ is

$$\text{Information Score}(e) = \text{Average relative information with respect to background}$$
$$= (1/N)\Sigma_{i=1,\ldots,N} I(f_{e,i}|g_i)$$

where $g_i$ is the background density for variable $i$ and $f_{e,i}$ is expert $e$'s density for item $i$. This is proportional to the relative information of the expert's joint distribution given the background, under the assumption that the variables are independent. As with calibration, the assumption of independence here reflects a desideratum of the DM and not an elicited feature of the expert's joint distribution. The information score does not depend on the realizations. An expert can give himself a high information score by choosing his quantiles very close together.

Evidently, the information score of $e$ depends on the intrinsic range and on the assessments of other experts. Hence, information scores cannot be compared across studies.

Of course, other measures of concentratedness could be contemplated. The above information score is chosen because it is

- familiar
- tail insensitive
- scale invariant
- slow.

The latter property means that relative information is a slow function; large changes in the expert assessments produce only modest changes in the information score. This contrasts with the likelihood function in the calibration score, which is a very fast function. This causes the product of calibration and information to be driven by the calibration score.

### 3.3 Decision Maker

A combination of expert assessments is called a *decision maker*. All DMs discussed here are examples of linear pooling. For a discussion of pros and cons of the linear pool, see Refs [1, 2, 15, 16]. The classical model is essentially a method for deriving weights in a linear pool. "Good expertise" corresponds to good calibration (high statistical likelihood, high $p$ value) and high information. We want weights that reward good expertise and that pass these virtues on to the DM.

The reward aspect of weights is very important. We could simply solve the following optimization problem: find a set of weights such that the linear pool under these weights maximizes the product of calibration and information. Solving this problem on real data, we have found that the weights do not generally reflect the performance of the individual experts. An example of this is given in Section 4.

As we do not want an expert's influence on the DM to appear haphazard, and we do not want to encourage experts to game the system by tilting their assessments to achieve a desired outcome, we must impose a strictly scoring rule constraint on the weighing

scheme. Roughly, this means that an expert achieves his/her maximal expected weight only by stating assessments in conformity with his/her true beliefs.

Consider the following score for expert $e$:

$$w_\alpha(e) = 1_\alpha(\text{calibration score}) \times \text{calibration score}(e) \times \text{information score}(e) \quad (2)$$

where $1_\alpha(x) = 0$ if $x < \alpha$ and $1_\alpha(x) = 1$ otherwise. Cooke [1] showed that Eq. (2) is asymptotically a strictly proper scoring rule for average probabilities. This means the following: suppose an expert has given his quantile assessments for a large number of variables and subsequently learns that his/her judgments will be scored and combined according to the classical model. If (s)he were then given the opportunity to change the quantile values (e.g. the numbers 5, 50, or 95%) in order to maximize the expected weight, the expert would choose values corresponding to his/her true beliefs. Note that this type of scoring rule scores a set of assessments on the basis of a set of realizations. Scoring rules for individual variables were found unsuitable for purposes of weighting, for more details the reader is referred to Cooke [1].

The scoring rule constraint requires the term $1_\alpha$*(calibration score)*, but does not say what value of $\alpha$ we should choose. Therefore, we choose $\alpha$ so as to maximize the combined score of the resulting DM. Let $\text{DM}_\alpha(i)$ be the result of linear pooling for item $i$ with weights proportional to Eq. (2):

$$\text{DM}_\alpha(i) = \Sigma_{e=1,\ldots,E}\ w_\alpha(e) f_{e,i} / \Sigma_{e=1,\ldots,E}\ w_\alpha(e) \quad (3)$$

The *global weight* DM is $\text{DM}_{\alpha^*}$ where $\alpha^*$ maximizes

$$\text{calibration score}(\text{DM}_a) \times \text{information score}(\text{DM}_\alpha) \quad (4)$$

This weight is termed global because the information score is based on all the assessed seed items.

A variation on this scheme allows a different set of weights to be used for each time. This is accomplished by using information scores for each item rather than the average information score:

$$w_\alpha(e, i) = 1_\alpha(\text{calibration score}) \times \text{calibration score}(e) \times I(f_{e,i} | g_i) \quad (5)$$

For each $\alpha$ we define the item weight $\text{DM}_\alpha$ for item $i$ as

$$\text{IDM}_\alpha(i) = \Sigma_{e=1,\ldots,E}\ w_\alpha(e, i) f_{e,i} / \Sigma_{e=1,\ldots,E}\ w_\alpha(e, i) \quad (6)$$

The *item weight* DM is $\text{IDM}_{\alpha^*}$ where $\alpha^*$ maximizes

$$\text{calibration score}(\text{IDM}_a) \times \text{information score}(\text{IDM}_\alpha) \quad (7)$$

Item weights are potentially more attractive as they allow an expert to up- or down weight himself/herself for individual items according to how much (s)he feels (s)he knows about that item. "Knowing less" means choosing quantiles further apart and lowering the information score for that item. Of course, good performance of item weights requires that experts can perform this up–down weighting successfully. Anecdotal evidence suggests

that item weights improve over global weights as the experts receive more training in probabilistic assessment. Both item and global weights can be pithily described as optimal weights under a strictly proper scoring rule constraint. In both global and item weights calibration dominates over information, information serves to modulate between more or less equally well-calibrated experts.

Since any combination of expert distributions yields assessments for the seed variables, any combination can be evaluated on the seed variables. In particular, we can compute the calibration and the information of any proposed DM. We should hope that the DM would perform better than the result of simple averaging, called the *equal weight decision maker* (*EWDM*), and we should also hope that the proposed DM is not worse than the best expert in the panel.

In the classical model, calibration and information are combined to yield an overall or combined score with the following properties:

1. Individual expert assessments, realizations, and scores are published. This enables any reviewer to check the application of the method, in compliance with the principle of *accountability/scrutability*.
2. Performance is measured and hopefully validated, in compliance with the principle of *empirical control*. An expert's weight is determined by performance.
3. The score is a long-run proper scoring rule for average probabilities, in compliance with the principle of *neutrality*.
4. Experts are treated equally, before the performance measurement, in compliance with the principle of *fairness*.

Expert names and qualifications are part of the published documentation of every expert judgment study in the database; however, they are not associated with assessments in the open literature. The experts reasoning is always recorded and sometimes published as expert rationales.

There is no mathematical theorem that either item weights or global weights outperform equal weighting or outperform the best expert. It is not difficult to construct artificial examples where this is not the case. Performance of these weighting schemes is a matter of experience. In practice, global weights are used unless item weights perform markedly better. Of course, there may be other ways of defining weights that perform better, and indeed there might be better performance measures. Good performance on one individual data set is not convincing. What is convincing is good performance on a large diverse data set, such as the TU Delft expert judgment database. In practice, a method should be easy to apply, easy to explain, should do better than equal weighting, and should never do something ridiculous.

## 4 APPLICATIONS OF THE CLASSICAL MODEL

Forty-five expert panels involving seed variables have been performed to date.[1] Because most of these studies were performed by or in collaboration with the TU Delft, it is

[1]These results are obtained with the EXCALIBUR software, available from http://delta.am.ewi.tudelft.nl/risk/. The windows version upgraded chi-square and information computational routines, and this may cause differences with the older DOS version, particularly with regard to very low calibration scores.

possible to retrieve relevant details of these studies, and to compare performance of performance-based and equal weight combination schemes. For studies by Ter Haar [17], the data has not been retrieved.

These are all studies performed under contract for a problem owner and reviewed and accepted by the contracting party. In most cases these have been published. Table 2 below lists these studies, references publications, and gives summary information. The number of variables and number of seed variables are shown, as is the number of effective seed variables. In general, the effective number of seeds is equal to the least number of seeds assessed by some expert. In this way each expert is scored with a test of the same power. In the Gas panel, the panel and the seed variables were split post hoc into corrosion and environmental panels.

The combined scores of EWDM, performance-based DM, and best expert are compared pairwise in Figure 1. Figure 2 compares the calibration ($p$ values) and information scores of the EWDM, the performance-based DM, and the best expert.

In 15 of 45 cases, the performance-based DM was the best expert, that is, one expert received weight one. In 27 cases, the combined score of the performance-based DM was strictly better than both the EWDM and the best expert. In one case [2], the EWDM performed best, and in two cases [16, 40] the best expert outperformed both equal weights and performance-based weights.

The EWDM is better calibrated than the best expert in 25 of the 45 cases, but in only two cases more informative. In 18 cases the combined score of the EWDM is better than that of the best expert. In 12 of the 45 cases the calibration of the best expert is less than or equal to 0.05; for the EWDM this happened in seven cases (15%).

The study on radiological transport in soil Genest and Zidek [16] was unusual in that all the experts and all DMs performed badly. Both the seed variables and the experts were identified by the National Radiological Protection Board, and reanalysis of the seed variables and expert data did not yield any satisfactory explanation for the poor performance. We concluded that this was simply due to the small number of experts and bad luck.

The motivation for performance-based weighting above equal weighting speaks for itself from this data. Most often the EWDM is slightly less well calibrated and significantly less informative, but sometimes the calibration of the EWDM is quite poor [41, 42]. Finally, we remark that the experts overwhelmingly have supported the idea of performance measurement. This sometimes comes as a surprise for people from the social sciences, but not for natural scientists. The essential point is that the performance measures are objective and fully transparent. It is impossible to tweak these measures for extrascientific expediency.

## 5 SEED VARIABLES, VARIABLES OF INTEREST, AND ROBUSTNESS

A recurring question is the degree to which performance on seed variables predicts performance on the variables of interest. Forecasting techniques always do better on data used to initialize the models than on fresh data. Might that not be the case here as well? Obviously, we have recourse to expert judgment *because* we cannot observe the variables of interest, so this question is likely to be with us for some time. Experts' information scores *can* be computed for the variables of interest and compared with the seed variables (see below). More difficult is the question whether calibration differences

**TABLE 2 Expert Judgment Studies**

| Case | Name/ Reference | Number of Experts | Number of Variables/ Seeds | Number of Effective Seeds | Performance Measure | Performance Weights | Equal Weights | Best Expert |
|---|---|---|---|---|---|---|---|---|
| **1** | Dsm-1 | 10 | 14/8 | 8 | Calibration | 0.66 | 0.53 | 0.54 |
| **Flange leak** | 12, 16 | | | | Information | 1.371 | 0.8064 | 1.549 |
| | | | | | *Combination* | *0.905* | *0.4274* | *0.836* |
| **2** | Dsm-2 | 8 | 39/12 | 11 | Calibration | 0.84 | 0.5 | 0.005 |
| **Crane risk** | 18 | | | | Information | 1.367 | 0.69 | 2.458 |
| | | | | | *Combination* | *1.148* | *0.345* | *0.012* |
| **3** | Estec-1 | 4 | 48/13 | 13 | Calibration | 0.43 | 0.43 | 0.14 |
| **Propulsion** | 12, 16 | | | | Information | 1.72 | 1.421 | 2.952 |
| | | | | | *Combination* | *0.7398* | *0.611* | *0.413* |
| **4** | Estec-2 | 7 | 58/26 | 18 | Calibration | 0.78 | 0.9 | 0.0001 |
| **Space debris** | 19 | | | | Information | 0.32 | 0.15 | 2.29 |
| | | | | | *Combination* | *0.25* | *0.14* | *0.0002* |
| **5** | Estec-3 | 6 | 22/12 | 12 | Calibration | 0.27 | 0.12 | 0.005 |
| **Composite materials** | 8 | | | | Information | 1.442 | 0.929 | 2.549 |
| | | | | | *Combination* | *0.39* | *0.111* | *0.013* |
| **6** | AOT (daily) | 9 | 38/38 | 6 | Calibration | 0.95 | 0.95 | 0.95 |
| **Option trading** | 20 | | | | Information | 0.5043 | 0.2156 | 0.5043 |
| | | | | | *Combination* | *0.4791* | *0.2048* | *0.4791* |
| **7** | AOT (risk) | 5 | 11/11 | 11 | Calibration | 0.8287 | 0.324 | 0.8287 |
| **Risk management** | 20 | | | | Information | 1.212 | 0.7449 | 1.212 |
| | | | | | *Combination* | *1.003* | *0.2413* | *1.003* |
| **8** | Grond-5 | 7 | 38/10 | 10 | Calibration | 0.7 | 0.05 | 0.4 |
| **Groundwater transport** | 21 | | | | Information | 3.008 | 3.16 | 3.966 |
| | | | | | *Combination* | *2.106* | *0.158* | *1.586* |

(*continued overleaf*)

**TABLE 2** (*Continued*)

| Case | Name/ Reference | Number of Experts | Number of Variables/ Seeds | Number of Effective Seeds | Performance Measure | Performance Weights | Equal Weights | Best Expert |
|---|---|---|---|---|---|---|---|---|
| **9** | Tuddispr | 11 | 58/36 | 36 | Calibration | 0.68 | 0.71 | 0.36 |
| **Dispersion panel TUD** | 1, 2 | | | | Information | 0.827 | 0.715 | 1.532 |
| | | | | | *Combination* | *0.562* | *0.508* | *0.552* |
| **10** | Tnodispr | 7 | 58/36 | 36 | Calibration | 0.69 | 0.32 | 0.53 |
| **Dispersionpanel TNO** | 2 | | | | Information | 0.875 | 0.751 | 1.698 |
| | | | | | *Combination* | *0.604* | *0.24* | *0.9002* |
| **11** | Tuddepos | 4 | 56/24 | 22 | Calibration | 0.45 | 0.34 | 0.45 |
| **Dry deposition** | 1, 2 | | | | Information | 1.647 | 1.222 | 1.647 |
| | | | | | *Combination* | *0.741* | *0.415* | *0.741* |
| **12** | Acnexpts | 7 | 43/10 | 10 | Calibration | 0.24 | 0.28 | 0.24 |
| **Acrylo-nitrile** | 4, 13, 22 | | | | Information | 3.186 | 1.511 | 3.186 |
| | | | | | *Combination* | *0.764* | *0.423* | *0.764* |
| **13** | Nh3expts | 6 | 31/10 | 10 | Calibration | 0.11 | 0.28 | 0.06 |
| **Ammonia panel** | 4, 13, 22 | | | | Information | 1.672 | 1.075 | 2.627 |
| | | | | | *Combination* | *0.184* | *0.301* | *0.158* |
| **14** | So3expts | 4 | 28/7 | 7 | Calibration | 0.14 | 0.14 | 0.02 |
| **Sulfur trioxide** | 4, 13, 22 | | | | Information | 3.904 | 2.098 | 4.345 |
| | | | | | *Combination* | *0.547* | *0.294* | *0.087* |
| **15** | Waterpol | 11 | 21/11 | 10 | Calibration | 0.35 | 0.35 | 0.16 |
| **Water pollution** | 23 | | | | Information | 1.875 | 1.385 | 2.06 |
| | | | | | *Combination* | *0.6563* | *0.4847* | *0.3296* |
| **16** | Eunrcdis | 8 | 77/23 | 23 | Calibration | 0.9 | 0.15 | 0.13 |
| **Dispersionpanel** | 5, 6, 24 | | | | Information | 1.087 | 0.862 | 1.242 |
| | | | | | *Combination* | *0.9785* | *0.129* | *0.161* |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **17** | Eunrcdd | 8 | 87/14 | 14 | Calibration | 0.52 | 0.001 | 0.52 |
| **Dry deposition** | 5, 6, 24 | | | | Information | 1.339 | 1.184 | 1.339 |
| | | | | | *Combination* | *0.697* | *0.001* | *0.697* |
| **18** | Eunrca_s | 7 | 80/8 | 6 | Calibration | 0.75 | 0.55 | 0.75 |
| **Rad. Transp. in animals** | 5, 24, 25 | | | | Information | 2.697 | 1.778 | 2.697 |
| | | | | | *Combination* | *2.023* | *0.978* | *2.023* |
| **19** | Euncrwd | 7 | 50/19 | 19 | Calibration | 0.25 | 0.001 | 0.01 |
| **Wet deposition** | 5, 6, 24 | | | | Information | 0.451 | 0.726 | 0.593 |
| | | | | | *Combination* | *0.113* | *0.00073* | *0.0059* |
| **20** | Eunrcint | 8 | 332/55 | 28 | Calibration | 0.85 | 0.11 | 0.73 |
| **Rad. internal dose** | 5, 24, 26 | | | | Information | 0.796 | 0.5598 | 0.822 |
| | | | | | *Combination* | *0.677* | *0.062* | *0.6001* |
| **21** | Eunrcear | 9 | 489/15 | 15 | Calibration | 0.23 | 0.07 | 0.0001 |
| **Rad. early health effects** | 5, 24, 27 | | | | Information | 0.2156 | 0.1647 | 1.375 |
| | | | | | *Combination* | *0.0496* | *0.01153* | *0.00014* |
| **22** | Euncrsoi | 4 | 244/31 | 31 | Calibration | 0.0001 | 0.0001 | 0.0001 |
| **Rad. trans. soil** | 5, 24, 25 | | | | Information | 1.024 | 0.973 | 2.376 |
| | | | | | *Combination* | *0.0001* | *9.7E–05* | *0.0002* |
| **23** | Gas95 | 15 | 106/28 | 17 | Calibration | 0.93 | 0.11 | 0.06 |
| **Environment panel** | 28 | | | | Information | 1.628 | 1.274 | 2.411 |
| | | | | | *Combination* | *1.514* | *0.14* | *0.145* |
| **24** | Gas95 | 12 | 58/11 | 11 | Calibration | 0.16 | 0.06 | 0.16 |
| **Corrosion panel** | 28 | | | | Information | 2.762 | 1.304 | 2.762 |
| | | | | | *Combination* | *0.4419* | *0.078* | *0.4419* |
| **25** | Mvblbarr | | 52/14 | 14 | Calibration | 0.43 | 0.22 | 0.04 |
| **Moveable barriers flood risk** | 29 | | | | Information | 1.243 | 0.57 | 1.711 |
| | | | | | *Combination* | *0.535* | *0.125* | *0.068* |

(*continued overleaf*)

**TABLE 2** (*Continued*)

| Case | Name/ Reference | Number of Experts | Number of Variables/ Seeds | Number of Effective Seeds | Performance Measure | Performance Weights | Equal Weights | Best Expert |
|---|---|---|---|---|---|---|---|---|
| **26** | Realestr | 5 | 45/31 | 31 | Calibration | 0.82 | 0.005 | 0.82 |
| **Real estate risk** | 30 | | | | Information | 0.7648 | 0.1735 | 0.7678 |
| | | | | | *Combination* | *0.6296* | *0.0009* | *0.6296* |
| **27** | Rivrchnl | 6 | 14/8 | 8 | Calibration | 0.53 | 0.64 | 0.53 |
| **River channel** | 31 | | | | Information | 0.843 | 0.289 | 0.843 |
| | | | | | *Combination* | *0.447* | *0.185* | *0.447* |
| **28** | Mont1 | 11 | 13/8 | 8 | Calibration | 0.66 | 0.53 | 0.66 |
| **Montserrat Volcano** | 32, 33 | | | | Information | 1.906 | 0.8217 | 1.906 |
| | | | | | *Combination* | *1.258* | *0.4355* | *1.258* |
| **29** | Thrmbld | 6 | 48/48 | 10 | Calibration | 0.3628 | 0.02485 | 0.3628 |
| **Thermal phys. Blds** | 7 | | | | Information | 0.5527 | 0.1424 | 0.5527 |
| | | | | | *Combination* | *0.2005* | *0.00354* | *0.2005* |
| **30** | Dikring | 17 | 87/47 | 47 | Calibration | 0.4 | 0.05 | 0.3 |
| **Dike ring failure** | 15, 34 | | | | Information | 0.614 | 0.7537 | 0.6462 |
| | | | | | *Combination* | *0.2456* | *0.03768* | *0.1938* |
| **31** | Carma | 12 | 98/10 | 10 | Calibration | 0.828 | 0.4735 | 0.828 |
| ***Campylobacter*** NL | 17 | | | | Information | 1.48 | 0.2038 | 1.48 |
| | | | | | *Combination* | *1.226* | *0.09648* | *1.226* |
| **32** | CARME-Greece | 6 | 98/10 | 10 | Calibration | 0.4925 | 0.5503 | 0.4925 |
| **Campy Greece** | 35 | | | | Information | 0.8611 | 0.3428 | 0.8611 |
| | | | | | *Combination* | *0.4241* | *0.1886* | *0.4241* |
| **33** | Opriskbank | 10 | 36/16 | 16 | B | 0.4301 | 0.338 | 0.1473 |
| **Oper. Risk** | 36 | | | | Information | 0.7827 | 0.3219 | 0.903 |
| | | | | | *Combination* | *0.3263* | *0.1088* | *0.133* |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **34** | Infosec | 13 | 32/10 | 10 | Calibration | 0.7071 | 0.7971 | 0.3135 |
| **Infosec** | 37 | | | | Information | 1.721 | 1.012 | 2.232 |
| | | | | | *Combination* | *1.217* | *0.7159* | *0.6999* |
| **35** | PM25 | 6 | 24/12 | 12 | Calibration | 0.578 | 0.6451 | 0.1195 |
| **PM25** | | | | | Information | 0.807 | 0.542 | 1.486 |
| | | | | | *Combination* | *0.466* | *0.3497* | *0.1776* |
| **36** | Ladders | 7 | 22/10 | 10 | Calibration | 0.2441 | 0.3005 | 0.00131 |
| **Falls ladders** | | | | | Information | 0.975 | 0.4638 | 1.801 |
| | | | | | *Combination* | *0.238* | *0.1394* | *0.00236* |
| **37** | Dams | 11 | 74/11 | 11 | Calibration | 0.615 | 0.492 | 0.01088 |
| **Dams** | 38 | | | | Information | 1.248 | 0.6446 | 2.359 |
| | | | | | *Combination* | *0.7677* | *0.3171* | *0.02566* |
| **38** | MVO seeds | 77 | 5/5 | 5 | Calibration | 0.6084 | 0.3946 | 0.6084 |
| **MVO seeds Montserrat follup** | 33, 39 | | | | Information | 3.116 | 1.147 | 3.116 |
| | | | | | *Combination* | *1.896* | *0.4525* | *1.896* |
| **39** | Pilots | 31 | 63/10 | 10 | Calibration | 0.4735 | 0.5503 | 0.1917 |
| **Pilots** | 32 | | | | Information | 0.6903 | 0.5946 | 1.403 |
| | | | | | *Combination* | *0.3269* | *0.2777* | *0.2689* |
| **40** | Setecidades | 19 | 27/10 | 10 | Calibration | 0.7901 | 0.1065 | 0.4281 |
| **Sete Cidades** | | | | | Information | 2.709 | 0.8409 | 2.474 |
| | | | | | *Combination* | *2.141* | *0.1713* | *1.059* |
| **41** | | 17 | 23/10 | 10 | Calibration | 0.7069 | 0.1135 | 0.04706 |
| **TeideMay_05** | TeideMay_05 | | | | Information | 2.178 | 1.681 | 3.322 |
| | | | | | *Combination* | *1.54* | *0.1907* | *0.1563* |
| **42** | VesuvioPisa21Mar05 | 14 | 79/10 | 10 | Calibration | 0.6827 | 0.4735 | 0.4706 |
| **Vesuvio** | | | | | Information | 2.43 | 1.485 | 3.622 |
| | | | | | *Combination* | *1.659* | *0.7029* | *0.1705* |

(*continued overleaf*)

**TABLE 2** (*Continued*)

| Case | Name/ Reference | Number of Experts | Number of Variables/ Seeds | Number of Effective Seeds | Performance Measure | Performance Weights | Equal Weights | Best Expert |
|---|---|---|---|---|---|---|---|---|
| **43** | Volcrisk | 45 | 30/10 | 10 | Calibration | 0.8283 | 0.1135 | 0.8283 |
| **Volcrisk** | | | | | Information | 0.7738 | 0.5571 | 0.7738 |
| | | | | | *Combination* | *0.641* | *0.06322* | *0.641* |
| **44** | Sars | 9 | 20/10 | 10 | Calibration | 0.6827 | 0.4735 | 0.06083 |
| **SARS** | | | | | Information | 1.34 | 0.6017 | 2.31 |
| | | | | | *Combination* | *0.9149* | *0.2849* | *0.1405* |
| **45** | Guadeloupe | 9 | 57/10 | 10 | Calibration | 0.4925 | 0.4735 | 0.0008 |
| **Guadeloupe** | | | | | Information | 2.158 | 1.176 | 3.649 |
| | | | | | *Combination* | *1.063* | *0.5567* | *0.00029* |

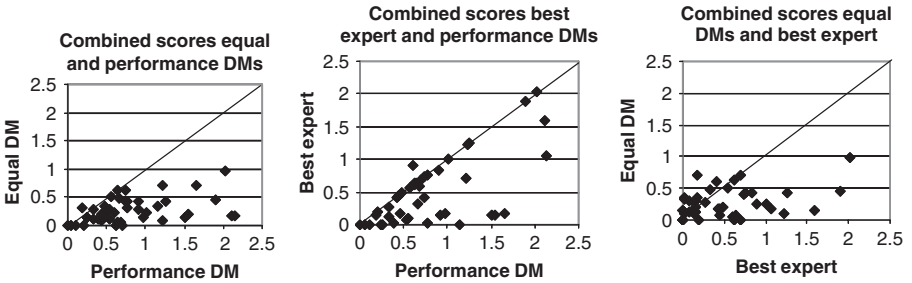



**FIGURE 1** Combined scores of equal weight DM, performance-based DM, and the best expert.

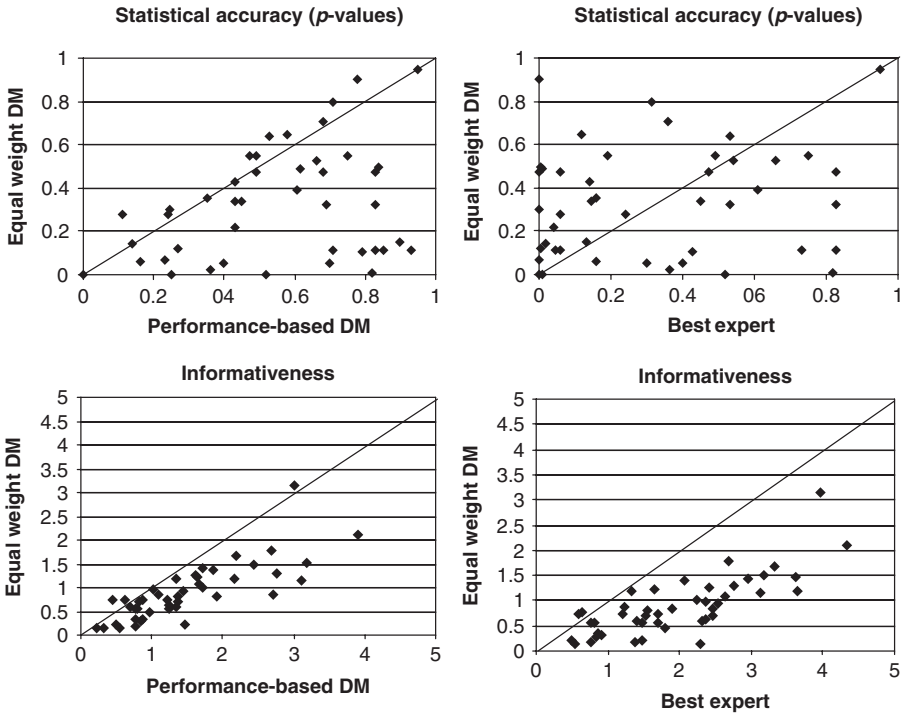



**FIGURE 2** Calibration ($p$ values) and information scores of equal weight DM, performance-based DM, and the best expert.

in experts and DMs "persist" outside the set of seed variables. Questions related to this are as follows

1. Are the differences in experts' calibration scores due to chance fluctuations?
2. Is an expert's ability to give informative and well-calibrated assessments persistent in time, dependent on training, seniority, or related to other psychosocial variables?

There has been much published and speculated on these questions, and the issue cannot be reviewed, let alone resolved here. If differences in experts' performance did

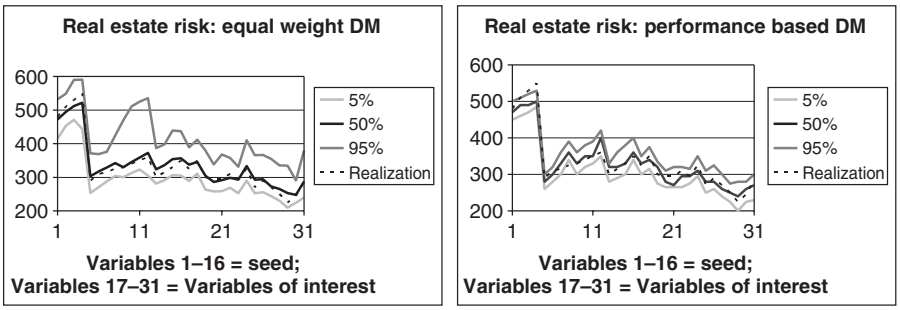



**FIGURE 3** Seed variables and variables of interest, Real Estate Risk.

*not* persist beyond the seed variables, then that would certainly cast a long shadow over performance-based combination. If, on the other hand, there are real and reasonably persistent differences in expert performance, then it is not implausible that a performance-based combination could systematically do "better than average". It is hoped that the TU Delft database can contribute to a further analysis of these issues.

Closely related is the question of robustness: to what extent would the results change if different experts or different seed variables had been used. This last question can be addressed, if not laid to rest, by removing seed variables and experts one at a time and recomputing the DM. We discuss a few studies to illustrate good and poor choices of seed variables and, where possible, compare with variables of interest.

### 5.1 Real Estate Risk

In this study, the seed variables were prime office rent indices for large Dutch cities, published quarterly (variables 1 through 16). The variables of interest were rents of the actual properties managed by the investment firm. After 1 year, the realized rents were retrieved and compared with the predictions. The results for the EWDM and performance DM are shown below.

The robustness analyses in this case are also revealing. First, we examine the five experts' (three portfolio managers and two risk analysts) and DM's scores, and the relative information of each of the experts to the equal weight combination of their distributions (Table 3). This gives a benchmark for how well the experts agree among themselves. The experts' densities are constructed relative to a background measure, so these comparisons also depend on the background measure. The relatively weak calibration performance of the EWDM is due to the fact that only 4 of the 16 seed variables were above the median assessment.[2] At the same time, the equal DM's medians are actually a bit closer to the realizations. Distance between median and realization is an example of a scoring variable, which is *not* taken into account by the performance-based DM.[3] Note also that the pattern of informativeness on seed variables is comparable to that on all variables; portfolio manager 3 is least informative and risk analyst 1 is most informative. Note also that low informativeness does not translate automatically into better calibration.

[2]The values cited in Table 3 are based on 31 seed variables, using also the variables of interest, which became available a year later.

[3]The reason is that distance is scale dependent. In this case, the scales of all variables are the same, so such a scoring variable could be used. Of course, such a rule may not be proper.

**TABLE 3 Real Estate Risk: Relative Information of the Five Experts to the Equal Weight Combination for All Variables and for Variables with Realizations**

| ID | Calibration | Mean Relative Information | | Number of Realization | Unnormalized Weight | Relative Information to Equal Weight DM | |
|---|---|---|---|---|---|---|---|
| | | All Variables | Seed Variables | | | All Variables | Seed Variables |
| Portfol1 | 0.3303 | 0.7932 | 0.8572 | 16 | 0.2832 | 0.5004 | 0.6241 |
| Portfol2 | 0.1473 | 1.02 | 0.9554 | 16 | 0 | 0.7764 | 0.6545 |
| Portfol3 | 0.02012 | 0.2492 | 0.1556 | 16 | 0 | 0.3633 | 0.2931 |
| Riskan1 | 6.06E−05 | 1.334 | 1.536 | 16 | 0 | 0.9575 | 1.21 |
| Riskan2 | 0.004167 | 0.5848 | 0.6126 | 16 | 0 | 0.4579 | 0.4402 |
| Performance DM | 0.3303 | 0.7932 | 0.8572 | 16 | 0.2832 | | |
| Equal DM | 0.05608 | 0.1853 | 0.179 | 16 | 0.01004 | | |

Next we remove the 16 seed variables one at a time and recompute the performance-based DM (Table 4).

The scores do not change much, but the relative information of the "perturbed DM" with respect to the original DM is rather large for eight of the variables, compared to the differences between the experts themselves. The explanation can be found by examining the robustness on experts (Table 5).

If we remove portfolio manager 1, the effect on the DM is large, compared to the largest relative information between a single expert and the equal weight combination. This is not surprising as portfolio manager 1 coincides with the performance-based DM. Interestingly, we get a significant change by removing portfolio manager 2. This is because the combination of portfolio managers 1 and 3 would give a higher score than portfolio manager 1 alone, or 1 and 2 alone. We should have to give portfolio manager 2 weight zero and portfolio manager 3 positive weight, even though the latter's calibration score is worse than that of the former. The proper scoring rule constraint prevents this from happening. This underscores the difference noted in Section 2 between optimization under the proper scoring rule constraint and unconstrained optimization. In the latter case, a better calibrated expert can have less weight than a poorly calibrated expert. The nonrobustness in Table 4 is caused by the fact that the removal of some seed variables cause the calibration of portfolio manager 2 to dip below that of portfolio manager 3.

### 5.2 AEX

In this case, the seed variables *were* the variables of interest, namely the opening price of the Amsterdam stock exchange, as estimated at closing the previous day. Note that some of the experts anticipated a large drop on the day corresponding to variable 20. This was reflected neither in the performance-based DM nor in the realization. Other than that, the pattern across seed variables does not look erratic. In spite of the excellent performance of the experts in this case, they were not able to predict the opening price better than the "historical average predictor". In other words, any information the experts might have had at closing time was already reflected in the closing price.

### 5.3 Dry Deposition

The seed variables were measured deposition velocities, though not configured according to the requirements of the study (per species, windspeed, particle diameter, and surface).

Here again, the poor statistical performance of the EWDM is due to the fact that all but one of the 14 seed variables fall above the median.

### 5.4 Dyke Ring

The seed variables were ratios of predicted versus measured water levels (at different water levels, around 2 m above the baseline). Variables of interest were the same, but at water levels above 3.5 m above the baseline. In this case, we had several realizations of this ratio from each of several measuring stations. This explains the step pattern of the quantiles; these are actually the same assessment with several realizations.

Although all 47 seed variables were used in the analysis, for purposes of comparing expert performance with that of other studies, the effective number of seeds was reduced to 10. This accounts for dependence in the experts' assessments and corresponds to the number most often used for such comparisons.

**TABLE 4 Real Estate Risk: Robustness Analysis on Seed Variables**

| | Relative Information/b | | | Relative Information/Original DM | |
|---|---|---|---|---|---|
| Excluded Item | All Variables | Seed Variables | Calibration | All Variables | Seed Variables |
| Q1Rent Amster. | 0.5875 | 0.6234 | 0.3578 | 0.3539 | 0.37 |
| Q2Rent Amster. | 0.5974 | 0.6341 | 0.3578 | 0.4402 | 0.4421 |
| Q3Rent Amster. | 0.7921 | 0.8583 | 0.5435 | 0 | 0 |
| Q4Rent Amster. | 0.7859 | 0.8401 | 0.5435 | 0 | 0 |
| Q1Rent Rotter. | 0.5871 | 0.6047 | 0.3578 | 0.4438 | 0.4565 |
| Q2Rent Rotter. | 0.5857 | 0.6004 | 0.3578 | 0.4491 | 0.4708 |
| Q3Rent Rotter. | 0.8009 | 0.8841 | 0.387 | 0 | 0 |
| Q4Rent Rotter. | 0.5872 | 0.6222 | 0.3578 | 0.3505 | 0.3575 |
| Q1Rent Denhaag | 0.7886 | 0.8478 | 0.387 | 0 | 0 |
| Q2Rent Denhaag | 0.7861 | 0.8406 | 0.387 | 0 | 0 |
| Q3Rent Denhaag | 0.784 | 0.8345 | 0.387 | 0 | 0 |
| Q4Rent DenHaag | 0.7845 | 0.8358 | 0.387 | 0 | 0 |
| Q1Rent Utrecht | 0.6034 | 0.6396 | 0.288 | 0.4589 | 0.4353 |
| Q2Rent Utrecht | 0.6069 | 0.6517 | 0.288 | 0.4663 | 0.4644 |
| Q3Rent Utrecht | 0.6013 | 0.6356 | 0.288 | 0.4656 | 0.464 |
| Q4Rent Utrecht | 0.794 | 0.8638 | 0.387 | 0 | 0 |
| Original Perf DM | 0.7932 | 0.8572 | 0.3303 | | |

**TABLE 5 Real Estate Risk: Robustness Analysis on Experts**

| | Relative Information/b | | | Relative Information/Original DM | |
|---|---|---|---|---|---|
| Excluded Expert | All Variables | Seed Variables | Calibration | Total Variables | Seed Variables |
| Portfol1 | 1.006 | 0.9484 | 0.1473 | 1.144 | 1.058 |
| Portfol2 | 0.637 | 0.6899 | 0.7377 | 0.2916 | 0.3328 |
| Portfol3 | 0.5297 | 0.4825 | 0.3303 | 0 | 0 |
| Riskan1 | 0.7921 | 0.8572 | 0.3303 | 0 | 0 |
| Riskan2 | 0.7079 | 0.8195 | 0.3303 | 0 | 0 |
| Original performance DM | 0.7932 | 0.8572 | 0.3303 | 0 | 0 |

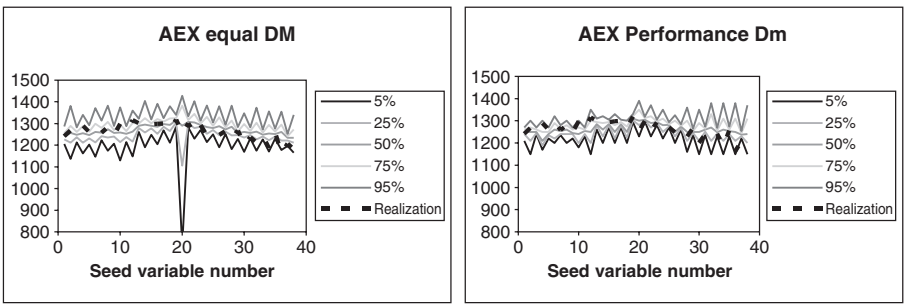



**FIGURE 4** Seed variables (which are the variables of interest), AEX.

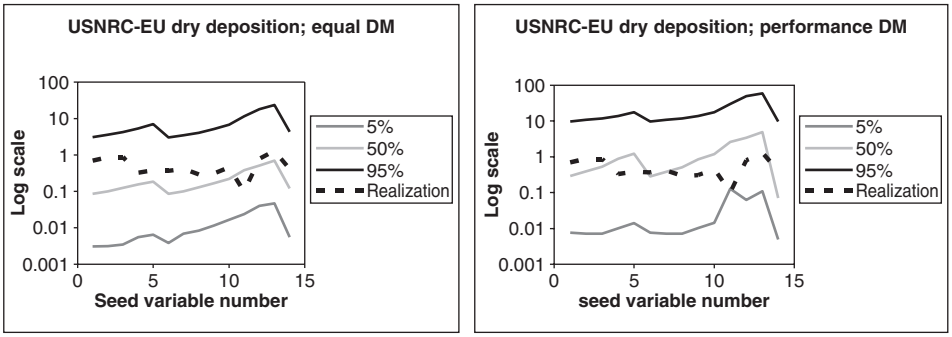



**FIGURE 5** Seed variables, USNRC-EU Dry Deposition.

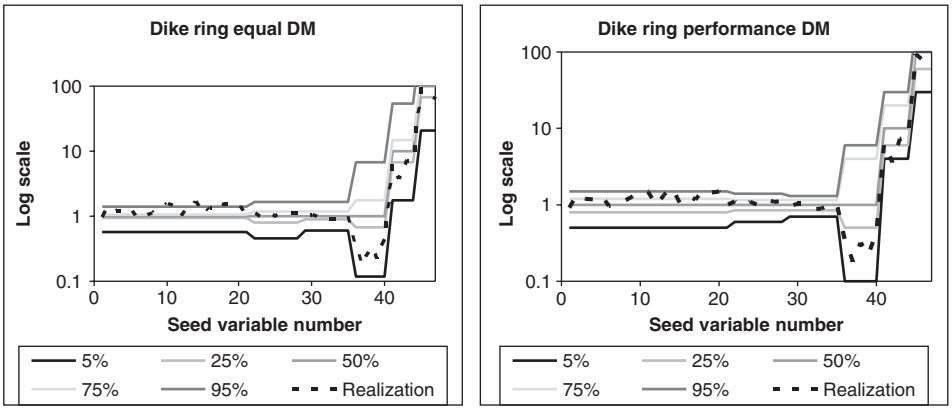



**FIGURE 6** Seed variables Dike Ring.

## 5.5 Space Debris

The seed variables were numbers of tracked space debris particles injected into orbit between the years 1961 and 1986. Variables of interest characterized the debris flux for 10 years into the future. It turned out that the experts did not possess year-by-year knowledge of the debris particles, and gave generic assessments assuming that the number was growing, where in fact the number appears to be quite random. This is a case in which the choice of seed variables was unsuccessful; the experts did not really have relevant knowledge to apply to the task.[4]

## 5.6 Out-of-Sample Validation?

In a review of the online version of this article, Clemen raised the important question: does the performance of the performance-weighted decision maker (PWDM) persist

[4]In this early study, the effective number of seed variables was chosen to optimize the DM's performance, a procedure which is no longer followed. The DOS version of the software used a table of the chi-square distribution and had problems with very low calibration scores. These problems will come to the fore, when the number of seed variables is high, as in this case.

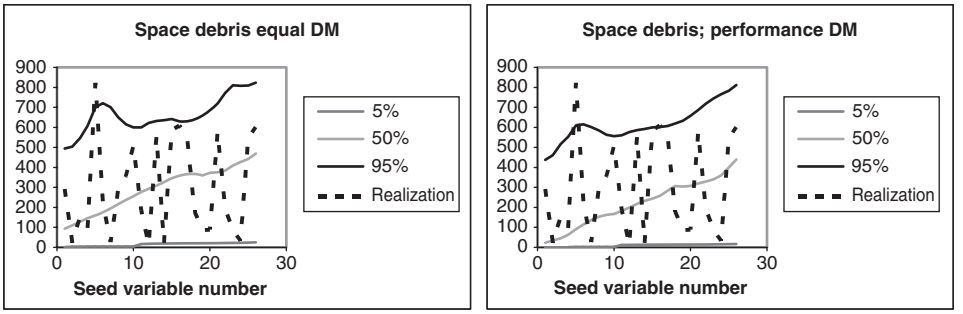



**FIGURE 7** Seed variables Space Debris.

beyond the set of seed variables. Clemen believes that there is no significant difference between the PWDM and the EWDM outside the variables on which PWDM has been constructed.

As noted above, PWDM does use optimization to remove a degree of freedom in the definition of the classical model. In every study, we routinely perform robustness analysis by removing seed variables (and experts) one at a time and recomputing PWDM. It is not uncommon to see the calibration scores of PWDM fluctuating by a factor 2 or 3 on 10 seed variables.

Out-of-sample validation involves basing PWDM on an initial set of seed variables, then using this PWDM on *other* variables and comparing performance of EWDM on these other variables. This corresponds to the way PWDM is actually used. We can do this by splitting the set of seed variables into halves, initializing the model on one half and comparing performance on the other half. Of course, this requires a relatively large number of seed variables. There are 14 studies with at least 16 seed variables. One of these, "TNO dispersion", eluded conversion to the format of the windows software and currently cannot be read. This leaves 13 studies. Dividing the seed variables into half gives two validation runs, using the first half to predict the second and conversely. Note that the variables on which the PWDM is initialized in these two runs are disjoint. The item weight PWDM could not be computed without writing a new code, so the choice of item versus global weights denied PWDM on this exercise.

The data from the 13 studies are shown in Table 6. In 20 of the 26 studies, the out-of-sample PWDM outperforms EWDM. The probability of seeing 20 or more "successes" on 26 trials if PWDM were no better than EWDM is 0.0012.

Clemen reports results on 14 validation studies that are somewhat more pessimistic (9 "success" on 14 trials). His method involves removing seed variables singly, computing PWDM on the remaining seeds, and using this PWDM to predict the eliminated seed. On a study with 10 seed variables, there are thus 10 *different* PWDMs. Each pair of the 10 DMs share eight common seeds. The criteria for selecting the 14 studies are not specified. It is difficult to see how all these factors would affect the results. Perhaps the following reasoning partially explains Clemen's less optimistic result: With a small number of seeds, removing one seed favors experts who assessed *that* seed badly and hurts experts who assessed *that* seed well, thus tilting the PWDM toward a bad assessment of *that* seed. This happens on *every* seed thus cumulating the adverse effect on PWDM. This does not happen when *one* PWDM predicts the entire out-of-sample set of seeds.

**TABLE 6 26 Out-of-Sample Validation Runs[a]**

| Study | DM | Calibration | Information | Combination |
|---|---|---|---|---|
| | *e1* | *0.42* | *0.646* | *0.2713* |
| TUD disper | PW(2)1 | 0.21 | 0.8744 | 0.1836 |
| | *e2* | *0.39* | *0.7844* | *0.3059* |
| | PW(1)2 | 0.005 | 1.525 | 0.007624 |
| | e1 | 0.52 | 1.119 | 0.5819 |
| TUD depos | *PW(2)1* | *0.52* | *1.42* | *0.7382* |
| | *e2* | *0.73* | *1.324* | *0.9669* |
| | PW(1)2 | 0.59 | 1.374 | 0.8108 |
| | e1 | 0.429 | 0.2793 | 0.1198 |
| Operrisk | *PW(2)1* | *0.5337* | *0.5749* | *0.3068* |
| | e2 | 0.5337 | 0.3646 | 0.1946 |
| | *PW(1)2* | *0.185* | *1.109* | *0.2053* |
| | e1 | 0.025 | 0.7386 | 0.01846 |
| Dikering | *PW(2)1* | *0.4* | *0.3859* | *0.1544* |
| | e2 | 0.025 | 0.7814 | 0.01954 |
| | *PW(1)2* | *0.05* | *0.6451* | *0.03225* |
| | e1 | 0.07 | 0.1424 | 0.009967 |
| Thermbld | *PW(2)1* | *0.48* | *0.5527* | *0.2653* |
| | e2 | 0.005 | 0.1424 | 0.0007119 |
| | *PW(1)2* | *0.07* | *0.7305* | *0.05113* |
| | e1 | 0.05 | 0.179 | 0.008948 |
| Realest | *PW(2)1* | *0.33* | *0.8572* | *0.2829* |
| | e2 | 0.18 | 0.1676 | 0.030168 |
| | *PW(1)2* | *0.35* | *0.6724* | *0.2353* |
| | e1 | 0.52 | 0.9662 | 0.5024 |
| EuDis | *PW(2)1* | *0.52* | *1.232* | *0.6408* |
| | e2 | 0.02 | 0.749 | 0.01498 |
| | *PW(1)2* | *0.08* | *1.204* | *0.09635* |
| | e1 | 0.001 | 1.108 | 0.0011089 |
| PintDos | *PW(2)1* | *0.11* | *1.038* | *0.1141* |
| 6exp. | e2 | 0.23 | 0.3262 | 0.07502 |
| 39 items | *PW(1)2* | *0.44* | *0.6748* | *0.2969* |
| | e1 | 0.001 | 0.3638 | 0.0003638 |
| Soil | *PW(2)1* | *0.001* | *0.4135* | *0.0004135* |
| | e2 | 0.0001 | 1.539 | 0.0001539 |
| | *PW(1)2* | *0.0001* | *1.551* | *0.0001559* |
| | e1 | 0.0001 | 1.235 | 0.0001235 |
| Gas | *PW(2)1* | *0.06* | *2.01* | *0.1206* |
| Environ | e2 | 0.72 | 1.274 | 0.9171 |
| | *PW(1)2* | *0.73* | *2.342* | *1.71* |
| | e1 | 0.1 | 0.2046 | 0.02046 |
| AOT | *PW(2)1* | *0.1* | *0.6685* | *0.06685* |
| 6 exp | e2 | 0.5 | 0.1793 | 0.08964 |
| 20 items | *PW(1)2* | *0.7* | *0.5799* | *0.4059* |
| | *e1* | *0.11* | *0.6611* | *0.07272* |
| EU | PW(2)1 | 0.0001 | 2.048 | 0.0002048 |
| WD | *e2* | *0.04* | *0.7983* | *0.03193* |
| | PW(1)2 | 0.04 | 0.7743 | 0.03097 |
| | *e1* | *0.75* | *0.2427* | *0.182* |
| estec-2 | PW(2)1 | 0.43 | 0.3623 | 0.1558 |
| | e2 | 0.68 | 0.07269 | 0.04943 |
| | *PW(1)2* | *0.35* | *0.1893* | *0.06627* |

Best performer is italicized. E1, the EWDM on the first half of the seed variables; E2, EWDM on the second half; PW(2)1, the PWDM constructed on the second half, predicting the first half; and PW(1)2, the PWDM constructed on the first half predicting the second half.

[a]PintDos involved 55 seed items, and 8 experts, but two experts assessed only a small number of seed variables. The other experts' seed assessments did not wholly overlap; 6 experts assessed 39 common seed variables used for this exercise. Similarly, AOT was restricted to 6 experts who assessed 20 common items. The Gas study was split into a corrosion and an environment panel. Many environment experts were also corrosion experts and their corrosion seed assessments were used in the original study. In this exercise, only the environment seeds were used for the environment panel. In the Dikering study, the multiple measurements from each measuring station were split.

In any case, Clemen's method is not the same as picking *one* PWDM and comparing it on new observations with the EWDM.

## 6 LESSONS LEARNED FROM ELICITATIONS

A detailed description of the design of an expert judgment study is given in Cooke and Goossens [34]. Suffice to say here that a typical study involves a dry run with one expert to finalize the elicitation questions. This is followed by a plenary meeting of all experts in which the issues are discussed, the study design is explained, and a short elicitation exercise is done. This involves a small number of seed variables, typically five. Experts are shown how the scoring and combining works. Afterwards, the experts are elicited individually. An elicitation session should not exceed a half day. Fatigue sets in after 2 h.

When experts are dispersed it may be difficult and expensive to bring them together. In such cases the training is given to each expert in abbreviated form. The EU-USNRC studies made the most intensive investment in training. In general, it is not advisable to configure the exercise such that the presence of *all* experts at one time and place is essential to the study, as this makes the study vulnerable to last minute disruptions.

The following are some practical guidelines for responding to typical comments:

**From an expert:** *I don't know that*

Response: *No one knows, if someone knew we would not need to do an expert judgment exercise. We are tying to capture your uncertainty about this variable. If you are very uncertain, then you should choose very wide confidence bounds*.

**From an expert:** *I can't assess that unless you give me more information*.

Response: *The information given corresponds with the assumptions of the study. We are trying to get your uncertainty conditional on the assumptions of the study. If you prefer to think of uncertainty conditional on other factors, then you must try to unconditionalize and fold the uncertainty over these other factors into your assessment*.

**From an expert:** *I am not the best expert for that*.

Response: *We don't know who are the best experts. Sometimes the people with the most detailed knowledge are not the best at quantifying their uncertainty*.

**From an expert:** *Does that answer look OK?*

Response: *You are the expert, not me*.

**From the problem owner:** *So you are going to score these experts like school children?*

Response: *If this is not a serious matter for you, then forget it. If it is serious, then we must take the quantification of uncertainty seriously. Without scoring we can never validate our experts or the combination of their assessments*.

**From the problem owner:** *The experts will never stand for it*.

Response *We've done it many times, the experts actually like it*.

**From the problem owner:** *Expert number 4 gave crazy assessments, who was that guy?*

Response: *You are paying for the study, you own the data, and if you really want to know I will tell you. But you don't need to know, and knowing will not make things easier for you. Reflect first whether you really want to know this*.

**From the problem owner:** *How can I give an expert weight zero?*

Response: *Zero weight does not mean zero value. It simply means that this expert's knowledge was already contributed by other experts and adding this expert would only*

*add a bit of noise. The value of unweighted experts is seen in the robustness of our answers against loss of experts. Everyone understands this when it is properly explained.*

**From the problem owner:** *How can I give weight one to a single expert?*

Response: *By giving all the others weight zero, see previous response.*

**From the problem owner:** *I prefer to use the equal weight combination.*

Response: *So long as the calibration of the equal weight combination is acceptable, there is no scientific objection to doing this. Our job as analyst is to indicate the best combination, according to the performance criteria, and to say what other combinations are scientifically acceptable.*

## 7 CONCLUSION

Given the body of experience with structured expert judgment, the scientific approach to uncertainty quantification is well established. This does not mean that the discussion on expert judgment method is closed.

First of all, we may note that a full expert judgment study is not cheap. Most of the studies mentioned above involved 1–3 man months. This cost could be reduced somewhat if we need not develop seed variables. However, simply using equal weights does not seem to be a convincing alternative. Other methods of measuring and verifying performance would be welcome, especially if they are less resource intensive.

The classical model is based on the two performance measures, calibration and information, in conjunction with the theory of proper scoring rules. It satisfies necessary conditions for rational consensus, but is not *derived* from those conditions. Other weighting schemes could surely be devised which do as well or better in this regard, and other performance measures could be proposed and explored.

Once we acknowledge that our models must be quantified with uncertainty distributions, rather than "nominal values" of undetermined pedigree, many new challenges confront modelers, analysts, and DMs.

Experts can quantify their uncertainty about potentially observable phenomena with which they have some familiarity. The requirements of the study at hand may go beyond that. For example, in quantifying the uncertainty of models for transport of radiation through soils, plants, and animals, it emerged that the institutes that built and maintained these models could not supply any experts who were able to quantify uncertainty on the transfer coefficients in these models. Experts could quantify uncertainty with regard to quantities, which can be expressed as functions of the transport models themselves. Processing data of this sort required development of sophisticated techniques of probabilistic inversion [43, 21].

Perhaps, the greatest outstanding problems concern the elicitation of, representation of, and computation with dependence. Everyone knows that the ubiquitous assumption of independence in uncertainty analysis is usually wrong, and sometimes seriously wrong. This is a subject that must receive more attention in the future [37].

## ACKNOWLEDGMENT

The authors gratefully acknowledge the contributions of many people who cooperated in developing this database. Willy Aspinall and Tim Bedford are independently responsible

for a quarter of the studies. This article is based on an article for a special issue, *Reliability Engineering and System Safety*, on expert judgment (doi:10.1016/j.ress.2007.03.001, available online 15 March 2007), which published reviewer comments. The present article incorporates part of the discussion with Clemen on out-of-sample validation.

## REFERENCES


1. Cooke, R. M. (1991). *Experts in Uncertainty*, Oxford University Press, Oxford.
2. Cooke, R. M. (1991). *Expert Judgment Study on Atmospheric Dispersion and Deposition Report Faculty of Technical Mathematics and Informatics No.01–81* , Delft University of Technology, Delft.
3. Goossens, L. H. J., Cooke, R. M., and Kraan, B. C. P. (1996). *Evaluation of Weighting Schemes for Expert Judgment Studies*, Final report prepared under contract Grant No. Sub 94-FIS-040 for the Commission of the European Communities, Directorate General for Science, Research and Development XII-F-6, Delft University of Technology, Delft.
4. Goossens, L. H. J., Cooke, R. M., and Kraan, B. C. P. (1998). Evaluation of weighting schemes for expert judgment studies. In *Proceedings PSAM4* , A. Mosleh, and R. A. Bari, Eds. Springer, New York, pp. 1937–1942.
5. Goossens, L. H. J., Cooke, R. M., Woudenberg, F., and van der Torn, P. (1998). Expert judgement and lethal toxicity of inhaled chemicals. *J. Risk Res.* 1(2), 117–133.
6. Goossens, L. H. J., Harrison, J. D., Harper, F. T., Kraan, B. C. P., Cooke, R. M., and Hora, S. C. (1998). *Probabilistic Accident Consequence Uncertainty Analysis: Internal Dosimetry Uncertainty Assessment*, Vols 1 and 2, Prepared for U.S. Nuclear Regulatory Commission and Commission of European Communities, NUREG/CR-6571, EUR 16773, Washington, DC, Brussels.
7. Cooke, R. M. (2004). The anatomy of the Squizzle –the role of operational definitions in science. *Reliab. Eng. Syst. Saf.* 85, 313–319.
8. NUREG/CR-6372 (1997). *Recommendations for Probabilistic Seismic Hazard Analysis:Guidance on Uncertainty and Use of Experts*, US Nuclear Regulatory Commission.
9. Winkler, R. L., Wallsten, T. S., Whitfield, R. G. Richmond, H. M. Hayes, S. R., and Rosenbaum, A. S. (1995). An assessment of the risk of chronic lung injury attributable to long-term ozon exposure. *Oper. Res.* 43(1), 19–27.
10. Budnitz, R. J., Apostolakis, G., Boore, D. M., Cluff, L. S., Coppersmith, K. J., Cornel, C. A., and Morris, P. A. (1998). Use of technical expert panels: applications to probabilistic seismic hazard analysis. *Risk Anal.* 18(4), 463–469.
11. Goossens, L. H. J., and Harper, F. T. (1998). Joint EC/USNRC expert judgement driven radiological protection uncertainty analysis. *J. Radiol. Prot.* 18(4), 249–264.
12. Cooke, R. M., Mendel, M., and Thijs, W. (1988). Calibration and information in expert resolution. *Automatica*, 24(1), 8–87–94.
13. Goossens, L. H. J., Cooke, R. M., and van Steen, J. (1989). *Final Report to the Dutch Ministry of Housing, Physical Planning and Environment: On The Use of Expert Judgment in Risk and Safety Studies*, Vols 1–5, TU Delft.
14. Yunusov, A. R. Cooke, R. M., and Krymsky, V. G. (1999). Rexcalibr-integrated system for processing expert judgement. In *Proceedings 9th Annual Conference Risk Analysis: Blz. 587–589: Facing the New Millennium*, L. H. J. Goossens, Eds. Delft University Press, ISBN: 90-407-1954-3, October 10–13, Rotterdam.
15. French, S. (1985). Group consensus probability distributions: a critical survey. In *Bayesian Statistics*, J. M. Bernardo, M. H. De Groot, D. V. Lindley, and A. F. M. Smith, Eds. Elsevier, North Holland, pp. 182–201.

16. Genest, C., and Zidek, J. (1986). Combining probability distributions: a critique and an annotated bibliography. *Stat. Sci.* 1(1), 114–1490.
17. Ter, Haar T. R., Retief, J. V., and Dunaiski, P. E. (1998). Towards a more rational approach of the serviceability limit states design of industrial steel structures paper no. 283. *2nd World Conference on Steel in Construction*, San Sebastian.
18. Akkermans, D. E. (1989). Crane failure estimates at DSM' Expert judgment in risk and reliability analysis; experience and perspective. *ESRRDA Conference, October 11, 1989*. Brussels.
19. Lopez de la Cruz, J. (2004). *Applications of Probability Models and Expert Judgement Analysis in Information Security*, Master's Thesis, TU Delft.
20. Van Elst, N. P. (1997). *Betrouwbaarheid beweegbare waterkeringen [Reliability of movable water barriers]*, *WBBM Report Series 35*, Delft University Press, Delft.
21. Chou, D., Kurowicka, D., and Cooke, R. M. (2006). Techniques for generic probabilistic inversion. *Comp. Stat. Data Anal.*, **50**, 1164–1187.
22. Goossens, L. H. J. (1994). *Water Pollution*, TU Delft for Dutch Mininstry of Environment, VROM.
23. Goossens, L. H. J., Cooke, R. M., Woudenberg, F., and van der Torn, P. (1992). *Probit Functions and Expert Judgment*, Report prepared for the Ministry of Housing, Physical Planning and Environment, The Netherlands; Delft University of Technology, Safety Science Group and Department of Mathematics, and Municipal Health Service, Rotterdam, Section Environmental Health.
24. Cooke, R. M., and Jager, E. (1998). Failure frequency of underground gas pipelines: methods for assessment with structured expert judgment. *Risk Anal.* 18(4), 511–527.
25. Brown, J., Goossens, L. H. J., Harper, F. T., Haskin, E. H., Kraan, B. C. P., Abbott, M. L., Cooke, R. M., Young, M. L., Jones, J. A., Hora, S. C., and Rood, A. (1997). *Probabilistic Accident Consequence Uncertainty Analysis: Food Chain Uncertainty Assessment*, Vols 1 and 2, Prepared for U.S. Nuclear Regulatory Commission and Commission of European Communities, NUREG/CR-6523, EUR 16771, Washington, DC, Brussels.
26. Goossens, L. H. J., Boardman, J., Harper, F. T., Kraan, B. C. P., Young, M. L., Cooke, R. M., Hora, S. C., and Jones, J. A. (1997). *Probabilistic Accident Consequence Uncertainty Analysis: Uncertainty Assessment for Deposited Material and External Doses*, Vols 1 and 2 Prepared for U.S. Nuclear Regulatory Commission and Commission of European Communities, NUREG/CR-6526, EUR 16772, Washington, DC, Brussels.
27. Harper, F. T., Goossens, L. H. J., Cooke, R. M., Hora, S. C., Young, M. L., Päsler-Sauer, J., Miller, L. A., Kraan, B. C. P., Lui, C., McKay, M. D., Helton, J. C., Jones, J. A. (1995). *Joint USNRC/CEC Consequence Uncertainty Study: Summary of Objectives, Approach, Application, and Results for the Dispersion and Deposition Uncertainty Assessment*, Vols 1–3, NUREG/CR-6244, EUR 15855, SAND94-1453, Washington, U.S. Nuclear Regulatory Commission and Commission of European Communities, DC, Brussels.
28. Cooke, R. M. (1994). Uncertainty in dispersion and deposition in accident consequence modeling assessed with performance-based expert judgment. *Reliab. Eng. Syst. Saf.* 45, 35–46.
29. Van der Fels-Klerx, H. J., Cooke, R. M., Nauta, M. J., Goossens, L. H. J., and Havelaar, A. H. (2005). A structured expert judgement study for a model of campylobacter transmission during broiler chicken processing. *Risk Anal*, **25**: (1), 109–124.
30. Offerman, J. (1990). *Safety Analysis of the Carbon Fibre Reinforced Composite Material of the Hermes Cold Structure*, TU-Delft/ESTEC, Noordwijk.
31. Willems, A. (1998). *Het gebruik van kwantitatieve technieken in risicoanalyses van grootschalige infrastructuurprojecten* (The use of quantitative techniques in risk analysis of

large infrastructural projects, in Dutch) Ministerie van Verkeer en Waterstaat, DG rijkswaterstaat, Bouwdienst, Tu Delft Masters Thesis, Delft.

32. Aspinall, W. (1996). *Expert Judgment Case Studies, Cambridge Program for Industry, Risk Management and Dependence Modeling*, Cambridge University, Cambridge.
33. Aspinall, W., and Cooke, R. M. (1998). Expert judgement and the Montserrat Volcano eruption. In *Proceedings of the 4th International Conference on Probabilistic Safety Assessment and Management PSAM4, September 13th–18th 1998*, Vol. 3, A. Mosleh, and R. A. Bari, Eds. Springer, New York, pp. 2113–2118.
34. Cooke, R. M., and Goossens, L. J. H. (2000). *Procedures Guide for Structured Expert Judgment*. Project report EUR 18820EN. Nuclear Science and Technology, specific programme Nuclear fission safety 1994–98, Report to: European Commission. Luxembourg, Euratom. Also in *Radiation Protection Dosimetry*, Vol. 90 No. 3.2000, 64 7, pp. 303–311.
35. Qing, X. (2002). *Risk Analysis for Real Estate Investment*, PhD Thesis, Department of Architecture, Delft University of Technology.
36. Bakker, M. (2004). *Quantifying Operational Risks within Banks According to Basel II*, Masters Thesis, Delft University of Technology, Department of Mathematics.
37. Kurowicka, D., and Cooke, R. M. (2006). *Uncertainty Analysis with High Dimensional Dependence*, John Wiley & Sons, New York.
38. Brown, A. J., and Aspinall, W. P. (2004). Use of expert opinion elicitation to quantify the internal erosion process in dams. *Proceedings of the 13th Biennial British Dams Society Conference*. University of Kent, Canterbury, 22–26th June 2004, p. 16.
39. Aspinall, W. P., Loughlin, S. C., Michael, F. V., Miller, A. D., Norton, G. E., Rowley, K. C., Sparks, R. S. J., and Young, S. R. (2002). The Montserrat volcano observatory: its evolution, organisation, role and activities. In *The Eruption of Soufrière Hills Volcano, Montserrat, from 1995–1999*, T. H. Druitt, and B. P. Kokelaar, Eds. Geological Society, London.
40. Claessens, M. (1990). *An Application of Expert Opinion in Ground Water Transport (in Dutch)*, DSM Report R 90 8840, TU Delft.
41. Cooke, R. M., and Slijkhuis, K. A. (2003). Expert judgment in the uncertainty analysis of dike ring failure frequency. In *Case Studies in Reliability and Maintenance*, W. R. Blischke, and D. N. Prabhakar Murthy, Eds. ISBN: 0-471-41373-9, John Wiley & Sons, New York, pp. 331–352.
42. Goossens, L. H. J., Cooke, R. M., Woudenberg, F., and van der Torn, P. (1995). Probit relations of hazardous substances through formal expert judgement. *Loss Prevention and Safety Promotion in the Process Industries*, Vol. 2, Elsevier Science B.V., pp. 173–182.
43. Kraan, B., and Bedford, T. (2005). Probabilistic inversion of expert judgments in the quantification of model uncertainty. *Manage. Sci.* 51(6), 995–1006.

## FURTHER READING

Frijters, M., Cooke, R. Slijkuis, K., and van Noortwijk, J. (1999). *Expert Judgment Uncertainty Analysis for Inundation Probability, (in Dutch) Ministry of Water Management*, Bouwdienst, Rijkswaterstaat, Utrecht.

De Wit, M. S. (2001). *Uncertainty in Predictions of Thermal Comfort in Buildings*, PhD. Dissertation, Department of Civil Engineering, Delft University of Technology, Delft.

Haskin, F. E., Goossens, L. H. J., Harper, F. T., Grupa, J., Kraan, B. C. P., Cooke, R. M., and Hora, S. C. (1997). *Probabilistic Accident Consequence Uncertainty Analysis: Early Health Uncertainty Assessment*, Vols 1 and 2, Prepared for U.S. Nuclear Regulatory Commission and Commission of European Communities, NUREG/CR-6545, EUR 16775, Washington, DC, Brussels.

Meima, B. (1990). *Expert Opinion and Space Debris*, Technological Designer's Thesis, Faculty ot Technical Mathematics and Informatics, Delft University of Technology, Delft.

Sarigiannidis, G. (2004). *CARMA-Greece: An Expert Judgment Study and the Probabilistic Inversion for Chicken Processing Lines*, Masters Thesis, Delft University of Technology, Department of Mathematics.

Sparks, R. S. J., and Aspinall, W. P. (2004). Volcanic activity: frontiers and challenges in forecasting, prediction and risk assessment. In *State of the Planet: Frontiers and Challenges*, *Geophysical Monograph Series*, R. S. J. Sparks, and C. J. Hawkesworth, Eds. IUGG/AGU Vol. 150, p. 414.

Van Overbeek, F. N. A. (1999). *Financial Experts in Uncertainty*, Masters Thesis, Department of Mathematics, Delft University of Technology, Delft.

Willems, A., Janssen, M., Verstegen, C., and Bedford, T. (2005). Expert quantification of uncertainties in a risk analysis for an infrastructure project. *J. Risk Res.* 8(12), 3–17.

# SECURITY AND SAFETY SYNERGY

NICKLAS DAHLSTRÖM AND SIDNEY DEKKER
*Lund University School of Aviation, Ljungbyhed, Sweden*

## 1 INTRODUCTION

Security and safety are concepts that share important features; they both involve the risk of occurrence of events with consequences that may range from trivial to disastrous. Yet as concepts they are also different, with security relating to intentional acts by individuals and safety relating to events caused by unintended consequences of a combination of a host of factors. In safety-critical industries, such as aviation and maritime transport, chemical and nuclear industry, and health care, safety is seen as the positive outcome of management of problems and trade-offs that are rooted in systems' complexity, goal interaction, and resource limitations. This perspective has led safety research to shift focus and go beyond individual acts (such as "human error") and move to systematic aspects of human, technological, and organizational performance [1]. It involves dealing with problems connected to regulations and standardized procedures, technology and automation, and efforts to understand the impact of communication, group dynamics, leadership, and culture on safety. The advancement of security issues in a complex modern society should be able to benefit from the knowledge gained through safety

industry operations in the field of Human Factors. This knowledge has the potential to make security more safe (for those who design and implement security measures as well as for those who are subjected to them) and effective (in terms of time and resources spent on security measures).

Organizations do not exist just to be secure or safe. They exist to produce or provide goods or services. Customers care about the goods or service—that is why they engage with the organization in the first place (Even where security actually is the goal of an organization it is provided as a complement to another product or activity—protection of property, transportation, etc.). This means that an understanding of the fundamental conditions for security and safety begins with an understanding of the balance between production and protection. Humans normally strive for an acceptable (rather than ideal) level of performance in relation to their goals and resources [2] and to not process all available data is a part of this resource-saving strategy [3]. Consequently, action is guided by an intuitive and implicit trade-off between cost and efficiency [4] or between thoroughness and efficiency [5]. However, this introduces the risk of overlooking possible consequences of these trade-offs, particularly long-term consequences [6]. From investigations of aviation accidents the systematic trade-offs in favor of efficiency/production versus safety/protection have been labeled as "drift" toward accidents [7]. The model of drift has been an important tool for increased understanding of accidents in the otherwise impressively safe global transportation system of aviation. Drift should also be a useful concept for understanding of failure of security systems. In the 24 months leading up to 9/11, there were 30 cases of passengers breaking through cockpit-doors [8]. This type of event may at the time have been recognized as an acceptable risk.

## 2 THE PRESENT SITUATION FOR SECURITY

Today, the situation is quite different. The pressure to respond quickly and decisively to perceived security threats can produce immense consequences—from severe disruption to significant financial loss. A recent example of this is the consequences of the events in the United Kingdom in September, 2006:

> "In the wake of the plot to smuggle liquids on board aircraft, mix them and use them as explosives the increased security measures during the following nine days meant that British Airway had to cancel about thousand flights resulting in estimated losses of 50 million pounds [9]."

In aviation, security is generally seen as an operational activity parallel and independent to safety. However, it is not unusual that security even by crews is seen as an intrusion (when performed by security staff) or as unwanted and unnecessary (when performed by crews themselves). There are even examples of how security and safety may conflict. The most prominent example, of course, is the locked cockpit door. The extra barrier can delay or interfere with cross-crew coordination, which has been identified previously as contributory to accidents [10]. A locked door can be especially problematic in case of escalating situations (disruptive passengers, or technical problems) where the threshold for coordinating may now have become higher. In a report by Nilsson and Roberg [11], crew members were unanimously negative in their view of the locked door. A manifestation of this problem occurred on an Air Canada Jazz flight in 2006. As a

captain returned from using the washroom in the cabin he could not get back into the cockpit. It was not possible to open the door:

> "For roughly 10 minutes, passengers described seeing the pilot bang on the door and communicating with the cockpit through an internal telephone, but being unable to open the cabin door. Eventually, the crew forced the door open by taking the door off its hinges completely, and the pilot safely landed the plane [12]."

The article also stated that "being locked out of the cockpit is a 'nonreportable' incident, there is no way of confirming their frequency as the airlines are under no obligation to report them". Beyond the entertaining qualities of this story, it raises questions regarding the parallel pursuit and of security and safety and their interaction.

## 3 EVOLUTION OF SAFETY, REVOLUTION OF SECURITY

Aviation safety has evolved, slowly but surely, over many decades. Technological, organizational, and regulatory developments, as well as greater insights into human and team performance, have all contributed to the steady "fly-fix-fly" improvement of aviation safety. Aircraft accidents have become a part of contemporary mythology—crowning heroes, identifying culprits and providing horror stories. All of this experienced and recounted by passengers to the rest of us; potential passengers who could have or may come to be caught up in similar events. There is not any abundance of similar stories and certainly not any similar mythology when it comes to aviation security. Although there certainly are hero stories (as that of the passengers of flight United 93), clear identification of culprits (as in cases of hijackings and bombings), and horrors to be shared also in this area the occurrence of such events have simply not been as frequent as safety-related accidents. Of course frequency alone explains little, but the abundance of safety-related accidents has produced numerous articles, books, documentaries, and movies that have helped to increase public awareness on safety issues. Such stories have also been successfully used in the training of airline crews in human limitations, communication, cooperation, and leadership for increased safety (Crew Resource Management (CRM) training). Security demands, in contrast to the gradual development of safety measures, have exploded dramatically over the past few years. This sudden tightening and acceleration could compromise the claim that security provides an essential service to society. See, as an example, this comment on the response after 9/11:

> "Confiscating nail files and tweezers from passengers seems like a good idea all around: The airlines don't mind because it doesn't cost them anything, and the government doesn't mind because it looks like it's doing something. The passengers haven't been invited to comment, although most seasoned travelers simply roll their eyes [13]."

Security measures can appear quite haphazard, arbitrary—capricious even—to passengers or crews or other people subjected to them. Computers that have to be taken out of bags at some airports but not at others. Elderly ladies must give up their knitting ware before entering an aircraft while other passengers do not need to give up elegant and equally sharp pens. "Incendiary material" may not be brought onto an aircraft but alcohol (to drink or to smell better) is accepted and even sold onboard. Every piece of such failing logic will gradually or quickly erode the willingness of those who are supposed

to be felt protected, to see themselves as participants guaranteeing their own security. Although the pictures from 9/11 will be remembered and should seem to provide more than enough of modern mythology the patience of passengers and willingness to accept current security measures is probably not endless. This is one perspective on the current status of security:

> It's been four years since the terrorist attacks of Sept 11, 2001, and backups at airport security checkpoint lines are growing, the army of federal airport screeners is still getting low performance marks and uncertainty dogs the contents of airline cargo holds. While the federal government has been spending about $4 billion a year on aviation security since hijackers transformed four jetliners into devastating weapons, critics say there aren't enough results to show for all that taxpayer money [14].

### 3.1 Production Pressures in Providing Security

As potential goodwill in regard to security might abate, there is a risk that mounting production pressures dictate the operational conditions for security operations. The effects of such production pressures have been seen in a vast number of aviation safety incidents and accidents and they are likely to have an influence also on security. A study of airport screening rather unsurprisingly found that "the longer passengers had to wait, the longer they were to be unsatisfied" and concluded that "There is little question that the effectiveness and efficiency of security screening is a key feature affecting passenger satisfaction" [15]. To reduce this problem computer-assisted passenger prescreening systems have been introduced and these "confirms passengers' identities, performs criminal and credit checks, and retrieves additional information, such as residence, home-ownership, income, and patterns of travel and purchases, used to construct a predicted threat rating" [16]. With the currently fierce competition in the aviation industry—between airlines (increased by the arrival of low-cost carriers), between airlines and business jets, and from high-speed trains (in many parts of Europe)—many security measures will be under pressure to adapt to the demands of "effectiveness and efficiency" from a short-term business perspective rather than to what passengers perceive as illogic and irrelevant threats stemming from vague and remote risks of criminal acts and terrorism.

A new segment of the aviation industry is partly based on the consequences of current security measures. An important reason for the emergence and anticipated success of a new type of small business jet aircraft (Very Light Jets, VLJs) is that the time demanded by security measures for scheduled flight at major airports is unacceptable for upper and middle management [17]. By operating or renting their own aircraft, flying direct and using small airports some of the time spent on security can be avoided or reduced for companies. The same reason has fueled a "remarkable upturn in business aviation" in Europe in recent years [17]. The experience from aviation safety is that this and other types of pressures on operations affect all organizational levels and induce risks of organizational drift toward future system failures.

To further understand the current relationship that passengers (or the public in general) have to security (as well as to safety) in aviation we can use two concepts from economic theory. The first is that of "externalities", that is a cost or benefit imposed on people other than those who purchase a good or service [18, 19]. Passengers buy a ticket to fly from A to B and expect this to be a secure and safe means of transportation (For the airline industry to imply anything else would be to discourage a substantial number of passengers.). Since security and safety are expected from this product and criminal

acts with severe consequences or accidents are rare (and this is stressed by the industry), consumers will see increased prices or procedural complications for flying as a negative externality. Of course, they do understand the need for baggage-screening and de-icing, but in day-to-day travel the meaning of these procedures often seems lost, as noted on consumer behavior "the tendency to trade-off costs and benefits in ways that damage their future utility in favor of immediate gratification" [20]. The paradox is that for the airline industry it is of great importance to be secure and safe to a level where passengers do not even consider potential threats when they make their decision to travel. As this level is achieved, however, passenger tolerance for increased costs and inconveniences to further reduce threats is declining. This explains the fundamental difficulties that everyone (security managers, pilots, cabin crew, screeners, etc.) involved in working with security encounters in day-to-day operations when trying to maintain the balance between production demands and the protection provided by the security system.

The tendencies described by the theory of externalities can be further reinforced by the theory of "lemons" [21]. This describes how interaction between quality differences and asymmetrical information can cause a market where guarantees are unclear to disappear. When quality is indistinguishable beforehand to the buyer (due to the asymmetry of information) incentives exist for the seller to pass off a low-quality good as a higher-quality one. Since the nonoccurrence of adverse security and safety cannot be guaranteed, the quality of security and safety operations is known to very few (and in the case of security we do want to keep this a secret) there is no incentive for any consumer of airline transport services to select airport or airline based on if they are more secure or safe than other. This explains the pressure put on the security and safety operations as it is unlikely that they ever will be able to provide evidence of the value they bring to the consumer [22].

## 4 EXPERIENCES FROM AVIATION HUMAN FACTORS OF RELEVANCE FOR SECURITY

### 4.1 Relation to Regulation, Standardization, and Procedures

Economic theories of human behavior provide us with some understanding of its potential problems with regards to security and safety. A seemingly reasonable response would then be to try to control human behavior. This means using laws, regulations, standardized procedures, manuals, guidelines, and other similar means to increase the reliability of human behavior and limit the risk it may induce in systems. Aviation has a long tradition of negotiating global regulatory frameworks that can ensure a high minimum level of safety [23]. Manufacturing and maintenance of aircraft, medical and other requirements for staff (pilots, cabin crew, air traffic controllers, etc.) selection and training as well as practically all operational aspects are guided by extensive regulation and enforced by aviation authorities. The regulations stipulate that all operators also should have standard operational procedures (SOPs) for all aspects of operation. In aviation these procedures are regarded by crews as the main source of safety and regulations demand that they are regularly practiced to a satisfactory standard in simulators, mock-ups, or classroom teaching.

Many think that regulation, standardization, and proceduralization are the main guarantors of aviation safety. Even though this might be historically true, the situation has always been more complex. While these efforts promote predictable organizational and

individual behavior and increase reliability they do not promote the flexibility to solve problems encountered in present complex sociotechnical systems [24]. Also, a blind adherence to regulations and procedures neglects the fact that much work has to be done in addition to, beyond or contrary to prescribed procedures [24]. A procedure is never the work itself, it cannot be that human intervention is always necessary to bridge the gap from written guidance to actual application in context. Note how the "work-to-rule" strike is not uncommon as a form of industrial action in aviation. Yet the commitment to rules and procedures is generally strong in aviation (although there are weaknesses in this commitment in some parts of the world). However, there are signs that further increase of aviation safety may need other methods than those used to achieve current levels of safety [25]. Most potential system failures in aviation have been anticipated and addressed by technical protection and procedural responses. But ill-defined, unexpected, and escalating situations have proved to be far more difficult to manage successfully and have resulted with tragic outcomes. An example of this is the in-flight fire on Swissair 111 [26], where the flight crew tried to follow procedures until the situation was entirely out of control. This accident showed that an overfocus on procedures and lack of training of general competencies needed in an emergency may conspire to turn a difficult situation to an unmanageable one.

When putting security systems together, training staff to achieve increased standardization and procedural adherence may be an intuitive and relevant first step. But further consideration is necessary. A profound understanding of human performance issues (including topics such as perception, decision making, communication, cooperation, and leadership) should be helpful to security staff for increasing the overall effectiveness of security operations. Such training should go beyond operational and procedural aspects, instead providing security staff with an increased awareness of the individual, group, and system limitations that may induce weaknesses in the security system. This training should be recurrent and closely integrated with other training as well as with an effective operational reporting system (see below).

### 4.2 Relation to Technology and Automation

As has been, and still is, the case for aviation safety, security seems to be driven by a reliance on technology to solve problems and increase efficiency (increased use of advanced identity cards, biometrics, surveillance cameras, sensors, background checks, data mining and for aviation specifically refined screening techniques, computer aided vetting of passengers, etc.). Focusing on technology is a prominent feature in the modern history of aviation safety [27]. The experiences of this development can provide some helpful guidance for security. Two important phases will be used as examples of the problems involved in the relation between aviation safety and technology.

The first great technological step of improving the safety of modern air transportation depended upon increased understanding of the physical stresses on aircraft frames as well as of fundamental physiological and psychological processes affecting pilots. As aviation entered the jet-age, safety increased due to the superior performance and reliability of jet engines compared to piston-engines. To be able to fly faster and higher than before did, however, have unforeseen consequences and in-flight break-up of aircraft (such as the Comet accidents in the 1950s) put the focus on the risks of structural failure. This focus on fundamental engineering and manufacturing issues corrected previous design flaws for coming generations of aircraft. Another accident type was that connected to

approaching an airport in darkness. This induces the risk of the so-called black-hole illusion, where the airport is perceived as being lower than it actually is. Accidents of this type were frequent until there was a push for instrument landing systems on more airports, improved instrument design, and more warning systems, which reduced the risk of this type of accident. Also, the opportunities for effective flight simulation provided by the technological development meant that this type of approach and landing could be practiced effectively. In both cases, the measures taken were relevant and had positive effects on aviation safety. However, aircraft accidents were steadily occurring even after these measures had been implemented. These accidents involved failures of communication, cooperation, and leadership problems, such as the United 173 accident at Portland airport or the Air Florida 90 accident at Potomac Bridge where the captain's decisions were accepted by other crew members in spite of their awareness of the risks involved. The existence of these types of problems was well known to the industry but previously obscured by the search for technological solutions. They did, however, become addressed through increased focus on Human Factors and the implementation of CRM-training in the industry.

In the 1980s, the arrival of modern computer technology in large transport aircraft was supposed to solve safety problems and reduce costs. New aircraft were equipped with computerized Flight Management Systems (FMS) which were supposed to not only reduce the workload of the pilots, but also monitor their actions and prevent actions that would risk the safety of the aircraft. The most important learning point to come out of the technological revolution in the cockpit was that changing the conditions for work always may solve some known safety problems but it will always create new ones [28]. Although the introduction of the new technology was a part of an overall trend toward greater safety it was also involved in a number of incidents and accidents where a mismatch between the human operator and the automation was the primary cause [29]. This included accidents with mode confusion (such as China Airlines at Nagoya and Air Inter at Strasbourg), programming errors of the FMS (Boeing 757 accident at Cali, Colombia), and aircraft upset (conflicting aircraft and operator control of the aircraft, such as the JAS Gripen accident in Stockholm). Again, the focus on technological solutions obscured the essential focus on its effects on the role of the human operator. There is a lesson here. As pressure mounts to make security more cost effective, time effective, and less inconvenient, the history of aviation automation may serve as a reminder that new technology alone is seldom the solution.

### 4.3 Human Performance, Communication, Cooperation and Leadership-Training and Reporting

An area where aviation safety has made significant progress is in training their operators in understanding potential safety risks associated with human performance, communication, coordination breakdowns, and leadership. Such training has been facilitated by the availability of well-investigated cases of aviation accidents. Gradually this type of training has gained increased recognition, both within aviation as well as in other safety-critical industries. The mandatory and recurrent training of Human Factors–related knowledge and skills is today a hallmark of the aviation industry and has become a model for similar training in maritime transportation, nuclear and chemical industry as well as health care.

The emergence of the concept of Cockpit Resource Management in the late 1970s was precipitated by a number of disastrous accidents (e.g. the most disastrous of them

all, where 583 persons became victims as two aircraft collided on the runway on the island of Tenerife). This became the start of a systematic approach to train crews to understand aspects of human performance, communication, cooperation, and leadership of importance to aviation safety. Later, the concept was renamed CRM, to involve also the cabin crew (This too was precipitated by accidents, such as the Kegworth accident, where information from cabin crew on visible effects of engine problems did not make it into the cockpit to augment the pilot's knowledge of the situation.). Analogously, engineering and technical staff have developed the concept of Maintenance Resource Management (MRM). In many countries, annual recurrent CRM courses are mandatory for maintaining active status for an airline pilot's license. Currently, there are ongoing discussions as to if CRM should be made available or even mandatory also for other categories of staff involved in operations, such as schedulers, coordinators, and management. The initials CRM would then stand for Company Resource Management.

Gradually, the focus of CRM-training has been turned to prevention and management of human error, based on the same content as previously but more explicitly framed around understanding error. This has included teaching of various accident models. Although the success of CRM is difficult to quantify in terms of fewer accidents or incidents or in any other measurable terms of increased safety or economic gain, the great interest from other industries (maritime transport, nuclear, chemical, and health care) in the concept seem to confirm its appeal.

One of the lesser discussed benefits of CRM-training is that it widens the understanding of human performance and, as a consequence, the willingness to report events and incidents. To create an overall effective system for safety (or security), it is important to first create an organization that is curious regarding error rather than one where punishment expected and thus reporting is avoided. Curiosity is a sign of willingness to learn why a certain event occurred and a starting point for learning for the whole organization. In aviation, it is not uncommon that crews report their own errors even though there would have been no way to detect that an error had been committed; since there is no good reason that other crews should have to experience the same error. The benefits of this type of reporting and of CRM-training are not easy to quantify and might be more convincingly argued in connection to examples from operations. In the period of 1997 to 2001 one of the four terminals at Sky Harbor airport in Phoenix, Arizona, had 125 security lapses [30]. The Transportation Security Administration (TSA) screener workforce alone consists of 45,000 employees at 448 airports [31]. From aviation safety we would conclude that this type of events will not disappear. But by complementing increasingly effective technological solutions with equally effective training and reporting there will be less of them.

Recurrent training of both security and safety (first aid, evacuation, fire-fighting, CRM) is mandatory for airline crews. These training events not only reinforce practical skills but also serve as important reminders of the threats and risks surrounding airline operations. It also gives crews the opportunity to discuss recent security- or safety-related events and come up with solutions to operational problems. If carried out according to its intentions, recurrent security, and safety, training strengthens organizational values and attitudes regarding their areas. Security staff could also benefit from systematic recurrent training of CRM-type, focused less on strict operation of technological equipment and more on Human Factors aspects of work.

### 4.4 Models and Culture

Beyond the training of individual operators, research efforts to understand (and increase) safety have focused on formulation of models that can explain how accidents occur and how they can be prevented. Traditional models have relied heavily on statistical analysis and vast representations of actions in search of a "root cause" for an accident. Also, they commonly rely on "folk models", that is general explanatory labels that only rename a phenomenon and do not actually provide any deeper analysis [32]. In recent times, highly influential models have focused more on "soft" organizational factors such as the norms and cultures in organizations and the effect of the balance between production and protection and how it is played out interactively between levels of an organization.

In the last decade, the concept of "culture" has received increased attention in safety research. People now refer to the lack of a sound "safety culture" as a reason for incidents and accidents. The focus on safety culture was preceded by attention in managerial literature on "organizational culture" or "company culture" [33]. From this the concept safety culture emerged and has been embraced in many industries. A safety culture is characterized as an "informed culture", that is the organization collects and analyses safety-related data to keep it informed on the safety status of the organization [34]. In particular, the following aspects of a safety culture are highlighted:

- *Reporting* — is considered of fundamental importance in the organization.
- *Just* — unintentional acts are not punished which creates trust to report.
- *Flexible* — ability to adapt to new information and changing circumstances.
- *Learning* — ability to extract learning from safety-related information.

There does not seem to be an equivalently researched and accepted "security culture", although this probably should be a term as relevant as it has proved to be for safety. Certainly, the concept seem to be implicitly present, as indicated by this statement: "because enhancing security depends on changing the beliefs, attitudes, and behavior of individuals and groups, it follows that social psychology can help organizations understand the best way to work with people to achieve this goal" [35].

Learning is, however, a dialectical aspect of culture. In the balance between production and protection the learning from day-to-day operations may easily be the contrary of that implied by Murphy's Law, that is, that things that can go wrong usually do. Actually, in normal operations things that can go wrong do not and there is a risk of learning the wrong lesson from this. Operators might interpret incidents as proof of safety and that it is ok to "borrow from safety" to increase production output. Production pressure on performance of "normal work" gradually effect standards and norms of this work in favor of production. This is the risk described by the model of "organizational drift" toward failure for complex sociotechnical systems. In security, drift of normal practice may create opportunities for those who deliberately want to cause harm to people and property.

Aspects of safety culture are present also in research on high reliability organizations (HROs) such as aircraft carriers and air traffic control [36]. One of the conclusions of this research is that stories that organizations tell about their own operations reveal something about their attitude and ability to learn from incidents. In HROs, incidents are seen as signs of weaknesses in the system and they are used by the organization to extract information about how to become safer. In other organizations incidents may be taken as evidence of the strength of the safety system and lead to the conclusion

that nothing needs to be changed. From this it could be claimed that something that is needed for security operations, particularly for training, is "good stories", both about the failure and success of its operations. While aviation safety has been able to use cases from well-investigated and publicly presented accidents, this is not the case for security.

There are a number of models and research results regarding safety culture and HROs that should be fruitful for security operations. The similarities of the conditions and performance of security and safety operations mean that learning from each other should be mutually beneficial. Both represent operations where seemingly everything is done to prevent adverse events, where adverse events are extremely rare (and potentially disastrous). Also, for both the operators have to maintain a high level of skills, knowledge, and awareness to keep day-to-day operation secure and safe as well as readiness to manage unusual and unpredicted events. The potential for systematic and recurrent Human Factors training for security as well as for joint security and safety training for staff from both types of operations should be explored.

## 5 CONCLUSION

Security and safety share fundamentally important features as operational activities with the goal to protect people, property, and the smooth economical functioning of organizations and society. Safety has been a focus of operations where risks have been overwhelmingly obvious since their inception (e.g. aviation, chemical, and nuclear industry) and demands on the safety of these operations have gradually increased. The demand for increased security has escalated recently and comprehensive development of it as a field of operations, beyond potential technological progress, is needed.

In spite of distinct differences in the nature of threats (intentional/unintentional), there are many areas (use of standardized procedures, human factors training, modeling for increased understanding of adverse events) where knowledge and experiences from safety operations can fruitfully spill over to security. To establish cooperation between these two fields, for example on regulatory and procedural development, training and simulation, as well as operational evaluation, would be to produce synergies not yet known today.

## REFERENCES

1. Dekker, S. W. A. (2006). *The Field Guide to Understanding Human Error*, Ashgate Publishing, Aldershot.
2. Simon, H. A. (1957). *Models of Man: Social and Rational*, John Wiley and Sons, New York.
3. Besnard, D., and Arief, B. (2004). Computer Security impaired by legitimate users. *Comput. Comput.* **23**, 253–264.
4. Bainbridge, L. (1993). *Difficulties in Complex Dynamic Tasks*, Discussion paper available at (2nd of February 2007): http://www.bainbrdg.demon.co.uk/Papers/CogDiffErr.html.
5. Hollnagel, E. (2002). Understanding accidents—From root causes to performance variability. *Proceedings of the 7th IEEE Human Factors Meeting*. Scottsdale, AZ.
6. Dörner, D. (1997). *The Logics of Failure*, Perseus Books, Cambridge, MA.
7. Dekker, S. W. A. (2002). *The Field Guide to Human Error Investigations*, Ashgate Publishing, Ashgate.
8. Thomas, A. R. (2003). *Aviation Insecurity: The New Challenges of Air Travel*, Prometheus Books, New York, p. 13.

9. Schofield, A. (2006). Security standoff. *Aviat. Week Space Technol.* **165**(8), 53.
10. Chute, R., Wiener, E. L., Dunbar, M. G., and Hoang, V. R. (1995). Cockpit/Cabin crew performance: recent research. *Proceedings of the 48th International Air Safety Seminar*. Seattle, WA, November 7–9.
11. Nilsson, M., and Roberg, J. (2003). Cockpit Door Safety—How does the locked cockpit door affect the communication between cockpit crew and cabin crew? In *Examination paper presented at Lund University School of Aviation*, Lund University School of Aviation, Ljungbyhed, Sweden.
12. Global National (2006). *Pilot Locked Out of Jazz Cabin Mid-flight*, Available at (4th of February 2007): http://www.canada.com/topics/news/national/story.html?id=ac82a8ec-3915-48f4-ad8d-e65274b8204a&k=44392
13. Schneier, B. (2006). *Beyond Fear—Thinking Sensibly About Security in an Uncertain World*, Copernicus Books, New York, p. 33.
14. Doyle, A. (2005). Security dilemma. *Aviat. Week Space Technol.* **163**(8), 52.
15. Gkritza, K., Niemeier, D., and Mannering, F. (2006). Airport security screening and changing passenger satisfaction: An exploratory assessment, p. 217, 219. *J. Air Transp. Manag.* **12**, 213–219.
16. Persico, N., and Todd, D. E. (2005). Passenger profiling, imperfect screening and airport security, p. 127. *Am. Econ. Rev.* **95**(2), 127–131.
17. Lehman, C. (2006). Complementary, my dear Watson. *Civ. Aviat. Train. Mag.* **6**, 6.
18. Simpson, B. P. (2003). *Why Externalities are Not a Case of Market Failure*, Available at (4th of February 2007): http://www.mises.org/asc/2003/asc9simpson.pdf.
19. Schneier, B. (2006). *Beyond Fear—Thinking Sensibly About Security in an Uncertain World*, Copernicus Books, New York.
20. Acquisti, A., and Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Secur. Priv. Mag.* **3**(1), 26–33.
21. Akerlof, G. A. (1970). The market for lemons: quality uncertainty and market mechanism. *Q. J. Econ.* **84**(3), 488–500.
22. Anderson, R. (2001). Why information Security is hard—An economic Perspective. Paper presented at the *17th Annual Computer Security Applications Conference*. Available at (1st of February 2007): http://www.acsa-admin.org/2001/papers/110.pdf.
23. Abeyratne, R. I. R. (1998). *Aviation Security: Legal and Regulatory Aspects*, Ashgate Publishing, Brookfield, VT.
24. Dekker, S. W. A. (2005). *Ten Questions About Human Error: A New View on Human Errors and Systems Safety*, Lawrence Erlbaum Associates, Mawhah, NJ.
25. Amalberti, R. (2001). The paradoxes of almost totally safe transportation systems. *Saf. Sci.* **37**(2-3), 109–126.
26. Transportation Safety Board of Canada (2003). *Aviation Investigation Report Number A98H0003*, Available at (1st of February 2007): http://www.tsb.gc.ca/en/reports/air/1998/a98h0003/a98h0003.asp.
27. Billings, C. E. (1996). *Aviation Automation: The Search for a Human-centered Approach*, Lawrence Erlbaum Associates, Mawhah, NJ.
28. Dekker, S. W. A. (2002). *The Field Guide to Human Error Investigations*, Ashgate Publishing, Aldershot.
29. Dekker, S. W. A., and Hollnagel, E. (1999). Computers in the cockpit: Practical problems cloaked as progress. In *Coping with Computers in the Cockpit*, S. W. A. Dekker, and E. Hollnagel, Eds. Ashgate Publishing, Aldershot, pp. 1–6.
30. Clois, W., and Waltrip, S. (2004). *Aircrew Security: A Practical Guide*, Ashgate Publishing, Aldershot, p. 3.

31. Bullock, J., and Haddow, G. (2006). *Introduction to Homeland Security*, 2nd ed., Butterworth-Heinemann, Burlington, MA, p. 213.
32. Dekker, S. W. A., and Hollnagel, E. (2003). Human factors and folk models. *Cogn. Technol. Work* **6**(2), 79–86.
33. Deal, T. E., and Kennedy, A. A. (1982). *Corporate Cultures: The Rites and Rituals of Corporate Life*, Penguin Books, Harmondsworth.
34. Reason, J. (1997). *Managing the Risks of Organizational Accidents*, Ashgate Publishing, Aldershot.
35. Kabay, M. (1993). Social psychology holds lessons for security experts. *Comput. Can.* **19**(24), 33.
36. Rochlin, G. I. (1993). Defining high-reliability organization in practice: a taxonomic prolegomenon. In *New Challenges to Understanding Organizations*, K. H. Roberts, Ed. MacMillan, New York, pp. 11–32.

# CRITICAL INFRASTRUCTURE PROTECTION DECISION MAKING

DENNIS R. POWELL
*Los Alamos National Laboratory, Los Alamos, New Mexico*
SHARON M. DELAND
*Sandia National Laboratories, Albuquerque, New Mexico*
MICHAEL E. SAMSA
*Argonne National Laboratory, Argonne, Illinois*

## 1 INTRODUCTION

The critical infrastructure protection decision support system (CIPDSS) is a Department of Homeland Security (DHS) risk assessment tool and analysis process that (i) simultaneously represents all 17 critical infrastructures and key resources [1] in a single integrated framework and (ii) includes a decision-aiding procedure that combines multiple, nationally important objectives into a single measure of merit so that alternatives can be easily compared over a range of threat or incident likelihoods. At the core of this capability is a set of computer models, supporting software, analysis processes, and decision support tools that inform decision makers who make difficult choices between alternative mitigation measures and operational tactics or who allocate limited resources to protect

the United States' critical infrastructures against currently existing threats and against potential future threats. CIPDSS incorporates a fully integrated risk assessment process, explicitly accounting for uncertainties in threats, vulnerabilities, and the consequences of terrorist acts and natural disasters. Unlike most other risk assessment tools, CIPDSS goes beyond the calculation of first-order consequences in one or just a few infrastructures and instead models the primary interdependencies that link the 17 critical infrastructures and key resources together, calculating the impacts that cascade into these interdependent infrastructures and the national economy.

## 2 BACKGROUND

Choices made and actions taken to protect critical infrastructures must be based on a thorough assessment of risks and appropriately account for the likelihood of threat, vulnerabilities, and uncertain consequences associated with terrorist activities, natural disasters, and accidents. Initiated as a proof-of-concept in August 2003, the CIPDSS project has conducted analysis on disruption of telecommunications services, a smallpox outbreak and an influenza pandemic, and the accidental release of a toxic industrial chemical. Partial capability does exist to support analysis of physical disruption; cyber, insider, radiological or nuclear threats; and natural disaster scenarios.

### 2.1 Decision Support System and Infrastructure Risk

The project was developed in a system dynamics language (Vensim) to facilitate rapid development of capability. This decision support system is designed to address various infrastructure- and risk-related questions, such as these example questions:

- What are the consequences of attacks on infrastructure in terms of national security, economic impact, public health, and conduct of government—including the consequences that propagate to other infrastructures?
- Are there critical points in the infrastructures (i.e. areas where one or two attacks could have extensive cascading consequences)? What and where are these points?
- What are the highest risk areas from a perspective incorporating consequence, vulnerability, and threat?
- What investment strategies can the United States make that will have the most impact in reducing overall risk?

### 2.2 Two Modeling Scales: National and Metropolitan

The system has been designed to operate at two distinct scales of modeling: the national scale and the metropolitan scale. The national model represents the critical infrastructures at the national level, with resolution at a state level. The metropolitan (metro) model is intended to represent the functions of critical infrastructures at the local level, in urban landscapes with a population of 500,000 or more.

Within these two modeling scales, many questions of critical infrastructure disruption can be addressed within a risk-informed framework. In general, both the models calculate the consequences of a disruption both within the affected sector and in related sectors linked by primary interdependencies. For example, a disruption in telecommunications could have an effect on banking and finance and even on traffic. Consequences are

computed in the broad metric categories of human health and safety, environmental effects, economic costs, public confidence, and national security.

### 2.3 Decision Model

Unique to CIPDSS is the coupling of the vulnerability and consequence simulation models with a decision model. This tool translates simulated fatalities, illnesses and injuries, economic costs, lost public confidence, and national security impacts into a single measure of merit for each mitigation measure, operational tactic, or policy option considered by a decision maker in a decision problem. Preferred options are plotted against threat or incident likelihood. As new intelligence information becomes available and as the view of the intelligence community evolves with respect to the near- and long-term capabilities and intentions of US adversaries, a preferred course of action that minimizes overall risk can be easily selected from a growing set of threat case studies.

## 3 INFRASTRUCTURE MODELS

Each infrastructure sector is represented by a model of the system that is captured in a system dynamics representation. Table 1 lists the critical infrastructures modeled in CIPDSS. The most common model form is a limited-capacity, resource-constrained model as shown in Figure 1. In this generic representation, the model is shown as a network of nodes, for example, variables that are linked by directed edges, or influences. The connection of variable A via a directed edge to variable B indicates that the value of A is used to calculate the value of B. This abstract relationship indicator hides the actual mathematical relationships, but serves as a graphical description of the workings of the model without delving into specifics. Nonetheless, it is the mathematical description,

**TABLE 1 Critical infrastructures represented in CIPDSS**

| **Critical infrastructures** |
|---|
| 1. Agriculture and food |
| 2. Banking and finance |
| 3. Chemical industry and hazardous materials |
| 4. Defense industrial base |
| 5. Emergency services |
| 6. Energy |
| 7. Government |
| 8. Information and telecommunications |
| 9. Postal and shipping |
| 10. Public health |
| 11. Transportation |
| 12. Water |
| **Key asset categories** |
| 13. National monuments and icons |
| 14. Nuclear power plants |
| 15. Dams |
| 16. Government facilities |
| 17. Commercial key assets |

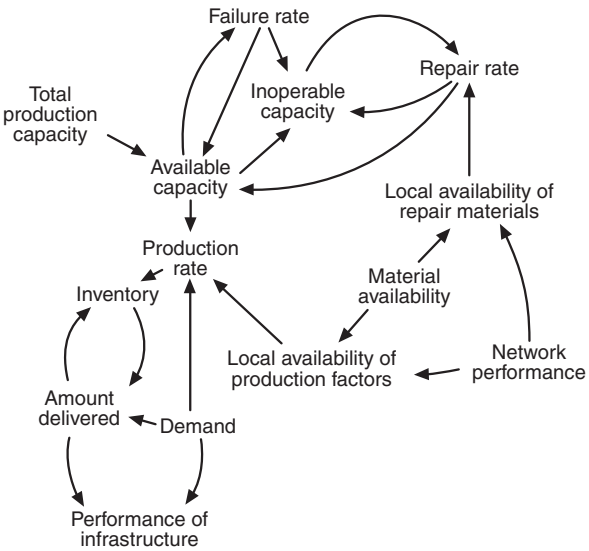



**FIGURE 1** Structure of a generic resource limited module.

for example, a system of coupled ordinary differential equations, embedded in the syntax of the Vensim model that defines the actual model.

A key aspect of the CIPDSS infrastructure models is the capturing of the primary interdependencies between infrastructures. In Figure 1, the dependencies are generically represented in the local availability of resources and materials and implicitly in the production operations. These functional dependencies are clearly called out in the infrastructure models. For example, the operation of telecommunication facilities depends on the supply of electrical power. Short durations of electrical power outages can be tolerated by the use of backup power generators. However, extended electrical power outages cause failure of selected equipment, which affects total communication capacity. The reduction in capacity may be compensated by other equipment with excess capacity (system resilience) or it may affect total throughput of calls. Because CIPDSS has a high level of representation of operations, not all dependencies are modeled, just the primary dependencies. Also, to maintain a consistent model resolution level, the effect of the dependency is modeled rather than the detailed interactions.

Each critical infrastructure sector is divided into a number of subsectors, which have a more uniform character and for which one or more separate Vensim subsector models are developed. For example, the emergency services sector is divided into (i) fire services, (ii) emergency medical services, (iii) law enforcement, and (iv) emergency support services. A Java-based program, the Conductor [2], is used to merge multiple system dynamics models, link variables that cross source code boundaries, and assemble a unified multisector model from individual sector model files. The Conductor identifies variables present in models with references to other source code files and resolves the references when the models are combined. As such, the program allows the models to be developed and tested at a modular level, but it enables simulation runs at the multisector level. The ability to develop modularly has allowed multiple developers from three geographically separated sites to codevelop the models.

### 3.1 Other Supporting Models to Represent Disruption Effects

Models of the infrastructure sectors and subsectors are in themselves insufficient to represent the full suite of effects and artifacts of a disruption. Since the output metrics of interest are human health and safety, a population model is used to account for those people injured by the disruption event compared with the natural processes of illness, injury, and death. Straightforward accounting of population groups in terms of birth/death processes and recovery from health impairment provide a basis for consequence modeling. To model the effect of scenario consequences on subcategories of the population, particularly workers in the critical infrastructures, the model uses occupation data from the US Bureau of labor statistics to estimate the initial size of the group. Because the scenario time frame that is modeled is usually on the order of a year or less, these models do not cover all of the dynamics that could arise in a disruption, for example, product substitution, restructuring of industry or practices, or evolutionary transformations that take years to manifest.

Economic modeling [3] assesses initial sector impacts from the incident in the individual sectors with interdependencies modeled to produce possible secondary effects. Most sectors compute revenue losses and other losses from clean-up, repairs, rebuilding, and so on. Other sectors, such as the energy subsectors, contain further information to give baseline revenue values with or without an incident. All of the metrics are passed into the economic sector model for further computation. Estimation of impacts to the rest of the economy is based on the North American Industry Classification System (NAICS) supersectors. Value-added, a measure of productivity in an industry is more conservative than lost sales or revenues since lost sales are often only temporary and can be recovered within a short period of time after an incident. Lost value-added tends to be permanent over short periods of time and is, therefore, a more accurate measure of the economic losses from temporary disruptions.

### 3.2 Scenario Models

While the infrastructure models exist as a body of interacting systems, the modeling of a disruption to one or more infrastructures often requires that specific code is developed to initiate a disruption event and stimulate the infrastructure models to render specific effects required by the disruption scenario. The models that accomplish these effects are called *scenario models*. Scenario models for biological threats, chemical threats, and telecommunications disruptions have been developed and form a robust basis for other threat scenarios listed in Table 2. For a given study, if an appropriate scenario model does not exist, it must be developed or adapted from a previously developed scenario model.

### 3.3 Consequence Models

Consequence models simulate the dynamics of individual infrastructures and couple separate infrastructures with each other according to their interdependencies. For example, repairing damage to the electric power grid in a city requires transportation to repair sites and delivery of parts, fuel for repair vehicles, telecommunications for problem diagnosis and coordination of repairs, and availability of labor. The repair itself involves diagnosis, ordering parts, dispatching crews, and performing repairs. The electric power grid responds to the initial damage and to the completion of repairs with changes in its operating capacity (the number of megawatts that can be distributed to customers). Dynamic processes like these are represented in the CIPDSS infrastructure

**TABLE 2 Threat scenario categories to be addressed by CIPDSS**

| |
|---|
| Biological |
| Chemical |
| Physical disruption |
| Radiological/nuclear |
| Insider |
| Cyber |
| Natural disaster |

sector simulations by differential equations, discrete events, and codified rules of operation, as appropriate for the sector being modeled.

### 3.4 Decision Support

The CIPDSS team has conducted an ongoing series of formal and informal interviews of critical infrastructure protection decision makers and stakeholders to identify requirements for the decision support system, scope out the decision environment, and quantify the prioritization of consequences. The taxonomy of decision metrics derived from this research involves six categories: (i) sector specific, (ii) human health and safety—public and occupational fatalities, nonfatal injuries, and illnesses, (iii) economic—immediate and interdependent costs of event, including the implementation and operating cost for optional measures, (iv) environmental—air and water emissions, nonproductive land, and intrinsic value loss, (v) sociopolitical—perceived risk, public confidence, trust in government sector-specific effects, and market confidence, and (vi) national security—continuity of military and critical civilian government services. The preferences of three representative decision makers were encoded using structured interview techniques to arrive at multiattribute utility functions consonant with the output of the consequence models and applicable to the case studies described below.

The primary building block for decision analysis in CIPDSS is a *case*. A case consists of two or more scenario pairs (base scenario pairs and alternative scenario pairs); each scenario pair is composed of a *readiness scenario* and an *incident scenario*:

- Base scenario pair
  - *Base readiness scenario.* Business-as-usual conditions; consequences in the absence of terrorist events or other disruptions.
  - *Base incident scenario.* Postulated event occurs with no additional optional measures implemented, beyond what exists at the time.
- One or more alternative scenario pair(s)
  - *Alternative readiness scenario.* A specific set of additional optional measures are in place; postulated event is not initiated.
  - *Alternative incident scenario.* Optional measures are in place; postulated event occurs.

Each scenario requires a separate simulation over a period of time (defined by the case) with the detailed national and metropolitan models. By comparing the alternative scenario pairs with the base scenario pairs, decision makers can evaluate the effects that various investments and strategies could have, if implemented. (The various investments and

strategies, labeled here as optional measures include hardware, processes, and strategies related to prevention, protection, mitigation, response, and recovery.)

### 3.5 Uncertainty and Sensitivity Analysis

Aggregate models such as those in the CIPDSS model set embody a degree of uncertainty in their formulation. Both uncertainty and sensitivity analyses [4] are essential tools in assessing the uncertainties arising when applying computer models to meaningful analyses. Rather than considering single predictions from the input space, prudent analysis considers the range of possible inputs and maps those to a range of outcomes. Uncertainty analysis defines methods to estimate the distribution of the model outputs, given uncertainties in the model inputs. Sensitivity analysis specifies a process by which sources of variance in the model outputs can be identified with uncertainties in the model inputs. Such information is useful when it is desirable to reduce the uncertainty of the outputs, as the information indicates which input variables are the greatest contributors to output variance. Both uncertainty analysis and sensitivity analysis are supported by the CIPDSS architecture and routinely applied when performing analyses. Although arbitrary experiment designs are supported, orthogonal array (OA), Latin hypercube sampling (LHS), and hybrid OA-based LHS designs are commonly used to support uncertainty and sensitivity analysis.

## 4 CASE STUDIES

Throughout its development cycle, CIPDSS has been exercised by producing a case study for each disruption capability. Each case study is used to expose each capability's potential cascading consequences and place a disruption scenario in a risk-informed context.

In general, CIPDSS can address case studies to support decision making relative to a standardized set of scenarios defined by DHS (Table 2), although not all capabilities are currently well developed. Current work is focused on the physical disruption capability, where the disruption may be caused by explosive devices, assault teams, natural events, or accidents. The program's goal is to cover all types of disruptions of interest to DHS policy makers.

In this section, three case studies are briefly described: a telecommunications disruption, an outbreak of a contagious disease, and an accidental release of a toxic industrial chemical.

### 4.1 Telecommunications Disruption Case Study

The earliest version of CIPDSS was exercised in a proof-of-concept case study that demonstrated the project's feasibility. The case study—chosen to broadly perturb many infrastructure sectors—involved a telecommunications disruption that degraded the operation of other infrastructure sectors. In each of three northeastern cities, major telecommunication switching stations were bombed with explosives in a simultaneous attack. Significant switching capacity was lost at each site and a large number of casualties were inflicted. CIPDSS consulted with the National Communications System and Lucent Technologies to assure appropriate modeling of the disruption in telecommunication services. Decision metrics and utility values were computed for several investment alternatives that would mitigate the impact of the incidents.

For the telecommunications case study, two optional measures were examined: (i) improving the restoration capability of the system and (ii) consolidating the targeted facilities away from dense urban areas. The former alternative was expected to reduce the secondary economic impact of the incident, while the latter was expected to reduce the impact on human health and safety. While undergoing repairs, the telecommunications system loses revenue as well as requiring capital to replace lost capability. The impact on human health and safety was caused by casualties imposed by the bomb blast. Casualties were relatively high because one switching facility was near a metro mass transportation station and the blast occurred at a time of day when commuter traffic was heavy. The alternative to consolidate the switching facilities and move them to a less busy part of the metro region was expected to cost $7 billion. This posed an interesting trade-off between the mitigation alternatives. In improving the restoration capability, presumed to cost $1.5 billion, the economic losses from the incident would be lower. On the other hand, consolidation of facilities would reduce fatalities and injuries. In accounting for such trade-offs, the decision modeling method combines the primary metrics of the consequences of a scenario with the implementation costs associated with the scenario. Another way to represent the decision, depicted in Figure 2, is as a decision tree, which consists of decision nodes and chance nodes. The utility of the base readiness scenario is 99.2 for a given decision profile. This is the expected utility for the chance node for each decision alternative. The expected utility of the base incident scenario is 16.3. For an attack having the probability of 0.1, the expected utility of the base alternative is, therefore, 90.9. The utilities of all alternatives are calculated and shown in Figure 2.

Figure 3 depicts a *decision map* that provides a convenient mechanism for the decision maker to assess investment alternatives as a function of the expected annual likelihood of the threat event. Figure 3 illustrates how a risk-neutral decision maker would prefer no action so long as the annual likelihood of the event is less than one incident in 13 years. When the likelihood is between one in 13 years and one in 5 years, that decision maker would prefer to improve the restoration capability; when the likelihood is greater than one in 5 years, that decision maker would prefer to consolidate facilities. The relative

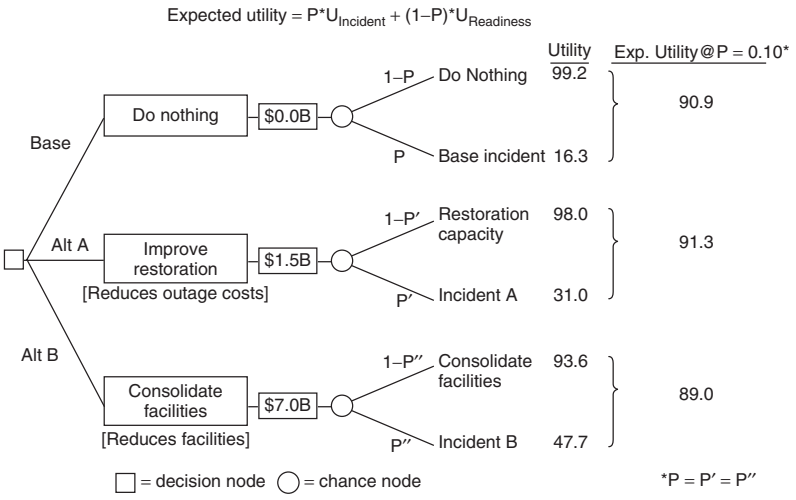



**FIGURE 2** Tree representation of decision alternatives.

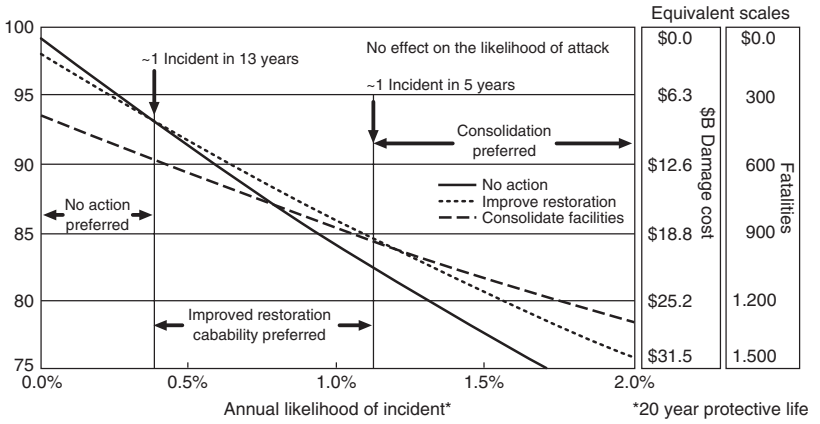



**FIGURE 3** Decision map of a scenario parameterized by the likelihood of the incident.

preferences are determined by the form of the decision maker's multiattribute utility function and risk tolerance profile.

### 4.2 Biological Pandemic Case Study

An analysis of a biological threat scenario was performed to assess infrastructure interdependency and economic effects resulting from the consequences of a highly infectious biological attack. To identify the conditions under which various alternatives are preferred, the consequences of the attack were combined with cost estimates for various protective measures within the decision model.

At the core of this case study is an infectious disease scenario model. The infectious disease model is a modified susceptible-exposed-infected-recovered (SEIR) model [5], based on an extended set of disease stages, demographic groupings, an integrated vaccination submodel, and representation of quarantine, isolation, demographic, and disease-stage-dependent human behavior. As a variant on the SEIR model paradigm, the CIPDSS model represents populations as homogeneous and well mixed with exponentially distributed residence times in each stage [6]. The use of additional stages and demographic groupings is designed to add additional heterogeneity, where it can be useful in capturing key differences in disease spread and response in different subpopulations.

The disease stages are generically represented so that the model can be used for a large number of infectious agents simply by adjusting the input parameters appropriately. For example, with the studied hypothetical biological agent like smallpox, the first stage is the exposed or incubating stage during which a vaccine can still be effective (about 3 days) and the next stage represents the remainder of the incubating period when the vaccine is no longer effective. This is followed by a prodromal phase when the disease is sometimes infectious and is symptomatic, but with nonspecific flu-like symptoms. The disease progresses into a rash stage, where the risk of contagion is highest, and then into the scab phase. The patient then either recovers from the disease, or dies.

The analysis specifically considered the following incident and alternatives:

- *Base incident.* 1000 people initially infected with smallpox and implementation of existing vaccination policies.

- *Alternative A.* Installation of biodetectors to provide early detection of the disease.
- *Alternative B.* Use of antiviral drugs to treat the disease.
- *Alternative C.* Mass quarantine to reduce the spread of the disease.
- *Alternative D.* Improved training of health care personnel to administer existing vaccines more rapidly.

Large-scale simulations were used to characterize the uncertainty in the consequence results and understand which model parameters had the strongest effects on the decision metrics. Considering uncertainities, the number of fatalities in the base incident scenario ranged from 277 to 7041. Incorporation of individual alternatives A–D reduced the lower end of the fatality range slightly and in all cases significantly reduced the maximum number of simulated fatalities. Primary economic costs in the metropolitan area, where 1000 persons are initially infected, were calculated to range from $7.5 to $9.5 billion, except for the mass quarantine alternative (Alternative C) where the primary economic costs would be up to three times greater because of loss of worker productivity during a quarantine. On a national scale, economic costs might easily be driven by a widespread self-isolation response resulting from the general population seeking to protect itself by reducing exposure to potentially infected individuals. A severe self-isolation response could significantly impact business and industrial productivity as workers stay home from their jobs and reduce normal spending by avoiding shopping and other commercial areas where they might come in contact with infected persons. The interdependent private sector economic costs and personal income losses associated with a severe, widespread self-isolation response were calculated to be as great as $450 billion, or 15–45 times the primary economic costs of the infectious disease event. Government costs could be similar.

Within the initially affected metropolitan area, the primary indirect or "cascading" effects of the incident involve the transportation and telecommunications sectors, with other sectors being affected by these in turn. Quarantine measures impact nearly half of the workers in the metropolitan area during the peak period of the crisis, resulting in much lower usage of the transportation system and losses in personal income because workers would not report to work and businesses would close temporarily.

In accordance with the numerous infectious disease model results that are currently available [7, 8], the CIPDSS results show that given the initiating event, a significant epidemic will ensue, with an average of 6100 nonfatal illnesses and 1500 fatalities in the base case. CIPDSS results particularly agree with Gani and Leach [9] who point out the importance of delays in detecting the first cases and the importance of setting up effective public health interventions. In the CIPDSS analysis, the addition of biodetectors provides a high degree of early warning, enabling a rapid effective response that almost completely stops the spread of the disease outside the initially infected metropolitan area, thereby significantly reducing the number of cases and subsequent mortalities. The study indicates that time to intervention and effective response is a critical component in controlling the health impacts resulting from a deadly infectious biological outbreak.

The national economic consequences are primarily caused by a behavioral response that could lead to widespread self-isolation and severe economic impacts. Because the magnitude of such a response is largely unstudied in the literature, the uncertainty surrounding this parameter is very great. Rather than assuming that more is known than is actually the case about the possible public self-isolation response to an intentional release of infectious smallpox virus, the analysis presents the decision model results parameterized with respect to the relative level of widespread self-isolation behavior.

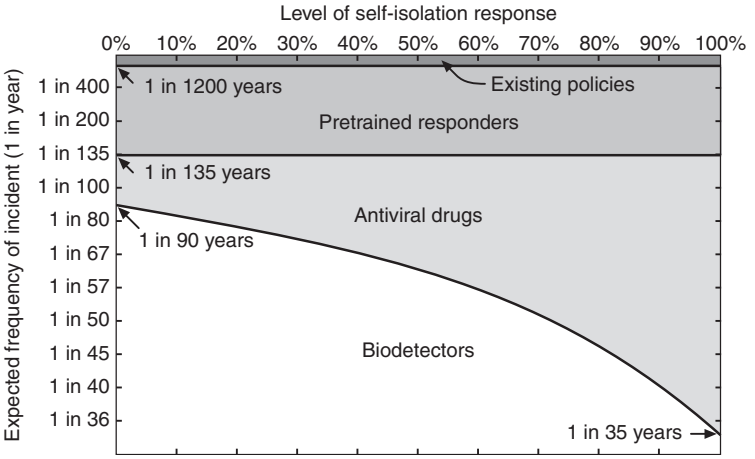



**FIGURE 4** A preference map for preferred alternatives in a biological disease case.

For a risk-neutral profile, a preference map was derived by combining the calculated consequences in a decision model based on multiattribute decision theory and by assigning the attribute trade-off values that are consistent with values suggested by several DHS decision makers (Figure 4). The preference map indicates that up to an expected likelihood of one incident in 1200 years, the preferred alternative would be to continue existing vaccination and quarantine policies, regardless of the level of national self-isolation response.

Likewise, between an incident likelihood of one in 1200 years and one in 135 years the preferred alternative would be to pretrain and implement a larger number of medical and emergency responders to vaccinate the public more rapidly, in the event of an intentional smallpox release. Without a widespread self-isolation response (0%), the antiviral drug alternative would be preferred when the incident likelihood increases to one in 90 years.

At greater incident likelihoods, the detector alternative is preferred because it produces the lowest level of combined consequences across all simulations of the scenarios. When the level of self-isolation response increases, the antiviral strategy is the preferred alternative at increasing incident likelihoods, being preferred over detectors at the maximum level of self-isolation and incident likelihood of one in 35 years. This trend in increasing self-isolation takes place because the biodetectors would result in earlier disease detection and thus public notification, which in turn would result in an earlier commencement of the economic impacts caused by the widespread self-isolation response.

### 4.3 Toxic Industrial Chemical Case Study

The chemical threat scenario analysis was performed to demonstrate the CIPDSS capability to provide risk-informed assessments of potential mitigation measures for this class of threats [10]. Coupled threat scenario, infrastructure interdependency, and economic effects models were used to estimate the consequences of an accidental release of a toxic industrial chemical, namely chlorine, in an urban setting. The consequences were combined with cost estimates for various protective measures within the decision model to identify the conditions under which various alternatives would be preferred. The analysis specifically considered the following incident and alternatives:

- *Base incident.* A large (70 percentile event) in a "normally prepared" community and a "normally trained" set of emergency responders.
- *Alternative A.* Installation of chemical detectors to detect the extent of spread of the chemical.
- *Alternative B.* Use of temporary or mobile triage/treatment sites to handle expected volumes of exposed persons.
- *Alternative C.* Application of comprehensive community preparedness training for chemical releases.
- *Alternative D.* Increased training and response preparedness for emergency responders and health providers.
- *Alternative E.* Application of comprehensive community preparedness training for chemical releases with an emphasis on significantly reducing the population response time.

The initiating event for the base incident and alternative mitigation measure scenarios is a statistical representation (model) of the *unmitigated* consequences of a large-scale chlorine release. The potential number of injuries and fatalities and the number of hospital beds and geographical areas rendered unusable during and some time after the passage of a toxic plume are estimated on a probabilistic basis. To accomplish this, historical accidental release data, maximum stored volumes, and meteorological data were used as inputs into a heavy gas dispersion model. Multiple runs were performed using plausible distributions on the dispersion model inputs to generate a generic statistical distribution of injuries and fatalities associated with specific toxic chemicals for four different regions of the United States, using actual geographic locations and population distributions as a basis for the calculations. The stochastic distributions of unmitigated injuries and fatalities were developed as a function of time, parameterized as a function of cumulative probability of the event, and normalized to a population base of 1 million persons in a 5-km radius from the release site to mask the identification of the actual site.

The analysis of health effects employed Acute Exposure Guideline Levels (AEGLs) developed by Environmental Protection Agency (EPA) and National Research Council (NRC) [11], for which six different averaging times ranging from 5 min to 8 h are given. Three AEGLs were used in the analysis as follows:

- Persons within AEGL-1 footprint could experience *adverse* effects such as notable discomfort, irritation, or certain asymptomatic nonsensory effects. The effects are transient and reversible upon cessation of exposure.
- Persons within AEGL-2 footprint could experience *irreversible* or other injuries, long-lasting adverse health effects, or an impaired ability to escape.
- Persons within AEGL-3 footprint could experience *life-threatening* health effects or death.

Furthermore, three additional health criteria that further disaggregate AEGL-3 were exercised to provide better definition of victim status or condition to the CIPDSS public health sector model. These additional criteria enabled a more complete modeling of healthcare response to the event.

In this analysis, an unmitigated base case is compared to each of five modeled mitigation measures with respect to key operational parameters in the CIPDSS models relative to the value of the same variable in the base incident scenario.

On the basis of the uncertainty analysis performed with the CIPDSS models, the minimum, mean, and maximum values for the mitigation measure costs, fatalities, injuries, economic losses, and losses in public confidence (decision metrics) for each of the above incident scenarios display virtually no variation in the results among the five alternative mitigation measure scenarios. Furthermore, there is almost no variation in the results between the alternative mitigation measure scenarios and the base incident scenario, which includes no additional mitigation measures. The reason for this is the rapidity with which the plume disperses; there is simply insufficient time to react. Even with accelerated response times, the majority of the population that would be exposed without additional mitigation measures would still receive exposure even with the additional mitigation measures.

Because all of the measures that were modeled had an insignificant effect on mitigating the consequences of a large-scale chlorine release, the various options differentiated on the basis of implementation cost alone. Thus, as calculated in the CIPDSS decision model, the order in which the measures would be preferred is in direct relationship to their implementation cost. The analysis indicated that investing in any of the mitigation options considered is less desirable than taking no action, regardless of how likely it may be that the incident would occur. Of course, this conclusion is obvious from the fact that none of the modeled measures had any significant mitigation effect on the consequences of an accidental release. The rank ordering of preference for the alternatives, shown in Figure 5, was (i) base case, no mitigation; (ii) alternative A, chemical detectors; (iii) alternative D, response preparedness and training; (iv) alternative E, community preparedness II; (v) alternative C, community preparedness I; and (vi) alternative B, mobile treatment facilities. These results are consistent with other studies of chlorine releases [12]. One conclusion to draw is that investment should focus on prevention of a chemical release rather than on improving mitigation efforts after a release.

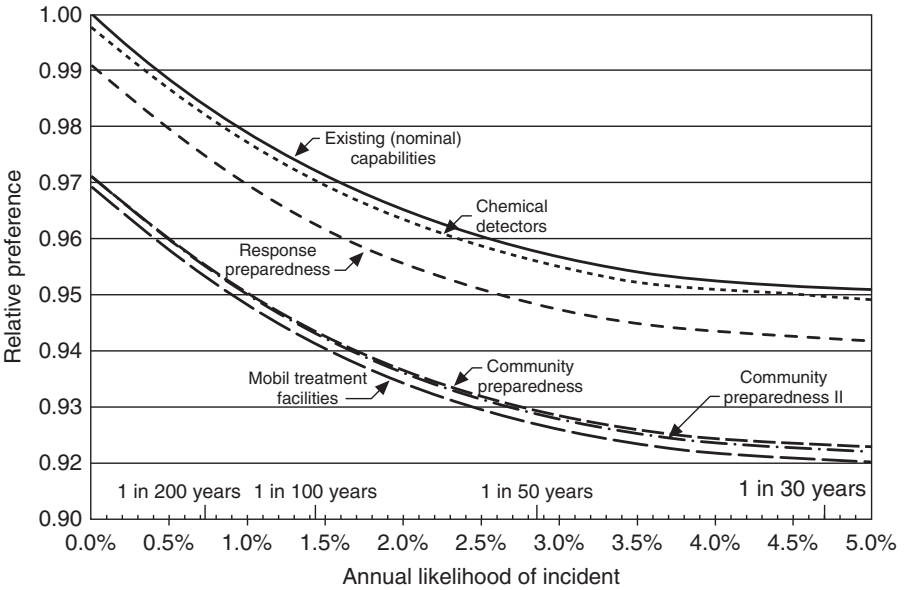



**FIGURE 5** The preference map for a chemical release scenario.

These results do suggest, however, that in the effort to protect the public from large accidental releases of chlorine, consideration should be given to measures designed to prevent the release rather than measures designed to mitigate the consequences of a release once it has occurred.

## 5 CONCLUSION

CIPDSS has demonstrated its capability to provide meaningful risk-informed decision support for several categories of threats of interest to the DHS. As a system dynamics suite of simulations, it has confirmed the ability of system dynamics to support a wide range of analyses of interest to policy makers through aggregate level simulation of multiple infrastructure systems.

Combined with the flexibility and extensibility conferred by the conductor, the uncertainty and sensitivity analysis capability, the decision model, and the breadth of coverage, including all 12 critical infrastructures and 5 key resource categories, CIPDSS is a unique capability for investigating consequences of infrastructure disruption. CIPDSS incorporates a fully integrated risk assessment process, explicitly and rigorously accounting for uncertainties in threats, vulnerabilities, and the consequences of terrorist acts and natural disasters. CIPDSS goes beyond the sole calculation of first-order consequences in one or just a few infrastructures. CIPDSS models the primary interdependencies that link the 17 critical infrastructures and key resources together and calculates the impacts that cascade into these interdependent infrastructures and into the national economy.

## REFERENCES

1. Moteff, J., and Parfomak, P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification*. Congressional Research Service, Report RL32631, Library of Congress, Washington, DC.
2. Thompson, D., Bush, B., and Powell, D. (2005). *Software Practices Applied to System Dynamics: Support for Large-Scale Group Development*. Los Alamos National Laboratory Report, LA-UR-05-1922, Los Alamos, NM.
3. Dauelsberg, L., and Outkin, A. (2005). *Modeling Economic Impacts to Critical Infrastructures in A System Dynamics Framework*. Los Alamos National Laboratory Report, LA-UR-05-4088, Los Alamos, NM.
4. Helton, J. C., and Davis, F. J. (2000). *Sampling-Based Methods for Uncertainty and Sensitivity Analysis*. Sandia National Laboratories, SAND99-2240, Albuquerque, NM.
5. Murray, J. D. (1989). *Mathematical Biology* vol **19**. Springer-Verlag, Berlin.
6. Hethcote, H. W. (2000). The mathematics of infectious diseases. *SIAM Rev*. **42**(4), 599–653.
7. Fraser, C., Riley, S., Anderson, R., and Ferguson, N. (2004). Factors that make an infectious disease outbreak controllable. *Proc. Natl. Acad. Sci. U.S.A.* **101**(16), 6146–6151.
8. Halloran, M. E., Longini, I. M., Jr. Nizam, A., and Yang, Y. (2002). Containing bioterrorist smallpox. *Science* **298**, 1428–1432.
9. Gani, R., and Leach, S. (2001). Transmission potential of smallpox in contemporary populations. *Science* **414**, 748–751.
10. Shea, D., and Gottron, F. (2004). *Small-Scale Terrorist Attacks using Chemical and Biological Agents: An Assessment Framework and Preliminary Comparisons*, Congressional Research Service, RL32391, Library of Congress, Washington, DC.

11. National Research Council (NRC). (1993). *Guidelines for Developing Community Emergency Exposure Levels for Hazardous Substances*. National Academy Press, Washington, DC.
12. Streit, G., Thayer, G., O'Brien, D., Witkowski, M., McCown, A., and Pasqualini, D. (2005). *Toxic Industrial Chemical Release as a Terrorist Weapon: Attack on a Chemical Facility in an Urban Area*. Los Alamos National Laboratory, LA-CP-0575 Los Alamos, NM.

## FURTHER READING LIST

United States of America. (1998). *Executive Office of the President*, Critical Infrastructure Protection, Presidential Decision Directive (PDD) 63.

United States of America. (2003). *Executive Office of the President*, The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.

United States of America. (2003). *Executive Office of the President. Homeland Security Presidential Directive–7*. Critical Infrastructure Identification, Prioritization, and Protection.

# THE USE OF THREAT, VULNERABILITY, AND CONSEQUENCE (TVC) ANALYSIS FOR DECISION MAKING ON THE DEPLOYMENT OF LIMITED SECURITY RESOURCES

NICHOLAS A. LINACRE

*Faculty of Land and Food Resources, the University of Melbourne, Parkville, Victoria, Australia*

MARC J. COHEN

*International Food Policy Research Institute, Washington, D.C.*

BONWOO KOO

*Department of Management Sciences, Faculty of Engineering, University of Waterloo, Ontario, Canada*

REGINA BIRNER

*International Food Policy Research Institute, Washington, D.C.*

## 1 OVERVIEW

The United Nations defines terrorism as "any action that is intended to cause death or serious bodily harm to civilians or noncombatants, when the purpose of such act,

by its nature or context, is to intimidate a population, or compel a Government or an international organization to do or abstain from doing any act" [1].

On the basis of rational-choice considerations (compare [2]), an organization will choose terrorist actions in addition to other actions, if terrorism contributes to reaching their goals at a relatively low cost and has high impact. Hence, it would be rational for terrorists to attack a target, if this allows them to realize their goals to a larger extent with costs lower than that would be incurred by other means. However, it may be argued that our rational-choice model has limitations in explaining suicide attacks, although these may follow logically from the ideological or religious beliefs of those who carry them out.

The rational-choice considerations are important because terrorists will consider perceived vulnerability and consequences in deciding on whether to launch an attack. Therefore, the allocation of security resources to counterterrorism is a complex task that requires decisions on the risk allocation mechanism, estimation of risk, and tolerable levels of risk. Until recently, few papers have been published on ways to allocate security resources. Innovations have applied game theory [3], portfolio theory and risk analysis approaches [4–6] to the allocation of security resources (For an extensive literature review see the special edition of *Risk Analysis* **27**(3)).

In this article, the risk analysis approach taken by Willis et al. [4–6] is discussed. This approach, known as *threat–vulnerability–consequence* (*TVC*) *analysis*, is related to catastrophe modeling (see [7]). Both TVC analysis and catastrophe modeling are examples of a more general statistical theory known as the *theory of loss distributions*, which are widely applied by actuaries in the insurance and reinsurance industries. The theoretical development of loss distributions can be found in Cox et al. [8–10] Before outlining the essential elements of TVC analysis, it is useful to reflect on traditional definitions of risk as the approach taken by Willis et al. [4, 6] modifies the traditional definition of risk to reflect the underlying structure of the risks encountered in terrorism analysis.

Traditionally risk is defined as the triplet $\langle s_i, p_i, x_i \rangle$ where $s_i$ is the risk scenario, which has a probability $p_i$ of occurring and a consequence $x_i$ if it occurs [11, 12]. A useful risk metric is defined as the probability of an event occurring multiplied by its associated consequence, $p_i \times x_i$. It is common for the expected value of the distributions to be used as point estimates in the calculation of $p_i \times x_i$ [13]. However, the measure for risk is uncertain and should be represented by a probability distribution, not a point estimate [14]. The traditional definition of risk is modified by [4, 6] and is defined as a function of TVC. This definition is similar to others proposed in risk literature, for example see [15–17].

The remainder of this article provides an overview of the TVC analysis framework, discusses TVC analysis and the deployment of resources, elaborates some of the challenges and limitations of TVC analysis, discusses methods of dealing with uncertainty, provides a summary of the current state of practice, and suggests linkages between areas of research currently addressing similar issues.

## 2 THREAT–VULNERABILITY–CONSEQUENCES (TVC) ANALYSIS FRAMEWORK

Risk is measured as the probability of a terrorist "event" and the associated consequence. The probability of a terrorist event is measured as the threat and vulnerability of the target.

Threat is measured as the probability of a specific target being attacked in a specific way during a specified period. Vulnerability is measured as the probability of a damage that can occur, given a threat. Consequences are the magnitude and type of damage resulting, given a successful terrorist attack.

### 2.1 Assessing Threats

The purpose of the threat assessment is to gain an understanding of where terrorists are targeting their activities; typically this is based on intelligence information gathered from a variety of sources, both human and technological. Threats may be general or specific, and security responses are conditioned on the nature of the information received [6]. Typically, an analysis will first assess whether a country or region is under a general threat from terrorist attacks. Subsequently, a view is formed of the probability or likelihood that a specific target will be attacked in a specific way during a specified time period; mathematically,

$$\text{Threat} = p(\text{attack occurs})$$

However, it is essential to consider both the economic and the political dimension of costs and benefits in assessing the level of threat. For example, if a terrorist group has an antipoverty ideology, using a technique that hits mostly poor people implies a political cost, because it reduces the credibility of their cause. Thus, in the mid 1980s, the Liberation Tigers of Tamil Eelam in Sri Lanka threatened to use disease pathogens to destroy the economically important tea crop and to deliberately infect rubber trees with the leaf curl fungus [18]. One reason that the Tigers never made good on this threat may be that most of the low-income estate workers, who depend on tea and rubber cultivation for their livelihoods, are ethnic Tamils.

### 2.2 Assessing Vulnerabilities

Different definitions of vulnerability appear in the literature. Haimes [16] defines vulnerability as the probability that damages (where damages may involve fatalities, injuries, property damage, or other consequences) occur, given a specific attack type, at a specific time, on a given target, or vulnerability is the manifestation of the inherent states of the system (e.g. physical, technical, organizational, and cultural) that can result in damage if attacked by an adversary. Pate-Cornell [19] defines vulnerability as the capacity of a system to respond to terrorist threats. Adopting the approach taken by Willis et al. [4, 6], vulnerability is mathematically represented as the probability that an attack results in damage:

$$\text{Vulnerability} = p(\text{attack results in damage}|\text{attack occurs})$$

Vulnerability is an estimate of the likelihood of a successful attack resulting in damage. Vulnerability depends on the organization of the infrastructure, on the controls that are in place at the borders, and on the monitoring systems.

### 2.3 Assessing Consequences

A consequence is an assessment of the impact or loss from a terrorist event. Willis [6] defines "consequence" as the expected magnitude of damage (e.g. deaths, injuries, or property damage), given a specific attack type, at a specific time that results in damage to a specific target. Mathematically,

$$\text{Consequence} = E(\text{damage}|\text{attack results in damage})$$

One can also distinguish between the short- and long-term consequences, which may have both an economic dimension (loss of productive capacity and food availability) and a political dimension resulting in persistent periodic cycles of conflict. International efforts to promote increased security are inherently difficult, because conflicts typically occur in countries where national governments have limited legitimacy and where far-reaching governance problems persist [5].

### 2.4 Risk Estimation

Terrorism risk may be thought of as function of the threat level, vulnerability to the threat, and consequence from the terrorist action. For example, the risk estimate could refer to an attack by terrorists against food trade using a particular disease or toxin. The threat would then be an estimate of the terrorists' priority for such attack against the available alternatives. Vulnerability could be estimated as likelihood of port interception and the consequences would be an assessment of the impact of the disease. TVC analysis is an interactive approach designed to elicit areas where high threat levels, extreme vulnerabilities, and high consequences overlap (Fig. 1). It is the intersection of these events that cause security concerns. Mathematical risk is estimated as

$$\begin{aligned}\text{Risk} = \; & p(\text{attack occurs}) \times p(\text{attack results in damage}|\text{attack occurs}) \\ & \times E(\text{damage}|\text{attack results in damage})\end{aligned}$$

## 3 TVC ANALYSIS AND THE DEPLOYMENT OF RESOURCES

TVC analysis should be viewed as part of an integrated terrorism risk management and response system that continually review prioritization decisions based on new knowledge. Components of the system include risk analysis including target selection and resource prioritization, risk mitigation including prevention of attacks and protection of assets, responses to attack, and mechanisms for recovery. Risk analysis provides identification and understanding of threats, assessment of vulnerabilities, and determination of potential impacts. Prevention provides detection and intervention measures, which are used to mitigate threats. Protection provides physical safeguards for critical infrastructure, property, and other economic assets. Response and recovery provide for the short- and medium-term private and public sector measures used to recover from a terrorist attack. TVC is an important component of this cycle, but it is not an end in itself.

TVC analysis attempts to provide a loss distribution for use in decision making. In this application, the distribution is a function of the threat to a target, the target's vulnerability to the threat, and the consequences should the target be successfully attacked. Risk metrics

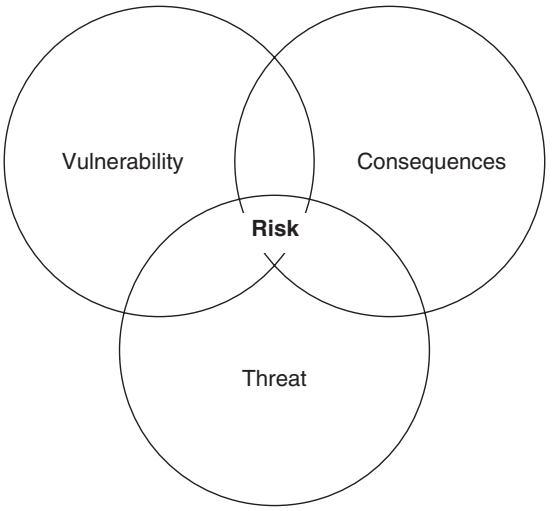



**FIGURE 1** Overlapping regions of high threat, vulnerability, and consequence of great security risk.

can be applied to the different loss distributions derived for different risks to facilitate risk-based prioritization of resources. Metrics may include expected value, variance, skew or skewness (a measure of the asymmetry of the probability distribution of a real-valued random variable), and kurtosis (observations are spread in a wider fashion than the normal distribution, fewer observations cluster near the average, and more observations populate the extremes), all of which can be used to compare different targets, thus facilitating the risk-based prioritization of resources. Alternative metrics used in applied finance include value at risk (VaR); for example, see [20].

## 4 LIMITATIONS OF TVC ANALYSIS

Willis [6] outlines two limitations for consideration when applying TVC analysis. Firstly, Willis [6] draws a distinction between risk assessment and resource allocation, and argues that an efficient allocation of homeland security resources should distribute resources where they can most reduce risks, not where risks are greatest. Secondly, Willis Willis [6] raises the difficult and contentious issue of establishing tolerable levels of risk, which is an important risk management decision. Both these issues are intertwined, as choices will depend on society's willingness to accept some types of risk and mitigate others.

The extent to which society self-insures risk and chooses to invest in risk mitigation is a complex issue. Willis [6] argues that risks may be tolerated simply because they are small compared to benefits obtained through the risky activity, and that risks may be tolerated because the available countermeasures could lead to equal or greater risks themselves. The extent to which rational choices will be made will depend on society's risk perceptions and on our ability to consider options. Simon [21] argues that individuals have a limited range of alternatives, that is we do not know all the decision options available to us, and, even if we do, our conceptual limitations and time prevent us from comparing all of the options available. Other evidence supports this view. For example,

Solvic et al. [22] argue that decision makers rarely have all options available to them. Given these constraints it may be difficult to rationally allocate resources according to the principle of greatest risk reduction.

## 5 APPLYING THE TVC ANALYSIS FRAMEWORK

In this section, we review various studies that attempt to address some aspect of the quantification of risk. Linacre et al. [5] provide evidence of the *ex-ante* consequences of agroterrorism in developing countries. Gordon et al. [23] provides an *ex-ante* economic consequence analysis of the impacts of a 7-day shutdown of the commercial aviation system in the United States. Rose et al. [24] use a computable general equilibrium analysis to quantify the economic effects of a terrorist attack on the electrical transmission system of Los Angeles. Simonoff et al. [25] provide a statistical analysis of electrical power failures, which can be used for risk scenario construction. Willis et al. [4, 6] provide guidance on developing risk-based allocation mechanisms for resource allocation and discuss some aspects of catastrophe modeling. Keeney [26] discusses how structuring of objectives can help in understanding the incentives of terrorists and defenders. Finally, Bier [3] provides a game-theoretic perspective on the issue where a defender must allocate defensive resources to a collection of locations and an attacker must choose which locations to attack.

## 6 DEALING WITH UNCERTAINTY

The methods above allow us to estimate risk, but we also need to put bounds on that risk. There are a number of ways of incorporating uncertainty about parameter values and assumptions in models. The following methods allow us to set bounds on our risk assessment results that represent the confidence we have in our answers.

Scenario (what-if) and sensitivity analyses are among the most straightforward ways to assess the effect of uncertainty, simply, by altering the parameter values and repeating the calculation [14]. Such an approach may become unwieldy when a large number of parameters are involved [14].

Worst-case analysis is the traditional approach to ecological risk assessment, which recognizes that uncertainty exists, but does not try to model it explicitly. Instead, the parameter values are set so that the overall risk estimate is conservative [14]. Many people argue that such approaches result in hyperconservative estimates of the risk and impose a high cost on society for little benefit.

Monte Carlo analysis uses probability theory and numerical analysis to combine uncertainty in a way that reveals how probable each of the possible outcomes is [14, 27–29]. Its usefulness depends on the availability of data to estimate parameters for statistical distributions. In many problems, the data will not be available to estimate the parameters or identify the distribution [30].

Interval Arithmetic provides another method to incorporate uncertainty. Most scientific disciplines quote best estimate values plus or minus an error term, expressing uncertainty in the best estimate. These measures can be expressed as intervals, which are a closed bounded subset of the real line $[a, b] = \{x : a \leq x \leq b\}$ [31]. Intervals have mathematical properties that allows us to propagate, or uncertainty about best estimate

**TABLE 1 Comparing TVC and Catastrophe Model Structure**

| TVC Analysis | Catastrophe Model |
|---|---|
| Assessing threats, for example, dirty bomb attack | Stochastic module randomly generates a catastrophic event |
| | Hazard module is used to determine the geographical effect of a catastrophic event brought about by variations in topography |
| Vulnerability analysis | Vulnerability module, which is used to calculate damage to buildings, contents, and business turnover, based on a number of factors including building type, design, and location |
| Consequence analysis | Financial module, which quantifies the financial loss to the insured |

numbers through a series of calculations [14]. Fuzzy Numbers are a generalization of intervals have mathematical properties that allow the propagation of uncertainty about best estimates numbers through a series of calculations [14].

## 7 FURTHER READING

As previously mentioned, there are a number of related developments in different subject areas that may have utility for researchers and decision makers involved in security resources prioritization. In the finance literature, the development of risk metrics such as VaR provide approaches for the comparison of different portfolios of risks (see [20]). Within the insurance and actuarial literature, loss distributions are relevant (e.g. [8–10]), extreme value theory [31], and catastrophe modeling. The structures of catastrophe models are similar to the structure of TVC analyses. Catastrophe models are composed of a number of modules and their relationship to TVC analysis is shown in Table 1 [7, 32, 33].

Catastrophe models may be used as a diagnostic tool to assess post event loss. The model may be designed to investigate ideas about the relationships between causal factors and, finally, the model may be designed to forecast the frequency and magnitude of events [32]. It is in this last use that TVC analysis and catastrophe models have a similar application.

The political risk literature also provides a theoretical and applied underpinning for quantitative valuations of risk associated with war and political instability. A useful starting point into this literature is [34]. Further background reading on risk provides important information on acceptable levels of risk (e.g. [35, 36]). Fischhoff et al. [37] provide a useful paper on expert and lay perceptions of risk. Kahneman and Tversky [38] provide a seminal paper on how people make risk decisions, and finally [14, 27] provide an important technical information on dealing with uncertainty.

## 8 CONCLUSIONS

TVC analysis offers a structured mechanism for addressing security resource allocations problems. However, it does not address the difficult and contentious issue of establishing

tolerable levels of risk, which is an important risk management decision. The extent to which rational decisions will be made over the choice of tolerable levels of risk will depend on societal perceptions of risk.

Rational-choice considerations also suggest that homeland security resources should be allocated to where they can most reduce risks, not necessarily where risks are greatest. The extent to which society is prepared to accept self-insurance of risks that cannot be readily mitigated is a complex issue and will also depend on societal perceptions.

Further limitations arise in TVC analysis because of uncertainty around the basic parameters used in the models. It may be that it is impossible, given the available data, to make confident decisions about the prioritization of security resources because of the level of uncertainty.

However, given all these limitations, TVC analysis remains an important methodological approach to assist decision makers, structure, explain, justify, and communicate decisions on security resource prioritizations.

## REFERENCES

1. UNEP (2004). *United Nations Environment Program, Global Environment Facility*. http://www.unep.ch/biosafety/index.htm.
2. Krueger, A. B., and Malečková, J. (2003). Education, poverty and terrorism—is there a causal connection? *J. Econ. Perspect.* **17**(4), 119–144.
3. Bier, V. M. (2007). Choosing what to protect. *Risk Anal*. **27**(3), 607–620.
4. Willis, H. H., Morral, A. R., Kelly, T. K., and Medby, J. (2005). *Estimating Terrorism Risk*. MG-388-RC. RAND Corporation, Santa Monica, CA.
5. Linacre, N. A., Koo, B., Rosegrant, M. W., Msangi, S., Falck-Zepeda, J., Gaskell, J., Komen, J., Cohen, M. J., and Birner, R. (2005). *Security Analysis for Agroterrorism: Applying the Threat, Vulnerability, Consequence Framework to Developing Countries*. Discussion Paper 138. International Food Policy Research Institute, Washington, DC.
6. Willis, H. (2007). Guiding resource allocations based on terrorism risk. *Risk Anal.* **27**(3), 597–606.
7. Grossi, P., and Kunreuther, H. (2005). *Catastrophe Modeling: A New Approach to Managing Risk*. Springer, New York.
8. Cox, D. R., and Hinkley, D. V. (1974). *Theoretical Statistics*. Chapman and Hall, London.
9. Hogg, R. V. (1984). *Loss Distributions*. Wiley, New York.
10. Klugman, S. A., Panjer, H. H., and Willmot, G. E. (1998). *Loss Models from Data to Decisions*. Wiley, New York.
11. Kaplan, S., and Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Anal.* **1**, 11–27.
12. Kaplan, S. (1997). The words of risk analysis. *Risk Anal*. **17**, 407–417.
13. Stewart, M. G., and Melchers, R. E. (1997). *Probabilistic Risk Assessment of Engineering Systems*. Chapman and Hall, Melbourne.
14. Ferson, S., Root, W., and Kuhn, R. (1998). *Risk Calc: Risk Assessment with Uncertain Numbers*. Applied Biomathematics, New York.
15. Ayyub, B. A. (2005). Risk analysis for critical infrastructure and key asset protection. *Presentation at Symposium on Terrorism Risk Analysis*. University of Southern California, January 13–14, 2005.

16. Haimes, Y. Y. (2004). *Risk Modeling, Assessment, and Management*, 2nd ed. John Wiley & Sons, Hoboken, NJ.
17. von Winterfeldt, D., and Rosoff, H. (2005). Using project risk analysis to counter terrorism. *Symposium of Terrorism Risk Analysis*. University of Southern California.
18. CNS (Center for Non-proliferation Studies). (2006). *Agroterrorism: Chronology of CBW Incidents Targeting Agriculture and Food Systems, 1915–2006.* Posted at http://cns.miis.edu/research/cbw/agchron.htm.
19. Pate-Cornell, M. E. (2005). Risks of terrorist attack. *Symposium of Terrorism Risk Analysis*. University of Southern California.
20. McNeil, A., Frey, R., and Embrechts, P. (2005). *Quantitative Risk Management: Concepts Techniques and Tools*. Princeton University Press, Princeton, NJ.
21. Simon, H. A. (1956). Rational choice and the structure of the environment. *Psychol Rev.* **63**(2), 129–138.
22. Slovic, P., Kunrether, H., and White, G. F. (1974). The perception of risk. In *Natural Hazards: Local, National, Global*, G. F. White, Ed. Oxford University Press, New York.
23. Gordon, P., Moore, J. E., Park, J. Y., and Richardson, H. W. (2007). The economic impacts of a terrorist attack on the U.S. commercial aviation system. *Risk Anal.* **27**(3), 505–512.
24. Rose, A., Oladosu, G., and Liao, S. (2007). Business interruption impacts of a terrorist attack on the electrical power system of Los Angeles: customer resilience to at total blackout. *Risk Anal.* **27**(3), 513–516.
25. Simonoff, J. S., Restrepo, C. E., and Zimmerman, R. (2007). Risk-management and risk-analysis-based decision tools for attacks on electric power. *Risk Anal.* **27**(3), 547–570.
26. Keeney, R. L. (2007). Modeling values for anti-terrorism analysis. *Risk Anal.* **27**(3), 585–596.
27. Morgan, A., and Granger, M. (1990). *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. Cambridge University Press, Cambridge.
28. Nelson, B. L. (1995). *Stochastic Modeling*. McGraw-Hill, New York.
29. Vose, D. (1996). *Quantitative Risk Analysis: A Guide to Monte Carlo Simulation Modelling*. John Wiley & Sons, Brisbane.
30. Ferson, S., Ginzburg, L., and Akcakaya, R. (2003). Whereof one cannot speak: when input distributions are unknown. *Risk Anal.* http://www.ramas.com/whereof.pdf.
31. Moore, R. E. (1979). *Methods and Applications of Interval Analysis*. SIAM, Philadelphia, PA.
32. Sanders, D. E. A. (2005). The modelling of extreme events. *Br. Actuar. J.* **11**(III), 519–572.
33. Kunreuther, H., and Michel-Kerjan, E. (2004). Challenges for terrorism risk insurance in the United States. *J. Econ. Perspect.* **18**(4), 201–214.
34. Howell, L. D., Ed. (2002). *Political Risk Assessment: Concepts, Methods, and Management*. The PRS Group Inc., East Syracuse, NY.
35. Slovic, P., Fischhoff, B., and Lichtenstein, S. (1975). Cognitive process and societal risk taking. In *11th Symposium on Cognition and Social Behavior*, J. S. Carroll, and J. W. Payne, Eds. Lawerence Erlbaum Associates, Carnegie-Mellon University, New York, pp. 165–184.
36. Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L., and Keeney, R. L. (1981). *Acceptable Risk*. Cambridge University Press, New York.
37. Fischhoff, B., Slovic, P., and Lichtenstein, S. (1982). Lay foibles and expert fables in judgements about risk. *Am. Stat.* **30**, 240–255.
38. Kahneman, D., and Tversky, A. (1984). Choices, values, and frames. *Am. Psychol.* **39**, 341–350.

# KEY APPLICATION AREAS

## AGRICULTURE AND FOOD SUPPLY

# VULNERABILITY OF THE DOMESTIC FOOD SUPPLY CHAIN

PETER CHALK
*RAND, Santa Monica, California*

## 1 INTRODUCTION

Over the past decade, the United States has moved to increase its ability to detect, prevent, and respond to terrorist threats and incidents. Much of this focus, which has involved considerable financial outlays, has aimed at upgrading public infrastructure through the development of vulnerability threat analyses designed to maximize both antiterrorist contingencies and consequence management modalities. Although many gaps remain, investments in preparedness, training, and response have helped with the development of at least nascent homeland incident command structures that have incrementally begun to span the ambit of potential terrorist attacks, from conventional bombings to more "exotic" biological, chemical, radiological, and nuclear incidents.

Agriculture and food production have received comparatively little attention in this regard, however. In terms of accurate threat assessments and consequence management procedures, these related sectors exist somewhat as latecomers to the growing emphasis that has been given to critical infrastructure protection (CIP) in this country. Indeed at the time of writing, total funding for protecting the nation's food supply stood at only $2.6 billion, a mere 2% of the US$130.7 billion in Congressional allocations earmarked for the United States Department of Agriculture (USDA) in Financial Year (FY) 2006.[1]

This article expands the debate on domestic homeland security by assessing the vulnerabilities of American agriculture and related products to a deliberate act of biological terrorism.[2] It begins by examining key attributes of contemporary US farming and food processing practices that make them susceptible to deliberate disruption. The article then examines the main impacts that would be likely to result from a concerted biological

[1]Agriculture, itself, was only included as a specific component of U.S. national counterterrorist strategy following al-Qaeda's attacks on the Pentagon and World Trade Center in September 2001 [1].

[2]For the purposes of this analysis, agro-terrorism will be defined as the deliberate introduction of a disease agent, either against livestock or into the general food chain, for the purposes of undermining national stability and/or engendering public fear. Depending on the disease agent and vector chosen, it is a tactic that can be used either to generate either economic, social, and political disruption or as a form of direct human aggression.

**TABLE 1 Selected FADs with Potential to Severely Impact Agricultural Populations and/or Trade**

| FAD | Mortality/Mortality | Zoonotic |
|---|---|---|
| Foot and Mouth Disease (FMD) | Less than 1%; however, morbidity near 100% | No |
| Classical swine fever (CSF) | High | No |
| African swine fever | 60–100%, depending on isolate virulence | No |
| Rinderpest (RP) virus | High | No |
| Rift valley fever (RVF) | 10–20% among adult populations; higher among young lambs, kids, and calves | Yes |
| Highly pathogenic avian influenza (AI) virus | Near 100% | Yes |
| Exotic Newcastle Disease (END) | 90–100% | Yes |
| Sheep and goat pox (SGP) viruses | Near 50%, although can be as high as 95% in animals less than one-year old | No |
| Vesicular stomatitis (VS) Virus | Low (however, morbidity near 90%) | Yes |

*Source:* Adapted from Committee on Foreign Animal Diseases, Foreign Animal Diseases.

attack against agriculture, focusing on both economic and political fallout. Finally an assessment of the operational utility of agro-terrorism is offered and contextualized in terms of the overall strategic and tactical calculations of the post-9/11 global jihadist militant movement.

## 2 VULNERABILITY OF US AGRICULTURE AND FOOD PRODUCTION TO BIOLOGICAL ATTACK

Agriculture and the general food industry are highly important to the economic and, arguably, political stability of the United States. Although farming directly employs less than 3% of the American population, one in eight people works in an occupation that is directly supported by food production [2]. In FY 2006, net cash farm gate receipts stood at over 64 billion, while a record US$68.7 billion was generated from agricultural exports—which, alone, equates to just under 1% of US Real Gross Domestic Product (GDP) [3].

Unfortunately, the mechanics for deliberately disrupting American agricultural and food production are neither expensive nor technically problematic. Many foreign animal diseases (FADs) can exist for extended periods of time on organic and inorganic matter and are characterized by rates of morality and/or morbidity (see Table 1 below), meaning that their latent potential to severely impact the health and trade in livestock is considerable. Significantly, the most lethal and contagious agents are nonzoonotic in nature, which necessarily precludes any need on the part of the perpetrator to have an advanced understanding of animal disease science or access to elaborate containment procedures (as there is no risk of accidental infection).[3]

[3]Analysis based on author interviews and field research conducted between 1999 and 2006.

Moreover, because contemporary farming practices in the United States are so concentrated and intensive,[4] a single point pathogenic introduction—if not immediately identified and contained—would be likely to spread very quickly. This is true both of crowded herds at the targeted facility and, due to the rapid and distant dissemination of animals from farm to market, to populations further afield. There is, in other words, no obstacle of weaponization to overcome as the primary vector for disease transmission is constituted by agricultural livestock itself.[5] This particular "facet" of agro-terrorism is noteworthy as the costs and difficulties associated with appropriately manufacturing viral and bacterial microbial agents for widespread dissemination are frequently cited as the most significant barriers preventing nonstate offensive use of biological agents.[6]

As noted above, early identification and containment of a disease is vital to physically check its geographic spread. However, there are at least three factors that work against such a (favorable) scenario. First, many veterinarians lack the necessary expertise and training to diagnose and treat Foot and Mouth Diseases (FMDs) of the sort that would be most likely to be used in a deliberate act of sabotage.[7] Second, producers are often reluctant to quickly report contagious outbreaks at their farms, fearing that if they do so they will be forced to carry out uncompensated (or at least undercompensated) depopulation measures.[8] Third, the possibility of emerging diseases being overlooked has steadily risen, largely because the scale of contemporary agricultural practices effectively negates the option of tending for animals on an individual basis.[9]

These various considerations have particular salience to FMD, which constitutes arguably the most threatening of all FADs. Although the disease is usually not fatal, it does cause the onset of rapid weight loss, oral/hoof lesions, lameness, and mastitis, effectively rendering any infected livestock population economically useless (in terms of milk and meat production).[10] More pointedly, FMD is extremely infectious,[11] environmentally hardy, frequently misdiagnosed,[12] and nonzoonotic—all of which directly contribute to its ease of management and potential rate of dissemination. The means for disseminating the virus could be as simple as scraping some vesicular droplets directly on to a cow (or other cloven hoof animal) or introducing the agent into a silage bin at a state agricultural fair or barn auction [6]. Given the intensive nature of contemporary American farming practices, a multifocal outbreak would be virtually assured: models developed by the USDA, for instance, have projected FMD that could be expected to spread to as many as 25 states in a minimum of 5 days.[13]

[4]Most dairies in the United States, for instance, can be expected to contain at least 1500 lactating cows at any one time, with some of the largest facilities host to upwards of 1000 animals.

[5]Analysis based on author interviews and field research conducted between 1999 and 2006.

[6]A good summary of the technical constraints inherent in weaponizing biological agents can be found in [4].

[7]Comments made by USDA officials attending the National Research Council National Security Implications of Advances in Biotechnology: Threats to Plants and Animals planning meeting, Washington D.C.:, August 1999.

[8]At the time of writing, no standardized or consistent system to compensate farmers affected by pathogenic outbreaks existed in the United States, with all indemnity payments determined on a case-by-case basis.

[9]Analysis based on author interviews and field research conducted between 1999 and 2006.

[10]For more on the etiology and effects of FMD see [5].

[11]FMD is one of the most contagious diseases known to medical science and has been equated as the animal equivalent to smallpox in terms of subject-to-subject spread.

[12]This reflects the general lack of expertise on the part of veterinarians in FAD identification as well as the fact that the clinical signs of FMD are not always immediately apparent (a pig, for instance, typically starts shedding vesicular droplets 7–10 days prior to symptoms becoming visibly evident).

[13]Author interviews with USDA officials, Washington D.C. and Maryland, 1999–2000.

Weaknesses and gaps are equally as pertinent to food processing and packing plants, particularly those that have proliferated at the lower to medium of the production spectrum. Thousands of these facilities exist across the United States, many of which exhibit uneven internal quality control,[14] questionable biosurveillance, and highly transient, unscreened workforces.[15] Entry–exit controls are not always adequate (and occasionally do not exist at all) and even basic measures, such as padlocking warehouses and storage rooms may not be practiced. Exacerbating problems are developments in the farm-to-table food continuum, which have greatly increased the number of potential entry points for easy to cultivate toxins and bacteria, such as botulism, *Escherichia coli*, and *Salmonella* (all of which are tasteless, odorless, and colorless).[16] Perishable, ready-to-eat products present a special hazard, largely because they are quickly distributed and consumed without cooking (a good "back-end" defense against microbial introduction) [8]. Moreover, because many small-scale operations do not maintain up-to-date (much less accurate) records of their distribution network, tracing exactly where a food item tainted in this manner may not be possible [9].

Underscoring these various difficulties is a dearth of definitive realtime technologies for detecting biological and chemical contaminants. As a result, possibilities for preemptive action are extremely limited as in virtually all cases health authorities would probably only become aware of an attack after it has occurred [10].

These gaps and weaknesses are particularly alarming given the lack of effective government regulation over food production and packing plants. While full implementation of the Hazard Analysis and Critical Control Points (HACCP)[17] is now theoretically in place at all factories that slaughter and process meat and poultry, the number of facilities that exist in the United States relative to available federal and state inspectors largely precludes options for enforced compliance and auditing.[18] Problems are even greater with regard to plants that deal with fresh-cut fruits and vegetables, most of which are devoid of any form of oversight or control [12]. Although a major food scare in 2006 involving spinach tainted with *E. coli* 0157:H7[19] has served to generate pressure for enhanced biosecurity and surveillance at these facilities, progress has been halting at best. Revised regulations issued by the Food and Drug Administration (FDA) in 2007[20]

[14]For instance, a facility manufacturing pre-packaged open-faced meat or poultry sandwiches fall under the authority of the USDA; those specializing in closed-faced varieties with identical ingredients come under the auspices of the Food and Drug Administration (FDA). The former will be inspected every day while the latter may only be checked once every five years [7].

[15]The Bush administration has pledged to upgrade the screening of workers employed at food processing and packing plants. At the time of writing, however, definitive checks had still to be put in place and it was still not apparent to what extent they would apply to small and medium scale plants throughout the United States.

[16]Analysis based on author interviews and field research conducted between 1999 and 2006.

[17]Under the HACCP rule, all meat and poultry producing facilities are required to identify critical control points where microbial contamination is likely to occur and enact Food Safety and Inspection Service (FSIS) designated systems to prevent or reduce the likelihood of it taking place. HACCP controls were introduced at the country's largest plants in January and have since been extended to all smaller facilities, including those with 10 employees or fewer.

[18]As of 2006, the number of inspectors at the USDA had declined from 9000 to 7500 and at the FDA from 2200 to 1962. See [11].

[19]The 2006 outbreak killed 3 and sickened 205. See [13].

[20]The 2007 guidelines are the first to have been issued since 1998. The new (voluntary) procedures call for constant monitoring and control of vulnerable places in the production cycle where bacteria are likely to form; urge regular record keeping for recalls; and outline recommendations relating to the health and hygiene of workers as well as sanitation operations. See [14].

remain voluntary; with the notable exception of California, most state governments have failed to put in place definitive guidelines of their own.[21]

## 3 IMPACT OF A MAJOR BIOLOGICAL ACT OF AGRO-TERRORISM

The ramifications of a concerted bioassault on the US meat and food base would be far-reaching and could extend beyond the immediate agricultural community to affect other segments of society. Perhaps one of the most immediate effects of a major act of biological agro-terrorism would be economic disruption, generating costs that could be expected to cross at least three levels. First, there would be direct losses resulting from containment measures and the eradication of disease-ridden livestock. Second, indirect multiplier effects would accrue both from compensation paid to farmers for the destruction of agricultural commodities[22] and revenue deficits suffered by both directly and indirectly related industries. Third, international costs in the form of protective embargoes imposed by major external trading partners would manifest.

As the 2001 FMD outbreak in the United Kingdom bears testimony, the overall extent of these costs could be enormous. The endemic, which led to the destruction of some 6,456,000 sheep cattle and pigs, is estimated to have cost the British government GBP2.7 billion (see Table 2), equivalent to over 0.2% of the country's GDP at the time. In addition, there were substantial knock-on effects to other sectors of the economy, impacting on even distantly related industries. Tourism, for instance, is projected to have lost between GBP2.7 and GBP3.2 billion of value added in 2001 as a result of the closure/quarantine of farms located in or near popular holiday destinations, such as the Lake District and Peak District [15].

The effects of a multifocal outbreak in the United States would far exceed these figures simply because the scale of agriculture in the country is far greater than that in the United Kingdom. The 1999 study that projected eight different scenarios associated with a theoretical FMD outbreak in California, for instance, concluded that losses from depopulation measures, quarantine, and trade/output disruption to this state alone would exceed US$13 billion [16].

The potential for punitive costs arising out of agro-terrorism are equally as pertinent to product contamination. At the time of writing, the projected costs to the American spinach industry of the 2006 *E coli* outbreak, noted above, were expected to be between $75 and $100 million, with each acre loss amounting to roughly $3700 for the farmer [17]. Although the incident was accidental, it provides a good data point to illustrate how quickly negative fiscal reverberations can ensue from cases of food poisoning.

Beyond its economic impact, a successful biological strike against agriculture could undermine confidence and support in government. Successfully releasing contagious agents against livestock might cause people to lose confidence in the safety of the food supply and could possibly lead them to question the effectiveness of existing contingency planning against weapons of mass destruction in general. Critics, perhaps unfairly

[21] Following the *E coli* outbreak, which originated from farms and production plants in Salinas and Oxnard, California moved to put in place stringent, mandatory rules covering water quality, worker sanitation, and wildlife control. At the time of writing, some 90% of the state's lettuce and leafy green processors were by these standards.

[22] Although the United States has no standardized system of compensation in place, Federal funds would be forthcoming in the event of a large-scale agricultural disaster such as a multifocal outbreak of FMD.

**TABLE 2 Expenditure by the United Kingdom Government in Response to the 2001 FMD Outbreak**

| Activity | Actual Expenditure to May 24, 2002 (GBP million) |
|---|---|
| **Payments to farmers** | |
| Compensation paid to farmers for animals culled and items seized or destroyedy | 1130 |
| Payments to farmers for animals slaughtered for welfare reasons[a] | 211 |
| **Total payments to farmers** | **1341** |
| **Direct costs of measures to deal with the epidemic** | |
| Haulage, disposal and additional building work | 252 |
| Cleaning and disinfecting | 295 |
| Extra human resource costs | 217 |
| Administration of the Livestock Welfare (Disposal) Scheme | 164 |
| Payments to other government departments, local authorities, agencies and others | 73 |
| Miscellaneous, including seriology, slaughterers, valuers, equipment, and vaccine | 66 |
| Claims against the Ministry of agriculture | 5 |
| **Total direct costs** | **1074** |
| **Other costs** | |
| Cost of government departments' staff time | 100 |
| Support measures for businesses affected by the outbreak[b] | 282 |
| **Total other costs** | **382** |
| **Total costs** | **2797** |

[a]Includes payments of GBP205.4 million under the Livestock Welfare (Disposal) Scheme and GBP3.5 million under the Light Lambs Scheme.
[b]Includes money available under European Union (EU) market support measures for agri-monetary compensation in respect of currency movements.

and with the benefit of hindsight, would doubtless demand why the intelligence services failed to detect that an attack was forthcoming and why the agriculture sector was left exposed. In an age where counterterrorism has emerged as arguably the country's single most important national security priority, such reactions could conceivably serve to undermine popular perceptions of state effectiveness, if not credibility.

The actual mechanics of dealing with an act of agricultural bioterrorism could also generate public criticism. Containing a major disease outbreak would necessitate the slaughter of hundreds of thousands of animals, particularly in cases where no concerted vaccination was in place. Euthanizing such volumes has the potential to generate vigorous opposition from the general population—not to mention farmers and animal rights advocates—particularly if slaughtering involved susceptible but nondisease showing herds (in so-called "stamping out" operations) and/or wildlife. To be sure, mass eradication has occurred in the past in the United States without triggering widespread civil disquiet. However, such operations have not involved large-scale husbandry (for the most part focusing on poultry flocks) nor have they been the subject of intensive media interest and scrutiny. It is these latter aspects that have relevance in terms of assessing the possible fallout from culling measures, largely because they necessarily mean there

has never been a visual point of reference to prepare the American general public for the consequences of eradicating highly visible animal herds [18].

The 2001 FMD outbreak in the United Kingdom, again, provides a salient example of the political ramifications that can result from mass animal eradication. The measures instituted by the Blair administration to stem the epidemic elicited significant criticism from farmers, scientists, opposition politicians (many of whom claimed that the government's actions were entirely unethical), and the public (especially after it discovered that FMD did not actually kill infected animals).[23] The following commentary in the Times newspaper is representative of the type of outrage that was expressed during the height of the crisis:

> Policy on foot and mouth disease is now running on autopilot . . . . Nothing in the entire history of the common agriculture policy has been so crazy. The slaughter is not declining but running at 80,000 a day . . . . At the last estimate, 95 percent of the three to four million animals dead or awaiting death are healthy . . . . The obscenity of the policy is said to be irrelevant "because of its success". Yet what other industry would be allowed to protect its profits by paying soldiers with spades to kill piglets and drown lambs in streams? What other industry could get civil servants to bury cattle alive or take pot shots at cows from a 60 ft range? What other industry can summon teams from Whitehall to roam the lanes of Forest Dean, as one frantic farmer telephoned me, "like Nazi stormtroopers seeking healthy sheep to kill on the authority of a map reference?" [19]

## 4 BIOLOGICAL ASSAULTS AGAINST AGRICULTURE AND TERRORISM MODUS OPERANDI

Despite the ease by which an act of agro-terrorism could be carried out and the severe political and economic ramifications that a successful assault could elicit, it is unlikely to constitute a primary form of terrorist aggression. This is because such acts would probably be viewed as "too dry" in comparison with traditional tactics in the sense that they do not produce immediate, visible effects. The impact, while significant, is delayed—lacking a single point of reference for the media to focus on (and highlight) [20].

In this light, it is perhaps understandable that biological attacks against agriculture have not emerged as more of a problem. Indeed, since 1912, there have only been 14 documented cases involving the substate use of pathogenic agents to infect livestock or contaminate related products (see Table 3). Of these, only three incidents could realistically be linked to a wider campaign of political violence and/or intimidation: the 1952 Mau Mau plant toxin incident in Kenya, the 1984 Rajneeshee Cult salmonella food poisoning in Oregon, and the release of sewer water onto Palestinian agricultural fields by Israeli settlers in 2000 (see Table 3).[24]

[23] Author observations, United Kingdom, June-July 2001.

[24] In addition to these cases, there have also been four confirmed uses of chemical agents to contaminate agricultural products: (i) The use of cyanide to poison the water supply of a 1000-acre farm owned and operated by Black Muslims in Ashville, Alabama (1970); alleged perpetrator: the local chapter of the Ku Klux Klan (KKK). (ii) The use of cyanide to poison Chilean grape exports (1989); perpetrator: antiPinochet militants. (iii) The use of chlordane (a pesticide) to contaminate animal feed manufactured by National By-Products, Inc. in Berlin, Wisconsim (1996); perpetrator: Brian "Skip" Lea, the owner of a rival animal food processing facility. (iv) The use of "black leaf 40" (an insecticide) to contaminate 200 pounds of ground beef in Michigan (2003); perpetrator: randy Betram, a disgruntled employee at the Byron Center Family Fare Supermarket. For further details see [21].

**TABLE 3 Nonstate Use of Biological/Toxic Agents Against Agriculture and Food, 1912–2006**

| Year | Nature of Incident | Alleged Perpetrators |
|---|---|---|
| **Confirmed use of agent** | | |
| 2000 | Contamination of Palestinian agricultural land with sewer water | Israeli settlers in the West Bank |
| 1997 | The spread of hemorrhagic virus among the wild rabbit population in New Zealand | New Zealand farmers |
| 1996 | Food poisoning using *Shigella* in a Texas hospital | Hospital lab worker |
| 1995 | Food poisoning of estranged husband using ricin | Kansas physician |
| 1984 | Food poisoning using *Salmonella* in salad bars in Oregon | Rajneeshee Cult |
| 1970 | Food poisoning of Canadian college students | Estranged roommate |
| 1964 | Food poisoning in Japan using *Salmonella* and dysentery agents | Japanese physician |
| 1952 | Use of African bush milk (plant toxin) to infect livestock | Mau Mau |
| 1939 | Food poisoning in Japan using *Salmonella* | Japanese physician |
| 1936 | Food poisoning in Japan using *Salmonella* | Japanese physician |
| 1916 | Food poisoning in New York using various biological agents | Dentist |
| 1913 | Food poisoning in Germany using cholera and typhus | Former chemist employee |
| 1912 | Food poisoning in France using *Salmonella* and toxic mushrooms | French druggist |
| **Threatened use of agent** | | |
| 1984 | Attempt to kill a racehorse with various pathogens (insurance scam); confirmed possession | Two Canadians |
| 1984 | Threat to introduce FMD into wild pigs, which would then infect livestock; no confirmed possession | Australian prison inmate |

*Source:* Carus, *Bioterrorism and Biocrimes*; Parker, *Agricultural Bioterrorism*, 2–21; CNS, "Chronology of CBW Incidents Targeting Agriculture and Food Systems, 1915–2006."

That being said, agro-terrorism could emerge as favored form of secondary aggression that is designed to exacerbate and entrench the general societal disorientation caused by a more conventional campaign of bombings. The mere ability to employ cheap and unsophisticated means to undermine a state's economic base and possibly overwhelm its public management resources give livestock and food-related attacks a beneficial cost/benefit payoff that would be of interest to any group faced with significant power asymmetries.

For at least two reasons, these considerations have particular relevance to the international jihadist movement that is ideologically personified by Al-Qaeda. First, Bin Laden has long asserted that using biological agents in any manner possible to harm western interests is a religious duty beholdent on all Muslims and one that is perfectly inline with religious precepts as set forth by Allah [22]. While the thrust of this message has undoubtedly been toward mass strikes intended to inflict large-scale loss of human life, the ability to pull off audacious operations on this scale is highly questionable given the tactical and strategic set-backs that have befallen Islamist extremists as a result of the Global War on Terror (GWOT) post-9/11.[25] Bioattacks against agriculture, however, would appear to be ideally suited to the operational constraints of the post-9/11 era in that they are cheap, low risk, easy to perpetrate, and well-attuned to the operational capabilities of locally based affiliates acting in a largely self-sufficient, if not fully independent manner.

Second, as discussed agro-terrorism has a genuine capacity to economically disrupt and destabilize. This would fit well with Al-Qaeda's self-declared intention to destroy Washington (and its western allies) through a concerted "bleed to bankruptcy" strategy. Initially enunciated by Bin Laden in 2004, this approach stems from a conviction that the United States is a "paper tiger" that can be crippled simply by removing the key anchors and pillars, which are critical to upholding the integrity of the country's fiscal base [24].[26] More specifically, it is a stratagem that seeks to impose a debilitating asymmetric cost-burden[27] on the American economy through the use of modalities that, while cheap, retain a realistic capacity to trigger cascading, ultimately nonsustainable monetary effects [26]. Disseminating biological agents against agricultural livestock and products would certainly fulfill such a requirement.

## REFERENCES

1. United States Department of Agriculture (2006). *2006 Performance and Accountability Report*, USDA, Washington, DC, 5, p. 48.
2. (a) Agriculture Research Service (2000). *Econoterrorism, a.k.a. Agricultural Bioterrorism or Asymmetric Use of Bioweapons*, unclassified briefing given before the USDA, February 28; (b) Henry, P. (2002). *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, Institute for National Strategic Studies, National Defense University, Washington, DC, p. 11.

[25]These set-backs include the loss of safehaven in Afghanistan, the elimination/detention of senior midlevel commanders and the seizure of terrorist finances. The combined effect has been to transform Al-Qaeda into a movement of movements that has become more nebulous, segmented, and polycentric in nature and one which has, accordingly, been forced to focus on attacks that offer "the course of least resistance". For more on the operational dynamics of Al-Qaeda post-9/11 see [23].

[26]For Bin Laden, the American economy constitutes the principal anchor of a morally bankrupt and dysfunctional western system that he regards has prevented Islam from assuming its "rightful" place as the world's pre-eminent religion and culture.

[27]Al-Qaeda has made much of the economic burden imposed by the GWOT, stressing that for every US$1 spent by the international jihadist movement, US$1 million was being expended by the United States. In many ways this assessment has been borne out. A study by the UK-based International Institute for Strategic Studies (IISS), for instance, calculated the costs of the global war on terror to Al-Qaeda at roughly US$500,000 compared to US$500 billion for Washington (not taking into account budgetary allocations for the war in Iraq). See [25].

3. (a) USDA *2006 Performance and Accountability Report*, 48; (b) *Statement by Keith Collins, Chief Economist, USDA, Before the Senate Appropriations Subcommittee on Agriculture, Rural Development and Related Agencies*, 30 march 2006, available on-line at http://www.usda.gov/oce/newsroom/congressional_testimony/Collins_SenateApprop_033006.doc, last accessed March 11, 2006.
4. Carus, S. (1999). *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents in the 20th Century*, Center for Counterproliferation Research, National Defense University, Washington, DC, pp. 26–29.
5. Committee on Foreign Animal Diseases (1998). *Foreign Animal Diseases*, United States Animal Health Association, Richmond, VA, pp. 213–224
6. *Observations Made During the Blue Ribbon Panel on the Threat of Terrorism to Livestock and Livestock Products*, White House Conference Center, Washington DC, December 8–9, (2003).
7. (a) *Testimony of Robert Robinson, "Food Safety and Security," given before the Subcommittee on Oversight of Government Management, Restructuring, and the District of Columbia of the Committee on Governmental Affairs*, U.S. Senate, Washington, DC, October 10, (2001); (b) Has politics contaminated the food supply. *NY Times* December 11, (2006).
8. Habenstreit, L. (2007). Workshop aims to protect Asia-Pacific region's food supply from deliberate contamination. *Foreign Agricultural Service (FAS) Worldwide*, available on-line at http://www.fas.usda.gov/info/fasworldwide/2007/01-2007/FoodDefense.htm, last accessed March 12, 2007.
9. California Department of Health and Human Services (2000). *Author Interviews*, Sacramento, August.
10. Canadian Food Inspection Agency (CFIA) (2006). *Workshop on the Assessment of Risk and Vulnerability in Relation to Terrorism*, Ottawa, March 21–23.
11. Martin, A. (2006). Stronger rules and more oversight for produce likely after outbreaks of E-coli. *NY Times*, December 11.
12. Pollan, M. (2006). The vegetable-industrial complex. *NY Times Mag*.
13. Food and Drug Administration (2007). *FDA Finalizes Report on 2006 Spinach Outbreak*, *FDA News*, March 23, available on-line at http://www.fda.gov/bbs/topics/NEWS/2007/NEW01593.html, last accessed March 27, 2007.
14. Burros, M. (2007). F.D.A. offers guidelines to fresh-food industry. *NY Times*.
15. *Foot and Mouth Disease 2001: Lessons to Be Learned Inquiry Report*, Her Majesty's Stationery Office (HMSO), London, 22 July 2002, pp. 130–135.
16. Ekboir, J. (1999). *Potential Impact of Footy-and-Mouth Disease in California*, Agricultural Issues Center, University of California, Davis, Davis, CA, p. 65.
17. (a) McKinley, J. Farmers vow new procedures; Bacteria eyed in boy's death. *NY Times* September 22, 2006; (b) Wood, D. (2007). Spinach growers tally losses. *Christ. Sci. Monitor* September 27, 2006, available on-line at http://www.csmonitor.com/2006/0922/p02s01-usec.html, last accessed March 27; (c) *Spinach Farmers Try to Grow Public's Confidence*, *MSNBC News*, October 2, 2006, http://www.msnbc.msn.com/id/15095551 last accessed March 27, 2007.
18. Agriculture Research Service (ARS) (2003). *Author Interview*, Washington, DC, October.
19. Jenkins, S. (2001). This wretched cult of blood and money. *The Times*
20. Jenkins, B. (1988). Future Trends in International Terrorism. In *Current Perspectives on International Terrorism*, R. Slater, M., and Stohl, Eds. Macmillan Press, London.

21. (a) Bioterrorism–the threat in the western hemisphere. Pan American Health Organization, 13th Inter-American Meeting, at the Ministerial Level, On Health and Agriculture. Washington, DC, 24–25 April, 2003; (b) *Chronology of CBW Incidents Targeting Agriculture and Food Systems 1915–2006*, Monterey Institute for International Studies (MIIS) Center for Nonproliferation Studies (CNS), June 2006, available on-line at http://cns.miis.edu/research/cbw/agchron.htm, last accessed March 27, 2007; (c) Wooton, J. (1970). Black muslims would sell farm to klan. *NY Times*; (d) Poison is suspected in death of 30 cows on a muslim farm. *NY Times* (March 16, 1970); (e) Jones, R. (1997). Product recalled in four states; animal feed tainted in Act of Sabotage. *Milw. J. Sentinel*; (f) Neher, N. *Food Terrorism: The Need for a Coordinated Response–The Wisconsin Experience*, Wisconsin Department of Agriculture, Trade and Consumer Protection, n.d.a.
22. (a) The world's newest fear: germ warfare. *Vanc. Sun* (Canada), September 24, 2001; (b) Fear and breathing. *Economist* September 29, 2001.
23. Chalk, P., Hoffman, B., Reville, R., and Kasupski, A.-B. (2005). *Trends in Terrorism: Threats to the United States and the Future of the Terrorism Risk Insurance Act*, RAND, Santa Monica, CA, pp. 11–16.
24. (a) Chalk et al., *Trends in Terrorism*, pp. 13–14; (b) Flynn, S. (2004). The neglected homefront. *Foreign Aff*. (September/October), 25.
25. Hunt, M. (2007). Bleed to bankruptcy. *Jane's Intell. Rev*. 14–15.
26. Hunt, M. (2007). Bleed to bankruptcy. *Jane's Intell. Rev*. 14–17.

## FURTHER READING

Administration plans to use plum island to combat terrorism. *NY Times* September 21, (1999).

Agriculture Research Service (1961). *Agriculture's Defense Against Biological Warfare and Other Outbreaks*, USDA, Washington, DC.

Agro-terrorism still a credible threat. *Wall St. J*. December 6, (2001).

Brown, C. The impact and risk of foreign animal diseases. *Vet. Med. Today* **208**(7).

Chalk, P. (2004). *Hitting America's Soft Underbelly. The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Food Industry*, RAND, Santa Monica, CA.

Gordon, J., and Bech-Nielsen, S. (1986). Biological terrorism: a direct threat to our livestock industry. *Mil. Med*. **151**(7).

Gorman, S. (1999). Bioterror down on the farm. *Natl. J*. **27**.

Hugh-Jones, M., and Brown, C. (2006). Accidental and intentional animal disease outbreaks: assessing the risk and preparing an effective response. In *Biological Disasters of Animal Origin: The Role and Preparedness of Veterinary and Public Health Services*, M. Hugh-Jones, Ed. Scientific and Technical Review, Dinh Nam, Vol. **25**, No. 1, Special Issue.

Kelly, T., Chalk, P., Bonomo, J., Parachini, J., Jackson, B., and Cecchine, G. (2004). The office of science and technology policy Blue Ribbon Panel on the threat of biological terrorism directed against livestock. *Proceedings of a Conference*, RAND, Santa Monica, CA.

Parker, H. (2002). *Agricultural Bioterrorism: A Federal Strategy to Meet the Threat*, McNair Paper 65. Institute for National Strategic Studies, Washington, DC.

Steele, N. (2000). *U.S. Agricultural Productivity, Concentration and Vulnerability to Biological Weapons*, Unclassified Briefing, Department of Defense Futures Intelligence Program, Washington, DC.

# THE GLOBAL FOOD SUPPLY CHAIN

JUSTIN J. KASTNER
*Kansas State University, Manhattan, Kansas*
COBUS L. BLOCK
*University of Wyoming, Laramie, Wyoming*

## 1 INTRODUCTION

Any attempt to understand the global food supply chain and its security must draw on multiple academic perspectives. Indeed, today's multidimensional global food supply chain—which features a range of state and private actors (e.g. producers, consumers, intermediary companies, and a cornucopia of regulatory institutions) and issues (e.g. social, economic, and political concerns)—is best understood using a multidisciplinary approach [1]. Perhaps fittingly, this article is authored by scholars affiliated with the expressly interdisciplinary *Frontier* program for the historical studies of border security, food security, and trade policy (http://frontier.k-state.edu). Drawing on food science, public health, history, political science, economics, and the discipline of international political economy, this article seeks to describe the inherent complexity of the global food supply chain including food security-seeking policies and programs that have been adopted by governments and food companies, external threats including, but not limited to, agroterrorism and bioterrorism, and novel approaches whereby public and private institutions and agents can better manage the safety and security of food supply chains that span borders. The article concludes with outstanding research questions and themes relevant to ensuring the safety and security of the global food supply chain.

## 2 THE GLOBAL FOOD SUPPLY CHAIN: A COMPLEX NETWORK OF INDUSTRY STANDARDS, GOVERNMENT REGULATIONS, AND BUSINESS PRACTICES

In today's globalized economy, food moves along a multisegmented production-to-consumption sequence: from primary producers to processors and manufacturers, to distributors and wholesalers, to retailers, and ultimately to consumers. This supply chain is further complicated when food crosses nation-state borders—perhaps multiple times. At different points, businesses and governments intervene in this flow to ensure food safety and food security.

The term *food security* is oftentimes contested and its meaning debated across history. Although previously food security connoted ensuring enough food for a population, today food security covers many different aspects of the global food supply chain—ensuring a safe, secure, adequate, as well as cost-effective food supply [2]. This comprehensive understanding of food security requires an appreciation that cross-border trade flows

*both* ensure food security through the provision of food imports and, potentially, can threaten food security through the introduction of accidentally introduced or deliberately introduced hazards.

The global food supply chain begins with the production-oriented foundation—agriculture. Agriculture, viewed by some as the "first step" in the supply chain, involves the growing of plants and raising of animals for food and other materials. Multiple countries are involved in agricultural production, and in many agricultural sectors production is concentrated in a relatively small set of geographically large countries. For example, in arable agriculture, China produces the most rice, wheat, and potatoes; the United States grows the most corn (maize) and soybeans (soya); and the Russian Federation produces the most barley [3].

From this, the first step of production is succeeded by a complex network of transportation, processing, manufacturing, packaging, distribution, retailing, and food service institutions. In the United States and elsewhere, history has witnessed the development of multiple laws, agencies, and regulations to help ensure the safety and security of the food supply. Although some countries (e.g. the United Kingdom) have since instituted efforts to consolidate governance (e.g. in the UK Food Standards Agency), others (e.g. the United States) continue to regulate the food supply chain with a litany of institutions and laws—arguably, as many as 15 agencies and 35 laws, depending on how one organizes and counts them [4, 5].

Although agriculture is viewed by some as the "first step" in the global food supply chain, attention is also due to those economic and technological realities at work that make agriculture—and, indeed, the subsequent steps of the global food supply chain possible—possible in the first place. Both economic forces (often through the form of foreign direct investment) and technology represent kinds of "prerequisites" that help ensure not only the production of food but also its distribution, safety, and security. In this regard, an historical perspective is illustrative. During the late nineteenth century, the agricultural production capacity of the United States expanded due in part to the provision of capital in the US agricultural enterprises. From ranches and meat-packing to farms and milling, Great Britain helped plant the seeds for food supply chains that would bring, to Britain and elsewhere, foodstuffs from the United States [6]. British investment in railroads and steamship transportation also assisted in the enabling of a supply chain that, in effect, helped ensure the provision of enough food for a growing British population [7]. The reality of foreign direct investment shows that there are, upstream from agricultural production, economic elements in the food supply chain.

Downstream from investment and agricultural production, one sees food transverse state borders. The volumes of food produced, exported, and imported are such that 100% inspection by food safety and food security officials is, quite simply, not possible [8]. Therefore, risk management—oriented approaches are needed. In recent history, many food companies and governments have adopted, for example, Hazard Analysis and Critical Control Point (HACCP) systems that can be used to manage risks in both domestic and global food supply chains. Broadly, the principles of HACCP were adopted in the United States and European Union (EU) in 1992 and 1993. The Codex Alimentarius Commission, which is one of the three food-trade standard-setting bodies recognized by the World Trade Organization (WTO), adopted HACCP principles in 1993 [9]. Since 1993, countries and companies across the globe have embraced HACCP through regulations as well as business practices.

Although HACCP deals with biological, chemical, and physical hazards in the food system, it does not necessarily ensure another key element of supply chain security: traceability and in-plant security. In a 2007 food industry magazine, Alan Naditz cites Washington State University food-bioterrorism expert Dr. Barbara Rosco Washington State University, in this regard; food-supply chain security requires knowledge of both the origin and status of food products and the only way to ensure that is to have robust programs that can trace food and ensure food-plant security [10]. Not surprisingly, recent years have witnessed ramped-up efforts to institute animal identification and crop traceability programs, as well as food defense planning designed to ensure food-plant security.

## 3 THREATS AND CHALLENGES TO THE NORMAL FUNCTIONING OF THE GLOBAL FOOD SUPPLY CHAINS

The global agricultural and food trade, long recognized as one of the most contentious areas of world economic affairs [11], has become more problematic as concerns about agroterrorism and bioterrorism have elicited new governmental regulations and business practices. In addition, health-protection regulations have spawned trade disputes,and previously excluded social considerations have entered into regulation and marketing activities along the global food supply chain. Today, economic and liability pressures are increasingly felt "upstream" in the supply chain. The example of China illustrates many formidable food-security challenges.

### 3.1 Agroterrorism and Bioterrorism

Since the terrorist attacks on the United States on September 11, 2001, renewed attention has come to the twin issues of "agroterrorism" and "bioterrorism." In this regard, the following definitions, courtesy of the Center for Food Security and Public Health at Iowa State University, offer an introductory explanation:

*Agroterrorism.* The use, or threatened use, of biological (to include toxins), chemical, or radiological agents against some component of agriculture in such a way as to adversely impact the agriculture industry or any component thereof, the economy, or the consuming public [12].

*Bioterrorism.* The use of microorganisms or toxins derived from living organisms to cause death or disease in humans, animals, or plants in civilian settings [13].

Agroterrorism threatens a nation-state's food security because it targets the ability of that nation to produce food—namely, the early production step in the food supply chain. An agroterrorist attack could, conceivably, lead to economic chaos in the form of higher food prices, unemployment, and disruption of international trade flows. Agriculture in geographically large countries is what security theorists term a *soft* target; it is virtually impossible to guarantee the protection of such geographically vast elements in the food supply chain. Bioterrorist attacks on the global supply chain involve intentional introduction of hazards into the food supply.

Concerns with agroterrorism and bioterrorism have spawned policy and regulatory responses by nation-state governments, worldwide. In 2002, the US Congress passed the *Public Health Security and Bioterrorism Preparedness and Response Act* (Bioterrorism Act). The Bioterrorism Act's third section, entitled "Protecting Safety and Security of Food and Drug Supply," granted new powers to the US Food and Drug Administration (FDA). These included the ability to detain suspect food import shipments and the

authority to mandate companies manufacturing food for US consumption to register their facilities. The US Department of Agriculture (USDA) Food Safety and Inspection Service, which regulates the meat and poultry industries, already had many of these new powers. Because of the Bioterrorism Act, the FDA can now detain food shipmentsif evidence indicates that they present a threat to humans or animals. Also, largely due to the 2002 Bioterrorism Act, hundreds of thousands of facilities—in the United States and abroad—must register with the FDA.

In addition to registration and detention authorities, the 2002 Bioterrorism Act has incorporated new regulatory steps into parts of the global food supply chain that cross the United States. The "prior notice" provision of the Bioterrorism Act requires that food companies notify the FDA of all food import shipments; the prior notice regulation is intended to help the FDA better manage risk. The detailed information submitted via "prior notice" is used by the FDA so they can better deploy resources to conduct inspections (e.g. targeting inspection resources toward new or unfamiliar food-shipping firms) and intercept contaminated products.

The Bioterrorism Act's food security provisions also included the development of new regulatory categories for threats and agents. The new categories address specific regulatory authorities. Department of Health and Human Service (HHS) agents include select agents, such as Ebola virus and *Yersinia pestis*, as well as toxins such as ricin; HHS has the sole authority over these agents. USDA-only agents include agents, such as foot and mouth disease virus and rinderpest virus that may affect animal or plant products; the USDA has the regulatory purview over these agents. Thirdly, overlap agents, including, for example, *Bacillus anthracis* (anthrax), may be subject to regulation by either or both HHS and USDA.

### 3.2 Trade Disputes Regarding the Use of Sanitary and Phytosanitary Measures

Global food supply chains have, in recent years, been complicated by disputes over import regulations related to sanitary (food safety and animal health) and phytosanitary (plant health) import-restricting measures. At the close of the twentieth century, transatlantic tensions over EU restrictions on the importation of North American beef produced with growth promoting hormones culminated in the first WTO ruling under the terms of the *Agreement on the Application of Sanitary and Phytosanitary Measures* (SPS Agreement) [14]. While typically adopted by governments to protect health, sanitary and phytosanitary regulations present a new kind of challenge for the global food supply chain; they offer a means by which nation-states can restrict trade under the guise of health protection [15].

International policy differences related to safety of genetically engineered organisms in food have also caused great consternation within supply chains [16]. In addition to fueling trade rows between, for example, the United States (US) and the EU, the GE issue has encouraged the adoption, in some countries, of technical standards designed to help companies ensure they are supplying and receiving food ingredients and products with especially particular (e.g. non-GE) specifications [3, pp. 95–96].

### 3.3 Social Regulations and New Upstream Pressures in the Global Food Supply Chain

The transatlantic divide over biotechnology policy, concurrent with a transatlantic rift of consumer views regarding GE foods, points to a broader trend within the global food supply chain: the adoption of business practices and government regulations that, for some, might be deemed as social regulations [16].

Today's food-trade agenda is increasingly dominated by such issues related more to production process preferences (e.g. organic agricultural practices) than end-product safety and security. (Organic agricultural practices, which are defined differently by different companies and nation-state governments, generally involves a system of farming that promotes "natural" rather than "artificial" forms of pest and disease controls and fertilizers [3].) Global activist and consumer-advocacy groups have exerted tremendous influence on companies—especially retailers in Europe—and a web of private and government standards have developed to cater to the organic and GE-free sentiments of consumers. Lamentably, this has resulted in some alarming consequences within the global food supply chain; for example, in 2002 shipments of North American food aid produced using GE technology were subject to import restrictions in Zambia, even during a time of famine and starvation [17]. Scholars writing for the *African Journal of Biotechnology* maintain that a balanced approach to the regulation of GE foods regulation is required [18].

Other upstream pressures—most notably, liability forces mediated by class-action and other lawsuits—are increasingly influential in the global food supply chain. As foodborne disease surveillance data has become more plentiful, and as public health authorities have become better adept at identifying sources of outbreaks, large-scale lawsuits have exerted new kinds of pressure upstream toward the agricultural production end of the food supply chain. The 2006 outbreak of *Escherichia coli* O157:H7, which cost the spinach industry millions of dollars through costs including, but not limited to, lawsuits, prompted produce-oriented firms to look further upstream and enhance microbial testing of irrigation water, soil amendments, and plant tissues [10].

### 3.4 Traceability and Transparency: the Example of China

China plays an important role in the global food supply chain as both a producer and a consumer. With 1.5 billion consumers, providing enough food in China represents a major policy challenge [19]. China is also a major exporter of agricultural and food products, including seafood that, in recent years, have fueled worries about food safety and security [20]. While countries in the developing world (e.g. the United States and Japan) that import products from China have cried for improved regulations, the growing "middle class" in China is also demanding better food, and higher safety levels. As told in a recent commentary by a *Frontier* research assistant studying food security and trade issues there, China is experiencing pressure from *both* foreign markets and its own people to offer a safer supply of food. To that end, a more secure food supply chain will be needed. Multiple challenges—amongst others, traceability, transparency, and time—require the attention of the Chinese government and agriculture and food sector. With 300 million low-income farmers, cash-based recordless transactions and slow distribution channels make it presently difficult to ensure supply chain traceability, as well as accurate records required for transparency, food quality, and business efficiency [21].

## 4 NOVEL APPROACHES TO MANAGING SUPPLY CHAINS ACROSS BORDERS

The multilateral trading system's framework for governing the global food supply chain features institutions and agreements that offer opportunities for uniquely managing food

security threats in international trade. Under the WTO *Agreement on the Application of Sanitary and Phytosanitary Measures* (WTO Agreement), WTO member countries have the right to establish regulatory measures to protect animal, plant, and human health on the basis of scientific principles; to facilitate trade, WTO members are encouraged to follow standards and guidelines developed by three international scientific standard-setting bodies (i.e. the World Organization for Animal Health (OIE), the Codex Alimentarius Commission, and the International Plant Protection Convention (IPPC)), often termed the *three sisters* [22].

The concepts of "regionalization" (also known as *zoning*) and "compartmentalization" are affirmed by the WTO, the SPS Agreement, and the three sisters. Both concepts present internationally endorsed means by which nation-states can preserve trade relations when sanitary (human or animal health) or phytosanitary (plant health) hazards threaten a country's trading status; however, the concepts are often difficult to implement. Because global agricultural biosecurity and food-safety concerns (such as highly pathogenic avian influenza, foot and mouth disease, and bovine spongiform encephalopathy (BSE)) persist, regulatory and business stakeholders have become increasingly interested in certifying subnational geographic disease-free zones (i.e. regionalization) as well as biosecure establishments, supply chains, and/or animal subpopulations (i.e. compartmentalization) for international trade.

Helpful definitions for the key terms for trade policy concepts of regionalization and compartmentalization include the following:

- *Zone/region.* A clearly defined part of a country containing an animal subpopulation with a distinct health status with respect to a specific disease for which required surveillance, control, and biosecurity measures have been applied for the purpose of international trade.
- *Compartment.* One or more establishments under a common biosecurity management system containing an animal subpopulation with a distinct health status with respect to a specific disease or specific diseases for which required surveillance, control, and biosecurity measures have been applied for the purpose of international trade [23].

Member countries of the OIE and WTO have, for years, used regionalization by defining disease-free areas with respect to, for example, particular animal diseases (foot and mouth disease, brucellosis, etc.). For example, both the USDA Animal and Plant Health Inspection Service and the EU Food and Veterinary Office have evaluated applications from trading partners seeking to certify, for trade purposes, disease-free regions or zones from which they can export animal products to the United States and EU.

The concept of compartmentalization is a recent addition to the OIE codes and "extends the application of a 'risk boundary' beyond that of a geographical interface and considers all epidemiological factors that can contribute to the creation of an effective boundary" [23, p. 873]. Compartmentalization may be applied to specific herds, feed supply chains, establishments, premises, etc. A disease-specific compartment might include a cattle establishment defined as a *bovine spongiform encephalopathy* free compartment through demonstrable feed source management, animal movement documentation, and livestock identification [23].

Interest in compartmentalization is growing. 2006 witnessed the development of general considerations for implementing compartmentalization. These guidelines include the

following factors: (i) the nature or definition of the compartment, (ii) epidemiological separation of the compartment from potential sources of infection, (iii) documentation of factors critical to the definition of the compartment, (iv) supervision and control of the compartment, (v) surveillance for the agent or disease, (vi) diagnostic capabilities, and (vii) emergency response, control, and notification capability [23]. Compartmentalization provides a unique opportunity for vertically integrated elements of the global food supply chain to, through business practices and regulatory oversight, insulate themselves from biosecurity problems experienced elsewhere.

## 5 FUTURE RESEARCH NEEDS

The global food supply chain will continue to develop by research and development (indeed, innovation and investment) into technologies that can help provide security. Among other research areas, how best to provide supply chain traceability and in-plant security are salient research questions. The trade policy concepts of regionalization and compartmentalization represent ways whereby governments and businesses (the key state and private actors involved in international trade) can better cooperate along the food supply continuum. However, important research policy questions remain. These include the following.

1. What challenges and opportunities do food companies perceive in the implementation of the concepts of regionalization and compartmentalization?
2. How are government policies, regulations, and workflows responding to regionalization and compartmentalization?
3. How can all actors involved with the global food supply chain work better together to ensure security?
4. How might tools such as traceability systems help develop compartmentalized segments of the global food supply chain?

## REFERENCES

1. Smith, D. F. and Phillips, J., Eds. (2000). Chapter 1: Food policy and regulation: a multiplicity of actors and experts. In *Food, Science, Policy and Regulation in the Twentieth Century*. Routledge, New York, pp. 1–16.
2. Kastner, J. and Ackleson, J. (2006). Chapter 6: Global trade and food security: perspectives for the twenty-first century. In *Homeland Security: Protecting America's Targets*, J. J. F. Forest, Ed. Praeger Security International, Westport, CT, London, pp. 98–116.
3. Knight, C., Stanley, R., and Jones, L. (2002). *Agriculture in the Food Supply Chain: An Overview*. Campden & Chorleywood Food Research Association Group and the Royal Agricultural Society of England, United Kingdom.
4. U.S. Government Acc ountability Office (2005). *Food Safety: Experiences of Seven Countries in Consolidating Their Food Safety Systems (GAO-05-212)*. US Government Accountability Office, Washington, DC.
5. Robinson, R. A. U.S. Government Accountability Office (2005). *Overseeing the U.S. Food Supply: Steps Should be Taken to Reduce Overlapping Inspections and Related Activities (GAO-05-549T)*. US Government Accountability Office.

6. Cottrell, P. L. (1975). *British Overseas Investment in the Nineteenth Century*. The MacMillan Press Ltd, London.
7. Rostow, W. (1948). *British Economy of the Nineteenth Century*. Oxford University Press, Oxford.
8. Jacob, M. (2008). Management of food hazards and incidents. *World Food Regul. Rev*. **18**(3), 22–23.
9. Caswell, J. A. and Hooker, N. H. (1996). HACCP as an international trade standard. *Am. J. Agric. Econ*. **78**(3), 775–779.
10. Naditz, A. (2007). Lock out food supply threats. *Food Quality* **14**(6), 20–27.
11. Avery, W. P., Ed. (1993). Agriculture and free trade. In *World Agriculture and the GATT*, Boulder, Colorado.
12. Davis, R. G. and Bickett-Weddle, D. (2004). *Agroterrorism Awareness Agroterrorism Awareness Education (version 12)*. Iowa State University Center for Food Security and Public Health, Ames, Iowa.
13. Dvorak, G. (2003). *Definitions. Bioterrorism Awareness Education (version 12)*. Iowa State University Center for Food Security and Public Health, Ames, Iowa.
14. Kastner, J. J. and Pawsey, R. K. (2002). Harmonising sanitary measures and resolving trade disputes through the WTO-SPS framework. Part I: A case study of the US-EU hormone-treated beef dispute. *Food Control* **13**(1), 49–55.
15. Moy, G. G. (1999). Food safety and globalization of trade: a challenge to the public health sector. *World Food Regul. Rev*. **8**(9), 21.
16. Isaac, G. (2002). *Agricultural Biotechnology and Transatlantic Trade: Regulatory Barriers to GM Crops*. CABI Publishing, Oxon, UK.
17. Agence France Presse (English) (2002). *Zambia Fears Genetically Modified Food Aid [AgNet Listserve from the International Food Safety Network]*, 12 August.
18. Segenet, K., Mahuku, G., Fregene, M., Pachico, D., Johnson, N., Calvert, L., Rao, I., Buruchara, R., Amede, T., Kimani, P., Kirkby, R., Kaaria, S., Ampofo, K. (2003). Harmonizing the agricultural biotechnology debate for the benefit of African farmers. *Afr. J. Biotechnol*. **2**(11), 394–416.
19. McGregor, R. and Anderlini, J. (2007). Pig disease adds 30% to China's pork price and fuels inflation fear. *Financ. Times*, 29 May, Sects. 1, 2.
20. Dyer, G. (2007). China arrests 774 in product crackdown. *Financ. Times*, 30 October, Sect. 2.
21. Block, C. (2008). *The Food Supply Chain and China*, Frontier podcast [podcast] 2008 30 June, [cited October 16, 2008]. Available from http://frontier.k-state.edu.
22. WTO (1998). Agreement on the application of sanitary and phytosanitary measures. In *The WTO Agreement Series: Sanitary and Phytosanitary Measures*. World Trade Organization, Geneva, pp. 29–49.
23. Scott, A., Zepeda, C., Garber, L., Smith, J., Swayne, D., Rhorer, A., et al. (2006). The concept of compartmentalisation. *Rev. Sci. Tech. Off. Int. Epiz*. **25**(3), 873–879.

## FURTHER READING

Frazier, T. W. and Richardson, D. C., Eds. (1999). *Food and Agricultural Security: Guarding Against Natural Threats and Terrorist Attacks Affecting Health, National Food Supplies, and Agricultural Economies*. New York Academy of Sciences, New York.

# ECONOMIC IMPACT OF A LIVESTOCK ATTACK

AMY D. HAGERMAN, BRUCE A. MCCARL AND JIANHONG MU
*Texas A&M University, College Station, Texas*

## 1 INTRODUCTION

Livestock are a potentially vulnerable target for the introduction of animal disease-causing agents. Large events have occurred from apparently inadvertent introductions. For example:

- A 2001 UK Foot-and-Mouth Disease (FMD) outbreak led to the slaughter of 6.1 million animals [1]
- A Bovine Spongiform Encephalopathy (BSE) outbreak in the United Kingdom between 1994 and 2004 was associated with over 151 deaths [2]
- Avian Influenza (AI) outbreaks in China since 2003 have been associated with up to a 25% reduction in poultry trade and over 25 deaths [3].

Such vulnerability raises the issue of exactly how vulnerable we are and what types of pre-event action and/or planning can be done to limit risk and bolster resiliency. This article reviews a number of economic aspects related to these issues.

## 2 THE IMPORTANCE OF CONSIDERING ECONOMICS

Often, recommendations on the management of animal disease is based primarily on epidemic simulation models that minimize the time to control disease outbreaks by limiting the disease spread while treating or removing infected animals. After the 2001 UK FMD outbreak, such modeling was termed "armchair epidemiology" and was strongly criticized [4]. The reason for the criticism was the policy of contiguous herd slaughter used in addition to the slaughter of infected and dangerous contact herds, which was considered by many to be excessive since this caused unnecessary long term damage to the livestock industry. Following the outbreak, the United Kingdom exhibited a declining trend in animal agriculture [5] that indicated that some producers instead chose to scale- or shut-down operations.

Animal disease impacts extend beyond the number of dead animals. A strategy chosen solely because it quickly "stamps out" the disease may not be the strategy that minimizes the total economic impact in either the short or long run. It should be noted at this point that neither can economics alone be used to determine optimal response strategies to animal disease. Rather it is a combined approach using an integrated epidemic-economic model that should be used for this type of analysis.

Ideally, this integrated approach would be dynamic and spatial in nature, [6] taking into account both, the time it takes to control the disease and the economic implications of the control strategies chosen. Control strategy efficacy can be measured in terms of lost animals and direct costs of disease management as well as national welfare losses, short- and long-term trade losses, environmental consequences, consumer demand shifts, and local impacts in terms of average affects and the distribution of effects. The economic portion of the analysis can capture some or all of these loss categories and integrate them into a single measure used to quantify the distribution of outcomes from an animal disease outbreak in a particular region. The reason economic models have not been more extensively used in the past is the difficulty in developing a model that can quantify those impacts that extend beyond the primary livestock markets.

## 3 ECONOMIC IMPACT CATEGORIZATIONS

Economic impacts can be divided into two categories: direct and secondary. Most studies examining livestock disease have focused on direct impacts of the disease. Due to the highly integrated nature of the modern economy, consequences of agricultural contamination at any given point along the supply chain could be manifested in other sectors of the economy as well. For example in the recent foot FMD outbreak in the United Kingdom, the largest category of losses came from tourism. Such losses are termed secondary losses.

The losses that should be examined in any given epidemic-economic study will vary depending on the type of disease, species of animals impacted and the importance of those species to the economy, as well as regional and international animal disease policies.

### 3.1 Direct Losses

Direct losses accumulate to the livestock sector as a direct consequence of an animal disease attack. This category of losses has received the most attention due to the ease with which they can be quantified, particularly for the supply side. Direct losses are also of interest in establishing the cost of a particular response policy from the viewpoint of a governing agency.

***3.1.1 Lost Animals and Changes in Animal Value.*** The most obvious direct loss is the number of animals or herds that are removed from the supply chain due to the disease. This may arise from massive preventative slaughter, as in the case of FMD, or death due to the disease itself, such as with BSE. It also captures increased culling and abortion in animals for production operations, as would be the case with Rift Valley Fever.

The value of animals lost can be calculated using a schedule of market values based on pre-disease market conditions. This is often the method used in studies for calculating indemnity payments to producers from preventative slaughter. There are two issues with using this method. First, it does not recognize the role of livestock as a capital asset [1]. In particular for purebred animal producers, the value of an animal represents an investment in genetic improvements that may not be accounted for in a per pound cash market value as it would for a commercial animal. Second, producers who have animals not infected but expecting to absorb the full revenue loss from a negative price change may be tempted to claim their herd has been in direct contact with infected herds in order to collect a

higher price per unit. It is suspected that the payout schedule was set too high in the 2001 FMD outbreak, leading to slaughter levels greater than necessary for disease control [7].

Welfare slaughter is an issue that has not received much attention in the literature, but has proven to be a real issue in historical animal disease outbreaks that include quarantine zones and strict movement restrictions. These policies may prevent feed grains and premade feeds from being shipped into the restricted regions plus movement of animals to feeding or other operations. For enterprises employing confined feeding or those raising young animals previous to feeding, the amount of feed on hand and facilities to keep animals beyond normal movement times may be insufficient to allow the animals to be kept. This leads to additional slaughter, and consequently higher indemnity payment levels to producers. As discussed in previous sections, producers expecting lower prices for animals post-outbreak may volunteer animals for welfare slaughter to prevent additional price change losses.

***3.1.2 Costs of Disease Management.*** The direct costs of disease management account for the resources required for response to the disease outbreak including the cost of vaccination, slaughter, disposal, cleaning, disinfecting, and administrative costs. This would include cost for labor, equipment, and materials [8]. The market price changes will also impact the losses producers face. Prices could change as a result of the supply shift caused by slaughter of live animals, the destruction of milk, meat, and meat products ordinarily destined for the market and the time lag for operations to return to full production. Some studies have assumed prices do not change at the national level, but this would only be the case in a very small disease outbreak that does not change the aggregate national supply or affect demand.

Another cost producers absorb is the loss in quality from withholding market-ready animals from slaughter. The additional time to slaughter causes carcasses to be too large or not be at the optimal level of conditioning to achieve one of the premium grades, which leads to carcass discounts. For some diseases, in order to ship meat products out of the region where the infection occurs, carcasses must either be processed into cooked meat products to kill the disease-causing agent or be put in nonhuman consumption products such as pet food.

Carcass disposal becomes a serious issue in a disease outbreak, resulting in large-scale animal mortality or large-scale slaughter. Factors such as environmental regulations and public health impacts will also determine the disposal method hierarchy established [9] in addition to the cost per unit for disposal and the time required to dispose of all carcasses. The type of control strategy employed can also affect the carcass disposal method chosen since it will, hopefully, reduce the number of dead animals [10].

***3.1.3 Trade Losses.*** Animal disease often has significant impacts on international trade. Outbreaks in the last decade have increased the volatility in international meat markets through their effects on consumer preferences, trade patterns, and reduced aggregate supply [11]. Upon confirmation of an animal disease outbreak, restrictions are often placed on where livestock and meat products can be exported as well as what products are shipped. The extent of these damages will vary by disease and country, but in general countries experiencing an animal disease outbreak will experience immediate restricted international trade due to domestic supply changes and world demand shifts until the infected country is shown to be disease free for a predetermined amount of time. Domestic market impacts may be partially offset by imports [1].

If the disease is not carried in the meat, localized cuts in production will reduce the livestock and meat products available for export. In addition, movement restrictions in the country will prevent normal supplies from reaching the market, and export restriction shift meat normally shipped overseas to domestic supply [1].

If the disease is carried in the meat, it either must be cooked to destroy the organism or it must be removed from the meat supply chain. Avian influenza has affected the international poultry market reducing trade by at least $10 billion per annum [12]. As a result of Highly Pathogenic Avian Influenza (HPAI), Thailand lost its position as the worlds' fifth largest exporter of poultry meat and Brazil replaced China and Thailand as the world's largest supplier of frozen raw chicken products [12, 13]. Upon confirmation of BSE in the United States in 2003, more than 50 countries either completely stopped beef exports from the United States or severely restricted them resulting in beef exports at only 20% of the previous year's levels [14].

Even in the case of diseases that can be transferred to humans through the meat, markets have historically been found to recover within two years; however, the nation that experienced the outbreak may take longer to recover their share of the world market [11]. At particular risk are developing countries.

***3.1.4 Additional Direct Costs Associated with Zoonotic Diseases.*** In the case of zoonotic diseases (diseases that can be transferred to humans through direct exposure to the animals, disease transfer vectors like mosquitoes, or through meat consumption), several additional direct costs are accumulated. When humans can become infected from a disease, there are additional healthcare costs and loss in productivity resulting from sickness and death to be considered. In addition, reduced meat consumption will occur while meat recalls are in place in order to prevent infection. Examples of zoonotic diseases that have been under world scrutiny recently are BSE and Avian Influenza. In the 2003 US BSE case, negative price impacts may have been enlarged because of decreased consumer confidence in beef products, although that effect was short-lived [14].

## 3.2 Secondary Losses

Secondary losses are less easily quantified, but ignoring them in a study can lead to severe under-estimation of the total cost of the outbreak. These studies are often done separately from the integrated epidemic-economic model analysis; however, they should ideally be included in the integrated model as much as possible. In some cases, such as environmental costs and psychological costs, the estimation may have to be done separately.

***3.2.1 Related Industries.*** Disease outbreaks can have effects that extend well beyond the meat production chain [2]. While industries directly in the meat production chain will typically experience the greater loss and have consequently been the focus of disease outbreak economics literature, little work has been done to ascertain the impact on service industries linked to the meat industry. A good example is the feed industry. In countries with large concentrated animal feeding operations, such as the United States, a significant source of demand for feed grains is represented by livestock demand. Disease outbreaks leading to large-scale animal mortality will reduce the domestic demand for feed grains. In addition, movement restrictions in the quarantine zone will restrict not only the transport of livestock but the transport of feed grain supply trucks or unit trains coming into or out

of the region. These disruptions and demand shifts will be reflected in the price of feed grains. Other industries that would be impacted by a disease outbreak are transportation, veterinary service, supply industries, and rendering services [2].

*3.2.2 Local Economies.* Disease outbreaks will have the greatest per capita impact on the area where the outbreak occurs. Local producers whose premises are depopulated must wait to rebuild their operation, removing the money that would have been spent on feed, supplies, and livestock-related services at local businesses. Movement restrictions divert commercial and tourist traffic coming through the region, removing income to local businesses like gas stations, hotels and restaurants. Businesses may choose to shut down or livestock operations may opt not to repopulate, decreasing the number of jobs available to local residents. Alternatively, the process of controlling the disease may provide some increased local employment but this would be short-term only.

In the 2001, FMD outbreak 44% of the confirmed cases occurred in the county of Cumbria [15]. Farmers and businesses in the county were surveyed after the outbreak to ascertain their losses. Although 63% of farmers in the county said they would continue farming, only 46% planned to build back up to their previous level of operation. There was an estimated direct employment loss of 600 full-time jobs and an indirect employment loss of 900 jobs [15].

Depending on the area of the country impacted by the animal disease and the size of the outbreak, tourism can represent a serious source of secondary losses. Returning to the Cumbria county survey, after the 2001 UK FMD outbreak, the loss in gross tourism revenues in that county were expected to be around £400 million. Reports predicted the recovery of the county economy would largely depend on the long-term recovery of the tourism industry [15]. On a national level, tourism was the largest source of losses related to the FMD outbreak at £2.7 to £3.2 billion [1].

Page et al. [16] observed that Avian Influenza could have significant shocks on tourism and McLeod et al. [13] estimated that the 2004 AI outbreak in Vietnam led to a 1.8% decline in GDP, where a 5% decline in tourist arrivals could lead to an additional 0.4% decline in GDP [17]. Furthermore, Kuo et al. [18] found that Asian tourism demand is reduced by about 74 arrivals after an AI incident and this reduction was greater than the impact of AI on global tourism.

*3.2.3 Environmental.* There are two primary environmental impacts related to animal disease outbreaks: water and air quality. Ground water can be negatively impacted by disease carcasses being buried in areas where materials can leach from decomposing carcasses. Preventing this could restrict the amount of on-farm burial in the event of an animal disease outbreak, leading to additional spread risks by moving animals to suitable sites or delays in disposal by alternative methods. Water quality is also impacted by runoff from cleaning depopulated premises and from dumping infected milk as a result of movement restrictions. In a study of the 2001 FMD outbreak in the Netherlands, the illegal discharge of milk into sewage systems, rivers and smaller waterways led to a high to very high probability of spreading the disease to other cattle operations within 6–50 km of the dump site [19].

Air quality can be impacted when animal pyre burning or curtain burning of carcasses is employed. Curtain burning is preferred since it reduces the emissions into the air, but it is not always feasible since it requires more time and resources than pyre burning [9]. Studies in the United Kingdom, where pyre burning was used extensively at one

point in the outbreak, have examined the levels of dangerous compounds in livestock, dairy products, and eggs produced nearby. Slight increases in concentrations of dangerous compounds were found in lamb, chicken, and eggs, but these were not samples destined for the food chains. In milk, dangerous compound concentrations were within acceptable ranges. Overall, the study concluded that there is no evidence that the pyres were responsible for contaminating food produced in that region [20].

Human health has been another concern related to air quality. Pyre burning releases considerable amounts of ash and pollutants into the atmosphere that can be breathed in by carcass disposal workers and local residents. A study in Cumbria county in the United Kingdom found that levels of respiratory irritants, although elevated above normal levels from the pyres, did not exceed air quality standards or exceeded them by very little. Furthermore, the pollutants were unlikely to cause damage to all but the most sensitive individuals (e.g. asthmatics and those with weak lungs) [21].

***3.2.4 Demand.*** Consumer demand response comes from two sources in an animal disease outbreak. The first is the easier of the two to quantify, the adjustment in consumption patterns from price changes. Historically, consumers have experienced a small net loss in overall welfare although this is partially offset by lower domestic prices [1]. The second impact is substitution in consumption patterns as a result of changes in consumer confidence. How much of an impact reaches consumers depends on several factors such as industry organization, consumer demographics, and information release policies.

*3.2.4.1 Industrial Organization.* In countries with complex meat supply chains, such as the United States, Australia, and Europe, the extent to which consumers are impacted will depend on the number of bottlenecks in the supply chain and the level of vertical integration. In the United States there are a few meat-packers controlling a large portion of the livestock being processed [22]. This market power means greater pressure could be placed on producers and possibly consumers under an animal disease event. There is a greater vulnerability to that industry if one or more of those packers is forced to shut down during the outbreak or permanently remain shut. This would most likely have a greater impact on farmers than consumers.

In addition, the growing popularity of value-added or ready-to-eat meals means most of the value of the product on the grocery store shelf is from the inputs other than the raw agricultural product. This means a lessened sensitivity of prices consumers face in the grocery store due to shocks at the farm level [2]. While this could have an influence on the price change consumers face, industry organization is not likely to be a factor in consumer confidence.

*3.2.4.2 Consumer Demographics.* Considerable work has been done on the factors influencing demand for meat in the United States, Europe, and more recently Asia. In general there are differences in attitudes toward meat quality and safety, which means actual consumer response will vary on a case-by-case basis for animal disease outbreaks. Consumer response to BSE has had long-term negative effects in Europe and Japan [2]. In France, Adda [23] examined the effect of past risk exposure for beef consumers. Consumer sensitivity to food safety concerns has been heightened by past risk exposure leading to decreased demand for meat from consumers who previously consumed medium to small amounts of beef and an increased demand in those groups for high quality meat products. In the United States, responses to food safety concerns is small,

particularly in comparison to price effect sensitivity [24]. As the result of AI, there are losses of consumer confidence and losses of competitive strength of poultry meat in the meat market [25].

A limited amount of work has been done on willingness to pay by consumers for animal disease prevention activities like traceability and country of origin labeling. Willingness to pay for disease control could potentially be impacted by consumer demographics and risk perception as well. In order to guarantee the safety of poultry meat, providing the traceability label of poultry products is suggested as one of the incentives for farms and marketing firms to supply safer food [26, 27] and estimated results from the research done in China found that consumers in Beijing, on average, had stated a significant willingness to pay (WTP) for traceability of poultry products which was approximately 9-10% of the base price [28].

*3.2.4.3 Information Release Policies.* Considerable work has been done on the impact of information release policies in the event of a food safety risk. Pope [29] found transparency on the part of the government and industry, in the event of an animal disease outbreak, reduced negative consumer response in Canada after the 2003 BSE outbreak [2]. In the UK, a "food publicity index" was used to show the inward shift in consumer meat demand after the 1996 BSE outbreak was influenced by the publicity surrounding the outbreak [30]. Although AI information has relatively small impacts on meat demand, its effects would last three months and indeed decrease the demand for turkey and increase the demand for beef in the US meat market [25].

## 4 EPIDEMIC-ECONOMIC MODEL DEVELOPMENT

As stated earlier, to estimate potential economic losses of agricultural contamination from infectious animal disease spread, an integrated epidemic-economic model is needed. Epidemic simulation information is necessary to evaluate the extent of the physical damages [31, 32] and evaluate economic costs of a potential outbreak in an integrated framework. The type of economic model used will vary depending on several factors such as the geographic scope of interest (farm, region, nation, or world), economic factor of interest (employment changes, price changes, or trade changes) and the extent of damages expected from a particular disease.

Such integrated models are primarily used to predict what would happen in the event of an outbreak of a specific disease in a specific region, or to assess the sensitivity of an outbreak to various control strategies. Models should capture both, the recovery over multiple time periods from the outbreak over the period of restocking and, recovering trade relationships to the time of full recovery. Furthermore, they should capture the geographic implications of the disease in terms of spread to other regions or countries [6]. Moreover, to assess risk through both the epidemic portion of the model and the economic portion, the iterations from the epidemic portion may be run through the economic portion as statistically independent trials. This is opposed to the standard practice of running only the averages from the epidemic model through the economic model.

The stochastic parameters in the epidemic model deal with the rate of disease spread and the effectiveness of control strategies. The spread rate of an infectious disease will determine the severity of economic damages and the appropriate combination of necessary prevention and response actions. Prevention is perhaps the most desirable policy

option for livestock disease attacks. Some examples of these policies include employing antimicrobial livestock drugs and vaccination, storage and transportation facility security, and trade inspection. The purpose of prevention activities is to decrease the probabilities of intentional or unintentional agricultural contamination incidents. Response, control and recovery actions are indispensable policies in the face of agricultural sabotage. Essentially these policies are focused on minimizing damages by stopping the spread of a possibly infectious contamination and minimizing the scope of the sabotage, as well as fixing the source of the sabotage, restoring and replacing the lost livestock branches in the food supply chain, and rebuilding consumer confidence.

## 5 CONCLUSION

Thorough, in-depth studies that include the costs of animal disease and evaluate both vulnerability and the consequences of control strategies, giving implications for livestock death loss and wider economic costs, allow for a greater degree of preparation, effectiveness of response, and faster recovery. This article has given an overview of the economic impacts of an animal disease attack and the approach to appraisal thereof. We also discuss multiple areas that have received little attention.

Thorough analysis requires collaboration, drawing on expertise from epidemiology, sociology, biology, and economics. This level of collaboration is difficult, but indispensable in dealing with the necessary issues. Also key to a quality economic assessment is the integration of models and the identification of the right economic impact categories for the disease and region of interest.

## REFERENCES

1. Thompson, D., Muriel, P., Russell, D., Osborne, P., Bromley, A., Rowland, M., Creigh-Tyte, S., and Brown, C. (2002). Economic costs of the foot-and-mouth disease outbreak in the United Kingdom in 2001. *Rev. Sci. Tech. Off. Int. Epiz.* **21**(3), 675–687.
2. Pritchett, J., Thilmany, D., and Johnson, K. (2005). Animal disease economic impacts: a survey of literature and typology of research approaches. *Int. Food Agribusiness Manage. Rev.* **8**(1), 23–46.
3. World Health Organization (WHO). (2009). *Cumulative Number of Confirmed Human Cases of Avian Influenza A/(H5N1) Reported to WHO*. Available at http://www.who.int/csr/disease/avian_influenza/country/cases_table_2009_06_02/en/index.html Accessed 2009 June.
4. Kitching, R. P., Thrusfield, M. V., and Taylor, N. M. (2006). Use and abuse of mathematical models: an illustration from the 2001 foot-and-mouth disease epidemic in the United Kingdom. *Rev. Sci. Tech. Off. Int. Epiz.* **25**(1), 293–313.
5. Bai, P., Banks, H. T., Dediu, S., Govan, A. Y., Last, M., Lloyd, A. L., Nguyen, H. K., Olufsen, M. S., Rempala, G., and Slenning, B. D. (2007). Stochastic and deterministic models for agricultural production networks. *Math. Biosci. Eng.* **4**(3), 373–402.
6. Rich, K. M., and Winter-Nelson, A. (2007). An integrated epidemiological-economic analysis of foot-and-mouth disease: applications to the southern cone of South America. *Amer. J. Agr. Econ.* **89**(3), 682–397.
7. Anderson, I. (2002). *Foot and Mouth Disease 2001: Lessons to be Learned Inquiry Report. Cabinet Office, UK*. Available at http://archive.cabinetoffice.gov.uk/fmd/fmd_report/index.htm. Accessed 2008 October.

8. Schoenbaum, M. A., and Disney, W. T. (2003). Modeling alternative mitigation strategies for a hypothetical outbreak of foot and mouth disease in the United States. *Prev. Vet. Med.* **58**, 25–52.
9. Scudamore, J. M., Trevelyan, G. M., Tas, M. V., Varley, E. M., and Hickman, G. A. W. (2002). Carcass disposal: lessons from Great Britain following the foot-and-mouth disease outbreaks of 2001. *Rev. Sci. Tech. Off. Int. Epiz.* **21**(3), 775–787.
10. Jin, Y., Huang, W., and McCarl, B. A. (2005). Economics of homeland security: carcass disposal and the design of animal disease defense. *Presented at the American Agricultural Economics Association Meetings. Rhode Island*.
11. Morgan, N., and Prakash, A. (2006). International livestock markets and the impact of animal disease. *Rev. sci. tech. Off. int. Epizoot.* **25**(2), 517–528.
12. Nicita, A. (2008). *Avian Influenza and the Poultry Trade*. World Bank, Policy Research Working Paper 4551.
13. McLeod, A., Morgan N., Prakash A., and Hinrichs J. (2005). *Economic and social impacts of avian influenza*. FAO Emergency Centre for Transboundary Animal Diseases Operations (ECTAD).
14. Hu, R., and Jin, Y. (2009). *The impact of North American BSE events on the US beef market: consequences of trade disruptions*. Working Paper.
15. Bennett, K., Carroll, T., Lowe, P., and Phillipson, J. (2002). *Coping with Crisis in Cumbria: Consequences of Foot-and-mouth Disease*. Center for Rural Economy, Newcastle University, Newcastle upon Tyne, United Kingdom.
16. Page, S., Yeoman, I., Munro, C., Connell, J., and Walker, L. (2006). A case study of best practice -Visit Scotland's prepared response to an influenza pandemic. *Tourism Manage.* **27**(3), 361–393.
17. Brahmbhatt, M. (2005). *Avian Influenza: Economic and Social Impact*. Available at http://go.worldbank.org/YELWWUIAY0. Accessed 2005 Oct.
18. Kuo, H. I., Chang, C. L., Huang, B. W., Chen, C. C., and McAleer, M. (2009). *Avian Flu and International Tourism Demand: A Panel Data Analysis*. Available at http://mssanz.org.au. Accessed June.
19. Schijven, J., Rijs, G. B. J., and de Roda Husman, A. M. (2005). Quantitative risk assessment of FMD virus transmission via water. *Risk Anal.* **25**(1), 13–21.
20. Rose, M., Harrison, N., Greaves, A., Dowding, A., Runacres, S., Gem, M., Fernandes, A., White, S., Duff, M., Costley, C., Leon, I., Petch, R. S., Holland, J., and Chapman, A. (2005). Dioxins and polychlorinated biphenyls (PCDD/Fs and PCBs) in food from farms close to foot-and-mouth-disease animal pyres. *J. Environ. Monit.* **7**, 378–383.
21. Lowles, I., Hill, R., Auld, V., Stewart, H., and Calhoun, C. (2002). Monitoring the pollution from a pyre used to destroy animal carcasses during the outbreak of foot-and-mouth disease in Cumbria, United Kingdom. *Atmos. Environ.* **36**(17), 2901–2905.
22. Love, H. A., and Burton, D. M. (1999). A strategic rationale for captive supplies. *J. Agric. Resour. Econ.* **24**(1), 1–18.
23. Adda, J. (2007). Behavior towards health risks: an empirical study using the "mad cow" crisis as an experiment. *J. Risk Uncertain.* **35**, 285–305.
24. Piggott, N. E., and Marsh, T. L. (2004). Does food safety information impact US meat demand? *Am. J. Agric. Econ.* **86**(1), 154–174.
25. Mu, J., Bessler, D., and McCarl, B. A. (2009). Avian influenza information: economic effects on U.S. meat markets. *Selected poster presentation at the March 2009 Department of Homeland Security Annual University Summitt. Washington, DC*.
26. Pouliot, S., and Sumner, D. (2008). Traceability, liability, and incentives for food safety and quality. *Am. J. Agric. Econ.* **90**, 15–27.

27. Brouwer, R., van Beukering, P., and Sultanian, E. (2008). The impact of the bird flu on public willingness to pay for the protection of migratory birds. *Ecol. Econ.* **64**, 575–585.
28. Jin, Y., and Mu, J. (2009). *Elicitation Effects of Using Payment Cards on Consumer Willingness to Pay*. Working paper.
29. Pope, C. (2003). Managing consumer confidence. *Presentation in the symposia the Economic Impact of Animal Disease on the Food Marketing Sector. Denver, CO*, July 11.
30. Loyd, T., McCorriston, S., Morgan, C. W., and Rayner, A. J. (2001). The impact of food scares on price adjustments in the UK beef market. *Agric. Econ.* **25**, 347–357.
31. Jalvingh, A. W., Nielen, M., Maurice, H., Stegeman, A. J., Elbers, A. R. W., and Dijkhuizen, A. A. (1999). Spatial and stochastic simulation to evaluate the impact of events and control measures on the 1997–1998 classical swine fever epidemic in The Netherlands. *Prev. Vet. Med.* **42**, 271–295.
32. Ferguson, N. M., Donnelly, C. A., and Anderson, R. M. (2001). The foot-and-mouth epidemic in great britain: pattern of spread and impact of interventions. *Science* **292**, 1155–1160.

## FURTHER READING

Agra CEAS Consulting Ltd. *Prevention and control of animal diseases worldwide: economic analysis--prevention versus outbreak costs. The World Organisation for Animal Health (OIE) Final Report, Part I*.

Burns, A., van der Mensbrugghe, D., and Timmer, H. (2009). *Evaluating the Economic Consequences of Avian Influenza*. Available at http://siteresources.worldbank.org/EXTAVIANFLU/Resources/EvaluatingAHIeconomics_2008.pdf. Accessed 2006 Jun.

Rich, K. M., Miller, G. Y., and Winter-Nelson, A. (2005). A review of economic tools for the assessment of animal disease outbreaks. *Rev. Sci. Tech. Off. Int. Epiz.* **24**(3), 833–845.

# SOCIAL, PSYCHOLOGICAL, AND COMMUNICATION IMPACTS OF AN AGROTERRORISM ATTACK

STEVEN M. BECKER

*University of Alabama at Birmingham School of Public Health, Birmingham, Alabama*

## 1 INTRODUCTION

As policy makers, the agriculture sector, researchers, emergency planners, and communities prepare to meet the enormous challenge posed by agroterrorism, increasing attention

has been devoted to such critical issues as field and laboratory detection, surveillance, mapping, improved outbreak modeling, vaccine development and improvement, and disposal and decontamination options. Far less consideration, however, has been given to social, psychological, and communication issues. Yet, the manner in which these issues are approached will be one of the principal determinants of an agroterrorism event's outcome. The ultimate aim of an agroterrorism attack, after all, is not to harm crops or ruin agricultural products; rather, it is to destroy confidence in the food supply and in societal institutions, create fear and a sense of vulnerability in the population, reduce people's hope and resolve, and weaken the society and the nation. Effectively addressing key social, psychological, and communication issues will be crucial to the success of quarantines or other mitigation measures, and to efforts to minimize exposure to threat agents, reduce the impacts of an incident, maintain public confidence and trust, and better assist affected individuals, families, and communities [1]. It is no exaggeration, therefore, to say that social, psychological, and communication issues constitute "make or break" factors in any effort to manage an agroterrorism event. Without sufficient attention devoted to these issues, "response efforts after a terrorist attack might be successful in narrowly technical terms but a failure in the broader sense. In effect, the battle might be 'won,' but the war would be lost" [2, p. 16].

## 2 LEARNING FROM THE 2001 FOOT-AND-MOUTH DISEASE OUTBREAK

Among the best ways to understand the nature and extent of the social, psychological, and communication challenges that an agroterrorism attack could pose is to learn from recent experience with large-scale disease outbreaks. In this regard, the 2001 foot-and-mouth disease outbreak in the United Kingdom is probably the most instructive. Although the 2001 outbreak was not the result of terrorism, it "presented unprecedented challenges which no one in any country had anticipated" [3, p. 6]. This included a host of serious social, psychological, and communication impacts. In addition, because of the open, forthright and thorough way that British society has examined the successes and failures in the handling of the epidemic, others have a rich opportunity to learn from this experience.

Foot-and-mouth disease is a viral disease that mainly affects cattle, pigs, goats, and sheep. Its symptoms include fever, vesicles (blisters) in the mouth or on the feet, pain, lameness, loss of appetite, and loss of condition [4]. The virus can survive for long periods of time and is powerfully contagious. Indeed, foot-and-mouth disease has variously been described as "the most contagious of all diseases of farm animals" [5, p. 2], "the most feared infection of domestic livestock" [6, p. 1], and "the most contagious disease of mammals" [7, p. 425]. Not only can animals be infective without displaying signs of the disease, the virus can also be transmitted in a host of ways. "The virus is present in fluid from blisters, and can also occur in saliva, exhaled air, milk, urine and dung. Animals pick up the virus by direct or indirect contact with an infected animal. Indirect contact includes eating infected products and contact with other animals, items or people contaminated with the virus, such as vehicles, equipment, fodder and anyone involved with livestock." [8, p. 13]

The rapidity with which the 2001 epidemic spread was astonishing. British officials estimate that by the time the virus was confirmed on February 20, some 57 farms in 16 counties had already been infected. By February 23, when a movement ban was imposed, 62 more premises were thought to have been infected, involving seven more counties

[8, p. 14]. In addition, the scale of the outbreak was remarkable. At the height of the crisis, "more than 10,000 vets, soldiers, field and support staff, assisted by thousands more working for contractors, were engaged in fighting the disease. Up to 100,000 animals were slaughtered and disposed of each day" [8, p. 1].

By the time the outbreak ended—221 days after it began—the toll was enormous: animals were slaughtered at more than 10,000 farms and related agricultural premises in England, Scotland, and Wales. Approximately 2000 locations were "slaughtered out" because foot-and-mouth disease had been confirmed there, while another 8000 were targeted either because they neighbored an infected farm ("contiguous culling") or because it was suspected that animals could have been exposed to the virus ("dangerous contacts"). While efforts were made to reduce pain and suffering, there were all too many situations where this aim was not achieved due to the scale of the operation and a shortage of trained personnel. Reports of frightened animals taking flight, animals being wounded, or animals being shot multiple times were not uncommon. Piles of dead animals awaiting disposal were a regular sight in affected areas, particularly in the early days of the culling operation; so, too, were trenches where carcasses were buried and "funeral pyres" where carcasses were burned. In the end, the total number of animals slaughtered for disease control purposes was staggering—over 4.2 million. Beyond that, 2.3 million other animals were slaughtered under "welfare provisions" because strict movement restrictions in affected regions made it impossible to get feed to them.

People living in the midst of the epidemic and associated carnage were hit hard emotionally, as when farms that had been in the family for generations were wiped out or when children's pets were required to be slaughtered. In addition, people were battered economically. Agricultural communities, including farmers and their families, people employed in agriculture, and area businesses, saw livelihoods and financial security disappear virtually overnight. Tourism—a vital industry in many of the affected areas—dropped precipitously, causing even greater economic damage and dislocation. Before the outbreak finished, it had even gone international, spreading to a limited extent to France, the Netherlands, Northern Ireland, and the Republic of Ireland [3, 8].

It is common in most disaster situations for people's responses and reactions to be marked by resilience and helping behaviors. The foot-and-mouth epidemic was no exception. Many communities remained united in the face of the invisible threat and there were countless acts of assistance and support. Amongst farmers and farming families, there was a continuing commitment to agriculture as a way of life despite the tremendous difficulties caused by foot-and-mouth disease [9]. In addition, many veterinarians and other professionals endured difficult conditions and went above and beyond the call of duty to help bring the outbreak under control. Finally, there were many examples of public sympathy and support for affected farmers and farming communities. People in the Southwest and other parts of the United Kingdom, for example, participated in a huge fund-raising effort aimed at helping those whose livelihoods had been ravaged by the epidemic. The Green Wellie Appeal, launched in March by the Western Morning News, saw participation from celebrities, businesses, schools, and thousands of people sympathetic to the plight of affected farmers. More than £1 million was raised [10].

At the same time, the outbreak also caused new strains, sharp conflict and division, profound distress, widespread loss of trust, and a host of other serious social, psychological, and communication impacts. These were partly a result of the damage wrought by the outbreak itself, but they were also compounded by serious shortcomings in preparedness and response efforts. Initially, "no-one in command understood in sufficient detail what

was happening on the ground." By the time the extent of the problem was fully grasped, a cascade of social, psychological, and communication effects had already begun. "A sense of panic appeared, communications became erratic and orderly processes started to break down. Decision making became haphazard and messy . . . . The loss of public confidence and the media's need for a story started to drive the agenda" [3, p. 6].

While no two events are ever alike, the range of individual, family, community, and societal effects experienced during foot and mouth provides a clear indication of the kinds of social, psychological, and communication impacts that could result from a large-scale agroterrorism attack. Some of the most significant effects evidenced during the 2001 outbreak are reviewed below.

## 3 SOCIAL, PSYCHOLOGICAL, AND COMMUNICATION IMPACTS

### 3.1 Isolation

Efforts to control the spread of the virus had the unintended consequence of causing widespread social isolation. A ban on animal movements, the creation of large exclusion zones around affected farms, the posting of "keep out" signs, the placing of disinfectant baths and mats, the closure of footpaths, parks, tourist attractions and heritage sites, prohibitions against all nonessential travel, and the closure of widespread areas of the countryside often combined to bring community life to a standstill. Farmer's markets, fairs, art shows, and other events were cancelled, and many other facets of social life—visiting neighbors, going to the pub, attending religious services, shopping, participating in clubs and community groups—ceased. Even the utilization and delivery of health and social services were affected. In the words of one official report, "children and families could not conduct normal lives . . . ." [11, p. 9]. Thus, at a time of maximum difficulty and stress, people were often cut off from normal social outlets, from each other, and from their community support networks.

### 3.2 A Sense of Being under Siege

Even where some degree of movement or interaction was possible, fear that other people could potentially spread the virus caused many farmers, farming families, and others to barricade themselves off from the outside world. The farthest that one could safely venture was to the end of his or her property. Children were even kept home from school for an extended period of time.

The sense of being on edge and under siege was reinforced every time there was an instance of someone ignoring warning signs or violating a closure order. Such occurrences appeared to happen at a variety of times and in a multiplicity of locations [12]. Reported problems included walkers pulling down disease-warning signs, people entering closed areas/footpaths, and people crossing farm property. A spokesperson for one police department was quoted as saying that numerous complaints had been received alleging that "people are either ignoring the signs or ripping them down. On one occasion a man walking his dog ripped a sign down and went straight down the path. Another time, a man led a child on horseback down a path" [13, p. 33]. In some instances, there were direct conflicts when farming families trying to protect their property from the virus encountered outsiders. Among the incidents described in media reports were one where

a farmer's wife confronted cyclists with a shotgun, and another where a farmer was attacked by two men walking a dog after he asked them to leave his farmland [13].

### 3.3 Hoaxes and Threats

Compounding the fear, uncertainty, and distress experienced by farming communities were hoaxes and threats perpetrated in the wake of the outbreak. In one case, for example, a farmer reported having found a pig's head that had apparently been thrown into the middle of his field of dairy cows. In another case, a vial and bloodstained gloves were left near a sensitive area of a farm. The overall number of such incidents was relatively small; but in the context of the enormous worries and uncertainties already being experienced by much of the countryside, even this small number was sufficient to add greatly to people's fears and sense of being under siege [12].

### 3.4 Noncompliance with Infection Control Measures

Adherence to measures aimed at controlling the spread of infection is a key to crisis management during a large-scale outbreak. During the foot-and-mouth disease outbreak, cooperation and compliance were often good. However, many exceptions were seen over the course of the outbreak. At times, and in some areas, the lack of compliance occurred often enough and was sufficiently serious to constitute a major concern. Compliance problems, which were identified in relation to both farms and transport, included unlicensed movement of animals, dirty vehicles, and vehicles spilling organic material onto roads. Some of these problems might have stemmed from lack of awareness, lack of training, unclear instructions, or ineffective communication. There is evidence, for example, that words such as biosecurity, blue box, and red box were not always well understood. But other problems—including the deliberate alteration of movement licenses and illegal entry to infected premises—were clearly intentional violations of infection control measures. In a number of cases, violators were fined or prosecuted if they were caught [12].

### 3.5 Conflict within Communities

Differences between those involved in agriculture and those dependent on tourism, changes and perceived inconsistencies in valuation and compensation levels, and divergent views on approaches to dealing with the crisis sometimes created new tensions and sharp conflicts. These conflicts divided neighbors and friends and had broader impacts as well. As a member of one farming family explained, the situation was damaging "not just the farming lifestyle, but the farming communities, the farming relationship" (Quoted in [14], p. 274). One of the most powerful descriptions of the combined effect of isolation, the state of siege, and splits between people was given by a resident of Holne at the Devon Foot and Mouth Inquiry (2002, p. 58):

> Divisions occurred within people and between different groups—"us and them." The "us" became narrower and smaller—only the immediate family. Thus psychological isolation exacerbated physical isolation. People withdrew from the nurturing of the community. The dangerous "not us" became wider and bigger: farmers, walkers; MAFF/DEFRA; those with no bio-security and those with excellent bio-security; those who left, those who remained; organic farmers, postmen, people with dogs; horse drivers and horse riders; children at

school and not; open pubs and closed pubs; those compensated and those not; those who cheated and those who played straight. Suspicion, guilt, panic, fear and abandonment were all apparent. What is left is lack of confidence, depression, lack of ability to respond, and despair.

### 3.6 Psychological Impacts

As the Royal Society of Edinburgh [11, p. 9] summed up, "for those involved, or even those not involved but living in the locality, there was trauma . . . . For many of these people, and perhaps especially their children, the events of 2001 were a nightmare . . . " Only a relatively small number of systematic studies of the outbreak's psychological impact were conducted, perhaps in part because of the difficulties inherent in a situation involving severe travel restrictions. But the research that was conducted has reinforced the conclusion that this was a highly distressing experience. In a study carried out shortly after the official end of the outbreak, Peck et al. [15] compared psychological morbidity in a badly affected area (Cumbria) and an unaffected area (the Highlands) using a 12-item version of the General Health Questionnaire that was mailed to farmers. Though small sample size limits how far the results can be generalized, the study found that farmers in the affected area had significantly higher levels of psychological morbidity than those in the unaffected area.

Other research (e.g. [16]) carried out in various locations and using a variety of methodologies has also examined emotional well-being and mental health in relation to the outbreak. Olff et al. [17] studied farmers whose animals were slaughtered during the outbreak and found that approximately half had high levels of traumatic stress symptoms. Deaville et al. [18] carried out a health impact assessment of the foot-and-mouth outbreak in Wales. Using a multimethod approach that combined validated quantitative instruments with qualitative interviews, the assessment found significant mental health effects in the study sample and identified such symptoms as sleeplessness, tearfulness, frustration, anger, and lack of motivation. Hannay and Jones [19] used a mail survey to examine how farmers and tourism workers in Dumfries and Galloway, Scotland were affected by the outbreak. The results indicated that both groups had experienced negative impacts in the areas of daily activities, feelings, overall health, social activities, social support, and quality of life [20]. Finally, Mort et al. [21] conducted a longitudinal qualitative analysis of weekly diaries and concluded that the foot-and-mouth experience was accompanied by distress, feelings of bereavement, fear of a new disaster, and loss of trust.

Looking across the psychological impacts of the outbreak, Peck [20] concluded that, despite the high levels of distress, there had been no increase in demand for mental health services in affected areas. Rather, farmers turned to "family, friends and veterinary surgeons for support" (p. 272). In addition, noted Peck, there was "an expressed willingness to use anonymized sources of support, such as telephone or internet helplines" (p. 275). This is fully consistent with reports from the many organizations that provided support to farmers, farming families, and others in affected communities. Crisis hotlines and stress helplines were flooded with calls, so that hours had to be extended and staffing had to be increased. The Rural Stress Information Network, for example, reported that with the onset of the outbreak, it had received more calls in a single month than in the entire preceding year [12].

No direct, systematic studies of the outbreak's effect on children—generally considered a vulnerable population—were carried out [22]. Nevertheless, it was apparent that the situation took a significant emotional toll on them. Children were often nearby when

parents' and grandparents' farms were slaughtered out. They witnessed piles of dead animals, saw and smelled the funeral pyres that burned for days, and sometimes even lost their own pets as a consequence of the crisis. In addition, children shared in the isolation that affected farm communities. They missed school for extended periods of time, were unable to socialize with friends, and saw their families' own distress on a daily basis. As one parent told the Devon Foot and Mouth Inquiry, "my children had never seen me cry before" [23, p. 50].

Children's stress manifested itself in many ways, from angry e-mail postings [24] to problems with bed-wetting. As one rural nurse wrote, "as time passed we had an increase in referrals for children who were bed-wetting, often after long periods of being dry" [25, p. 60]. In a health assessment carried out in Wales by Deaville et al. [18], over half of the study's respondents indicated that the outbreak had affected their children.

Although most attention has focused on farmers and their families, it should also be borne in mind that foot-and-mouth was often a distressing experience for those charged with fighting the outbreak. Professionals on the front lines worked very long hours, were often away from home, and regularly witnessed horrific sights. Furthermore, although some frontline personnel felt that their work was supported by farmers, community residents, and the broader public, this was often not the case. Indeed, because of the high level of controversy, anger, frustration, and mistrust surrounding almost every aspect of foot-and-mouth, it was not uncommon for frontline staff to find themselves the target of relentless hostility and derision. Some professionals even reported that they were ashamed to be identified as government agency staff members. This state of affairs undoubtedly made an already emotionally taxing situation even more difficult for some frontline workers.

### 3.7 An Overwhelming Demand for Information

Just as the crisis developed with breathtaking rapidity, so too did the demand for information. Requests for information quickly exceeded all expectations, and communication resources and personnel were severely stretched. For example, during the early part of the outbreak, staff at the Carlisle Disease Emergency Control Centre found themselves having to field some 6500 calls per week even as they worked feverishly to deal with the outbreak. On the national level, the resources of a helpline at the headquarters of the Ministry of Agriculture, Fisheries and Food were quickly exceeded, as were those of a much larger governmental foot-and-mouth disease helpline that had been set up utilizing a call center at the British Cattle Movement Service. As a result, officials established an overflow service through a private contractor. By March–April, the national foot-and-mouth disease helpline was hitting 7000 calls per day. Over the course of the 31-week outbreak, government-sponsored helplines responded to literally hundreds of thousands of calls from farmers and the general public [8]; [12].

Aside from the overwhelming numbers of calls, one of the biggest challenges affecting the helpline effort was the difficulty those operating it had in obtaining information that was sufficiently detailed, accurate, and up-to-date. Helpline staff often had to rely on the website operated by the Ministry of Agriculture, Fisheries and Food. Although the Ministry had succeeded in quickly establishing the website after the outbreak began, and although it was widely used (by March–April it was seeing an average of 50,000 user sessions per day), the site did not always contain the most recent information [26, p. 321; 8; 12]. Particularly in situations where other sites were more up-to-date, this added to confusion and suspicion.

Poortinga et al. [27] carried out a multimethod study of how people ($n = 473$) in two communities—one potentially at risk from foot-and-mouth and another not close to any cases—viewed the trustworthiness of various sources of information about the outbreak. Among those scoring lowest on trust were government ministers and food manufacturers. The media fell exactly in the middle of the list (number 7 out of 13 information sources), perhaps because of concerns about sensationalism and exaggeration. Who, then, were seen as the most trustworthy sources of information? Topping the list were veterinary surgeons, followed by farmers, and then friends and family. In other words, people often trusted animal health professionals and *local* sources (e.g. word of mouth, the grapevine) far more than the national media and the national government. The crisis also saw the emergence of new "virtual" communities and networks that were able to link people despite the isolation created by the outbreak [28].

### 3.8 Conflict over Control Measures

Efforts to dispose of the huge number of slaughtered animal carcasses encountered significant community opposition. In part, this was due to a lack of consultation with stakeholders. "The speed with which decisions were taken, from site selection to construction and use, meant that there was little time for consultation . . . . The lack of consultation angered local communities . . . the lack of information and perceived insensitivity to local concerns aggravated the situation" [3, p. 114].

One major focus of opposition was the so-called funeral pyres (fires) that were extensively used in affected areas. Concerns included smoke contamination, dioxins, the powerful stench, and the problem of ash removal. In one locale, protests by business people and other residents forced officials to substantially reduce the size of a major burning operation. In another location, families blockaded trucks carrying carcasses to a funeral pyre. In yet another area, residents blocked trucks from entering a pyre site [12].

Plans for burial of carcasses also provoked anger and protest. People's concerns included possible transport leakage, seepage of leachate, and contamination of watercourses and drinking water supplies. Near one proposed site, for example, several hundred people from three villages came together to oppose burial plans. Although the vast majority of protests against burial sites were peaceful, there were isolated exceptions. In one situation, for example, earth-moving equipment was used to crush a police van after protesters attempted to stop plans for mass burial of animal carcasses [12].

At times, opposition and protest were local in nature. But at other times, the issue of what to do with the carcasses of dead animals pitted region against region. In one area, for example, hundreds of people marched to protest plans to bring dead sheep from other areas of Britain to their county for burial [12]. In such situations, there was a powerful sense that people were being asked to shoulder more than their fair share of the burden. As Bush et al. [29] commented, "in the final analysis, local hostility to the burial sites was not only about the shortcomings of consultation and the failure to take seriously local knowledge, or the doubts about possible risks to either human health or the local environment. It was equally about the injustice of being singled out as a local repository for the by-product" of a national disaster.

### 3.9 A Breakdown of Trust and Confidence

Despite dedication and hard work from many civil servants, disease control professionals, and frontline staff, strategic problems such as a slow recognition of the severity of the

outbreak, a slow early response, controversy over the mass slaughter policy, perceived inconsistencies in compensation procedures, conflict over carcass disposal, and a lack of adequate consultation with stakeholders, all contributed to a loss of faith in the overall handling of the situation. Communication problems further damaged public confidence [26]. In the end, the foot-and-mouth disease crisis resulted in a "breakdown of trust between many of those affected directly or indirectly and their Government" [3, p. 7].

## 4 IMPLICATIONS FOR AGROTERRORISM PREPAREDNESS AND RESPONSE

The 2001 foot-and-mouth disease outbreak in the United Kingdom—while not a terrorist event—provides a clear indication of the types of social, psychological, and communication impacts that could occur as a consequence of a large-scale agroterrorism attack. The spectrum of effects ranges from the distress suffered by individual farming families who see their life's work disappear overnight to broad social impacts such as community division, regional conflict, and loss of trust. Furthermore, as the 2001 experience makes clear, these impacts may be profound and widespread. Indeed, there is a real potential for the severity of social, psychological, and communication impacts of an agroterrorism attack to be even greater than what was seen during the foot-and-mouth epidemic. For example, an event involving a zoonotic agent would present an additional layer of challenges. Likewise, the possibility of multiple or repeated attacks could make it vastly more difficult to reestablish people's sense of security.

It will be crucial to learn from the foot-and-mouth outbreak and other experiences and incorporate these insights into agroterrorism contingency planning, training, preparedness, and response. Some of the key lessons that relate to social, psychological, and communication issues are discussed in the following sections.

### 4.1 Enlist the Public as a Partner

Although some level of disagreement and conflict is probably inevitable in a situation like the foot-and-mouth outbreak, it is now generally accepted that the situation was made far worse because of a lack of consultation with communities during the crisis. However, the problem ran deeper; even *before* the outbreak, there was failure to adequately engage stakeholders—including communities—in the emergency planning process. For example, stakeholders were "not formally consulted in preparing contingency plans" [8, p. 40]. Today, foot-and-mouth preparedness planners in the United Kingdom employ a much more inclusive, participatory approach.

Nearly every aspect of managing an agroterrorism event will depend upon gaining the cooperation and confidence of agricultural communities and the broader public. Thus, it is essential for agroterrorism planning and preparedness efforts to view them as full-fledged partners. Stakeholders need to be involved in plan development long before an event occurs [30], and their participation in training exercises is vital. Similarly, the development of emergency information and outreach strategies cannot possibly be fully effective without community input and feedback. More broadly, there is a need to engage agricultural communities and the public in discussions about the agroterrorism threat long before an event occurs. This will permit full consideration of different management strategies, disposal options, compensation issues, and other potentially controversial matters, and

facilitate the development of participatory decision-making processes that are seen as fair, transparent, credible, and effective.

### 4.2 Adequate Resources and Preparation for Information Hotlines

It is clear from the foot-and-mouth experience that, in the event of an agroterrorism attack, the demand for information from official hotlines will be massive. If public confidence is to be maintained, agencies will need to have well-rehearsed plans, phone facilities, and trained personnel to rapidly set up and operate such hotlines. Hotline arrangements—including mechanisms to ensure that accurate and up-to-date information is available—should be regularly and realistically tested through exercises. Depending on the nature of an agroterrorism event, there may also be substantial information demands from veterinarians, county extension agents, health departments, doctors, and others involved in responding to the situation. Thus, agencies will also need to be able to rapidly provide special hotlines and appropriate informational materials tailored to meet the needs of professionals.

### 4.3 Adoption of a Pre-Event Message Development Approach

An agroterrorism event and its resulting impacts could unfold with great speed, leaving agencies little or no time to develop effective communication strategies, informational materials, and emergency messages. In such a situation, events could easily outstrip communication efforts, leaving information vacuums that could quickly be filled with misinformation and rumors. This, in turn, could greatly complicate efforts to control an outbreak and contribute to the erosion of trust and confidence.

One promising solution that has broken new ground is to adopt what has come to be known as the "pre-event message development" approach. In a nutshell, the idea is to carry out research on the concerns, information needs, and preferred information sources of key audiences; utilize the findings to prepare emergency messages and other materials; and carefully test them long before an event occurs [31–33].

Interest in this approach developed out of the experience of the Centers for Disease Control and Prevention (CDC) during the 2001 anthrax letter incidents. With concern about the incidents growing rapidly, CDC found itself having to field large numbers of calls from the public, requests by health officials for real-time information, and inquiries from the media. With events moving quickly and with staff already stretched assessing and managing the incidents, it became difficult to keep up with the demand for information.

Reflecting on the experience, CDC later concluded that efforts to manage future emergencies would benefit from the use of a more proactive approach wherever possible. The agency enlisted the assistance of four US schools of public health, which carried out a multiyear, multisite research program to (i) understand the perceptions, information needs, self-protection concerns, preferred information outlets, and trusted sources for a range of population groups; (ii) identify core content for emergency messages; and (iii) pre-test draft message components (including the identification of confusing terms). CDC is now using these findings to craft more effective emergency messages, materials, and web content related to the human health aspects of unconventional terrorism agents.

The communication challenges associated with an agroterrorism event would be immense. So too would the stakes. Should public trust and confidence be lost, they will

be difficult to regain. The "pre-event" approach is not easy. It requires investment in research and a commitment to translate that research into practice. However, adoption of a "pre-event" approach increases the chances that agencies can stay "ahead of the curve" rather than falling hopelessly behind. Rather than starting from scratch and guessing what information key stakeholders and the general public want, the use of a "pre-event" approach enables agencies to build on an empirically grounded foundation. "During an actual emergency, the focus of attention can be on developing incident specific information" that can quickly be incorporated into already tested materials [31].

### 4.4 A Broader Approach to Communication

Clearly, a vital part of any effective communication strategy during an agroterrorism event will involve working closely with the news media to get needed information out to the public. As practical experience and the literature on risk communication have shown, this means having the infrastructure and trained personnel to rapidly respond to media requests for information; being able to provide experienced, credible, well-informed spokespersons for interviews; being able to provide opportunities for visuals; and having press kits with relevant statistics and succinct and clear resource materials available. In addition, an effective communication strategy also requires reaching out to different types of media, including television, radio, and newspapers [34].

However, as important as the media component of a communication strategy may be, it is essential to remember that some population segments may not be reached through the media or may prefer or trust other sources of information. As noted earlier, during the 2001 foot-and-mouth disease outbreak in the United Kingdom, it was not uncommon for people to give more credence to trusted local sources, word of mouth, and the "grapevine" than to the national media or national government. This is consistent with some recent research on bioterrorism issues suggesting that, in some situations, there could be urban–rural differences in terms of preferred information sources. For example, one recent study noted that, whereas urban respondents reported looking to the media first for information, rural respondents reported looking first to local authorities [35].

In light of these findings, it is critical for an agroterrorism communication strategy to complement the mass media component with a carefully thought-out community outreach component. This should include steps to ensure that accurate, up-to-date information is rapidly and continuously provided directly to trusted local figures (e.g. county extension agents and veterinarians) and trusted community organizations and networks (e.g. farming organizations, houses of worship). The extensive involvement of stakeholders well before an event should greatly facilitate the identification of community networks that may be important for such outreach efforts.

During the foot-and-mouth outbreak, parts of the farming community (particularly younger farmers and their families) also made extensive use of information technology. In an agroterrorism situation, it will be important to ensure that informational websites are easily found, user friendly, written in clear language, informed by an understanding of people's concerns, and regularly updated with the latest information.

### 4.5 Ability to Rapidly Expand Crisis Hotlines and Peer/Social Support

As noted earlier, many people having to cope with the impacts of the foot-and-mouth outbreak turned to crisis hotlines and stress helplines. With an agroterrorism attack likely

to produce widespread emotional distress, it will be vital for emergency response plans to include mechanisms for rapidly expanding crisis/stress hotline services. Facilities, needed equipment and resources, and trained personnel should be identified in advance, as should ways of communicating the availability of the services. In addition, strategies for facilitating peer/social support should be included in planning. For example, mental health professionals can play "an educational and consultative role for veterinary surgeons, farming organizations, self-help groups ... and local radio" [20, p. 275].

### 4.6 Special Services and Materials for Children

In any disaster situation, children have unique vulnerabilities. They may be exposed to the same frightening sights, sounds, and smells as adults, but not have the maturity or experience to interpret and understand what is going on around them. Although children are often resilient, there is no doubt that an agroterrorism event would be a highly distressing situation for them. It is important, therefore, for agroterrorism preparedness planning to include appropriate mental health support and interventions for children. This should include a particular focus on schools and day-care settings. "Children spend the majority of their waking hours at school or in a child-care setting. These settings are familiar and comfortable to children, and generally are experienced as safe, secure environments. As such, school and child-care settings are excellent locations for working with children before, during, and after a disaster" [22, p. 24]. In addition, it will be important to develop age-appropriate informational materials, explanations, coloring books, and messages to help children and families understand and cope with the situation [22].

### 4.7 Support for Frontline Personnel

As the foot-and-mouth epidemic demonstrated, the job of managing a large-scale outbreak can put frontline personnel under enormous strain. Likewise, during an agroterrorism event, long work hours, fatigue, extended periods of time away from home and family, the risk of injury, regular exposure to upsetting images, the uncertainty of the situation, and perhaps even public hostility could put frontline personnel at significantly increased risk for emotional distress. Agroterrorism planning, therefore, should include a robust mental health component aimed at supporting frontline personnel. This should include such measures as predeployment briefings, provision of self-care and stress management information, regular rest breaks, buddy/peer support arrangements, and support groups.

### 4.8 Human Health Issues

To the extent that human health concerns arise in relation to a suspected or actual agroterrorism attack (e.g. when zoonotic agents are involved or simply when rumors of possible human health effects gain prominence), it will be essential for agencies and spokespersons with a high level of credibility on health issues to be at the center of public communication efforts. Research on terrorism situations involving unconventional agents (including biological threats) has shown that many of people's concerns, and many of the questions they want answered, relate directly or indirectly to health [32, 35–37].

In addition, other research on terrorism in general has demonstrated that when people are asked who they would trust to "give accurate and reliable information about what is happening and what to do in the event of a terrorist attack," it was the professionals and organizations knowledgeable about health and health care that were ranked the highest [38]. The CDC was ranked the highest, with 84% of the population indicating it would

either "completely trust" or "somewhat trust" the agency to provide accurate and reliable information. Others on the list included "Doctor who is expert" (83%), the Surgeon General (76%), and the National Institutes of Health (75%). Figures such as the Secretary of Homeland Security and the Attorney General ranked much lower (68% and 65% respectively).

The lesson is clear. If human health issues are involved in an agroterrorism event, communication with the general public needs to put health issues at the center, messages need to be "front-loaded" with information that answers people's health questions, and the information should be provided by spokespersons recognized for having high credibility on health issues (e.g. the CDC).

### 4.9 More Realistic Plans and Exercises

There is a pressing need to better integrate social, psychological, and communication issues into agroterrorism contingency plans and training exercises. Many plans and exercises continue to give only minimal attention to these crucial considerations. Key areas (e.g. provision of appropriate services, development of an effective risk communication strategy, maintenance of trust and confidence) need to be explicitly addressed, and relevant roles and coordination issues need to be delineated and practiced on a regular basis. Without adequate consideration of relevant social, psychological, and communication issues, plans and exercises will be unrealistic and of limited value in preparing agencies and responders to deal with the complex challenges posed by an agroterrorism attack.

## 5 RESEARCH DIRECTIONS

In addition to implementing the lessons learned from the foot-and-mouth outbreak and other relevant experiences, it will be important in the coming years to carry out further research related to the social, psychological, and behavioral aspects of agroterrorism. In this regard, the topics identified in the 2002 National Research Council report on agricultural terrorism continue to be relevant [1]. For example, it would be useful to conduct additional work on how best to assist individuals and communities affected by an agroterrorism attack and how best to speed recovery.

Another key area of research involves improving our understanding of the factors that affect compliance with infection control measures during large-scale agricultural disease outbreaks. What factors serve to facilitate compliance and what factors make compliance less likely? How, for example, do different work practices, economic situations, or local customs come into play? A better understanding of such factors will aid in the development of more realistic and more effective infection control strategies.

Finally, it would be valuable to expand research on emergency communication during large-scale agricultural disease outbreaks. It is clear from the foot-and-mouth experience that communication problems exacerbated the outbreak's impacts and damaged public trust and confidence. The stakes and the costs of failure could be even higher in an agroterrorism event. There is, therefore, a pressing need for additional research to better understand people's concerns, information needs, and preferred information sources in relation to agroterrorism threats. Improved emergency communication—including the development of empirically grounded, pre-event messages—could play an important role in reducing an outbreak's spread, mitigating its impacts, and maintaining trust, social cohesion, and public confidence.

## ACKNOWLEDGMENTS

This article is based, in part, on fieldwork conducted by the author in the United Kingdom during and after the 2001 foot-and-mouth disease outbreak. The author is grateful to the many individuals and organizations that helped facilitate this work. Special thanks are due to the US Embassy in London, the Department for Environment, Food and Rural Affairs, the Rural Stress Information Network, the Ministry of Defence, and the National Farmers Union. Thanks are due as well to A. Becker, D. Franz, and R. Gurwitch, who provided helpful comments on earlier versions of the manuscript. Finally, the author wishes to thank the Lister Hill Center for Health Policy, and the Smith Richardson Foundation (International Security and Foreign Policy Program), which provided support for the research.

## REFERENCES

1. National Research Council (2002). *Countering Agricultural Bioterrorism*, Committee on Biological Threats to Agricultural Plants and Animals. The National Academies Press, Washington, DC.
2. Becker, S. M. (2001). Meeting the threat of weapons of mass destruction terrorism: toward a broader conception of consequence management. *Mil. Med.* **166**(S2), 13–16.
3. Anderson, I. (2002). *Foot and Mouth Disease 2001: Lessons to be Learned Inquiry*, Stationery Office, London.
4. Donaldson, A. (2004). Clinical signs of foot-and-mouth disease. In F. Sobrino, E. Domingo, Eds. *Foot and Mouth Disease: Current Perspectives*, Horizon Bioscience, Norfolk, pp. 93–102.
5. Brown, F. (2004). Stepping stones in foot-and-mouth research: a personal view. In F. Sobrino, E. Domingo, Eds. *Foot and Mouth Disease: Current Perspectives*, Horizon Bioscience, Norfolk, pp. 1–17.
6. Rowlands, D. J., Ed. (2003). *Foot-and-mouth Disease*, Elsevier Science B.V., Amsterdam.
7. Blancou, J., Leforban, Y., and Pearson, J. E. (2004). Control of foot-and-mouth disease: role of international organizations. In F. Sobrino, E. Domingo, Eds. *Foot and Mouth Disease: Current Perspectives*, Horizon Bioscience, Norfolk, pp. 425–426.
8. National Audit Office (2002). *The 2001 Outbreak of Foot and Mouth Disease*, Stationery Office, London.
9. Bennett K., Carroll, T., Lowe, P., and Phillipson, J., Eds. (2002). *Coping with Crisis in Cumbria: Consequences of Foot and Mouth Disease*, Centre for the Rural Economy, University of Newcastle upon Tyne, Newcastle upon Tyne.
10. Western Morning News (2001). *Foot and Mouth: How the Westcountry Lived Through the Nightmare*, Western Morning Press, Plymouth.
11. Royal Society of Edinburgh (2002). *Inquiry Into Foot and Mouth Disease in Scotland*, Royal Society of Edinburgh, Edinburgh, Scotland.
12. Becker, S. M. (2004b). Learning from the 2001 foot and mouth disease outbreak: social, behavioral and communication issues. *Scientific Panel on Agricultural Bioterrorism: Countering the Potential for Impact of Biothreats to Crops and Livestock*, American Association for the Advancement of Science, Seattle, Washington, April 14, 2004.
13. Ingham, J., (2001). Look at the human suffering caused by efforts to keep this invisible enemy at bay. Daily Express, p. 33.
14. Bennett, K., and Phillipson, J. (2004). A plague upon their houses: revelations of the foot and mouth disease epidemic for business households. *Sociol. Ruralis* **44**(3), 261–284.

15. Peck, D. F., Grant, S., McArthur, W., and Godden, D. (2002). Psychological impact of foot-and-mouth disease on farmers. *J. Ment. Health* **11**(5), 523–531.
16. Garnefski, N., Baan, N., and Kraaij, V. (2005). Psychological distress and cognitive emotion regulation strategies among farmers who fell victim to the foot-and-mouth crisis. *Pers. Individ. Dif.* **38**(6), 1317–1327.
17. Olff, M., Koeter, M. W. J., Van Haaften, E. H., and Kersten, P. H. (2005). Gersons BPR Impact of a foot and mouth disease crisis on post-traumatic stress symptoms in farmers. *Br. J. Psychiatry* **186**(2), 165–166.
18. Deaville, J., Kenkre, J., Ameen, J., Davies, P., Hughes, H., Bennett, G., Mansell, I., and Jones, L. (2003). *The Impact of the Foot and Mouth Outbreak on Mental Health and Well-being in Wales*, November. Institute of Rural Health and University of Glamorgan, Glamorgan.
19. Hannay, D., and Jones, R. (2002). The effects of foot-and-mouth on the health of those involved in farming and tourism in Dumfries and Galloway. *Eur. J. Gen. Pract.* **8**, 83–89.
20. Peck, D. F. (2005). Foot and mouth outbreak: lessons for mental health services. *Adv. Psychiatr. Treat.* **11**(4), 270–276.
21. Mort, M., Convery, I., Baxter, J., and Bailey, C. (2005). Psychosocial effects of the 2001 UK foot and mouth disease epidemic in a rural population: qualitative diary based study. *British Medical Journal* **331**, 1234.
22. Gurwitch, R. H., Kees, M., Becker, S. M., Schreiber, M., Pfefferbaum, B., and Diamond, D. (2004). When disaster strikes: responding to the needs of children. *Prehospital Disaster Med.* **19**(1), 21–28.
23. Mercer, I. (2002). *Crisis and opportunity: Devon foot and mouth inquiry 2001*, Devon Books, Tiverton Devon.
24. Nerlich, B., Hillyard, S., and Wright, N. (2005). Stress and stereotypes: children's reactions to the outbreak of foot and mouth disease in the UK in 2001. *Child. Soc.* **19**(5), 348–359.
25. Beeton, S. (2001). How foot and mouth disease affected a rural continence service. *Nurs. Times* **97**(40), 59–60.
26. Gregory, A. (2005). Communication dimensions of the UK foot and mouth disease crisis, 2001. *J. Public Aff.* **5**(3–4), 312–328.
27. Poortinga, W., Bickerstaff, K., Langford, I., Niewohner, J., and Pidgeon, N. (2004). The British 2001 Foot and Mouth crisis: a comparative study of public risk perceptions, trust and beliefs about government policy in two communities. *J. Risk Res.* **7**(1), 73–90.
28. Hagar, C., and Haythornthwaite, C. (2005). Crisis, farming & community. *J. Community Inform.* **1**(3), 41–52.
29. Bush, J., Phillimore, P., Pless-Lulloli, T., and Thomson, C. (2005). Carcass disposal and siting controversy: risk, dialogue and confrontation in the 2001 foot-and-mouth outbreak. *Local Environ.* **10**(6), 649–664.
30. Levin, J., Gilmore, K., Nalbone, T., and Shepherd, S. (2005). Agroterrorism workshop: engaging community preparedness. *J. Agromedicine* **10**(2), 7–15.
31. Vanderford, M. L. (2004). Breaking new ground in WMD risk communication: the pre-event message development project. *Biosecur. Bioterror.* **2**(3), 193–194.
32. Becker, S. M. (2004a). Emergency communication and information issues in terrorism events involving radioactive materials. *Biosecur. Bioterror.* **2**(3), 195–207.
33. Becker, S. M. (2005). Addressing the psychosocial and communication challenges posed by radiological/nuclear terrorism: key developments since NCRP 138. *Health Phys.* **89**(5), 521–530.
34. U.S. Department of Health and Human Services (2002). *Communicating in a Crisis: Risk Communication Guidelines for Public Officials*, Center for Mental Health Services, Substance Abuse and Mental Health Services Administration, U.S. Department of Health and Human Services, Washington, DC.

35. Wray, R., and Jupka, K. (2004). What does the public want to know in the event of a terrorist attack using plague? *Biosecur. Bioterror.* **2**(3), 208–215.
36. Glik, D., Harrison, K., Davoudi, M., and Riopelle, D. (2004). Public perceptions and risk communication for botulism. *Biosecur. Bioterror.* **2**(3), 216–223.
37. Henderson, J. N., Henderson, L. C., Raskob, G. E., and Boatright, D. T. (2004). Chemical (VX) terrorist threat: public knowledge, attitudes, and responses. *Biosecur. Bioterror.* **2**(3), 224–228.
38. Marist College Institute for Public Opinion (2003). *How Americans Feel About Terrorism and Security: Two Years After 9/11* , Survey conducted on behalf of the National Center for Disaster Preparedness and the Children's Health Fund. August.

## FURTHER READING

Brown, C. (2003). Vulnerabilities in agriculture. *J. Vet. Med. Educ.* **30**(2), 112–114.

Chalk, P. (2004). *Hitting America's Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against the U.S. Agricultural and Food Industry*, The Rand Corporation, Santa Monica, CA.

Hugh-Jones, M. E. (2002). Agricultural bioterrorism. In *High-Impact Terrorism: Proceedings of a Russian—American Workshop. National Research Council in Cooperation with the Russian Academy of Sciences*, The National Academies Press, Washington, DC, pp. 219–232.

# FOREIGN ANIMAL DISEASES AND FOOD SYSTEM SECURITY

BARRETT D. SLENNING

*Department of Population Health and Pathobiology, College of Veterinary Medicine, North Carolina State University, Raleigh, North Carolina*

JIMMY L. TICKEL

*Emergency Programs Division, North Carolina Department of Agriculture and Consumer Services, Raleigh, North Carolina*

## 1 INTRODUCTION

Food safety and security takes many forms and requires differing methods, depending on the nature of the threat, the kind of agricultural commodity vulnerabilities involved, and

the consequences of the event. Major threats to western agricultural economies are foreign animal diseases (FADs), such as foot and mouth disease (FMD) or highly pathogenic avian influenza. In fact, such are the threats, through direct effects on food production and security, as well as through direct and indirect impacts on public health and economic stability, that all nations have developed major programs for detecting and eradicating these diseases as soon as is practicable. Most such programs are aimed toward quickly regaining international trade, and so, utilize severe control methods such as stop movement orders (SMOs) and "stamping out/eradication" (SOE) programs. However, SOE was designed and proven under market systems very different from those in modern agriculture. Further, the focus on international trade, at least for the United States (USA), is misguided. In the end, SOE programs have shown themselves to have the potential, if not the probability, to trigger cascades of unintended consequences;consequences that can destroy the farms and food security they were intended to protect. Modern agriculture requires that we rethink our focus and methods, such that the goal is to maximize farm survival through intelligent use of business continuity methods by accessing new technologies and tools, and through exploiting characteristics of modern agricultural markets.

## 2 BACKGROUND

To understand how SOE programs came to be, and why they no longer are fully appropriate in the modern age, we need to look back at agriculture as it was when the plans and perspectives were designed and initially used, and then see how the landscape has changed.

### 2.1 Agriculture in the Twentieth Century

For most of the twentieth century, agriculture was seen as ubiquitous, small-scale, and oriented or marketed locally: farms were relatively small, and much of the population was involved in agriculture; farms did not move; animals and products remained within a fairly local economy. FAD outbreaks that could result in a loss of foreign trade were considered to be one of the few threats that could create a national disaster. However, since FAD outbreaks were projected as local events, the solution to restoring trade was to quickly contain the small outbreak and eradicate the disease. Thus, FAD responses were aimed at identifying affected herds or flocks and destroying them to minimize impacts on trade agreements and markets [1]. Additionally, these programs carried unstated presumptions that the only risks agriculture faced were from accidental or natural threats, and these assumptions colored the scenarios against which programs were designed. The concept of intentional attacks or of accidental market-spread outbreaks were not serious considerations for researchers or decision makers.

### 2.2 Agriculture in the Twenty-First Century

Currently, agriculture is large-scale, highly mobile, and interdependent. Agriculture is dependent on transportation and just-in-time management. While agriculture is still a major economic sector across the country, a very small proportion of the population makes their living through farming. Exports are not primary aspects of US livestock; in 2007, the percent of domestic production going to exports for beef, pork, and poultry

were 5.4%, 14.3%, and 15.7%, respectively, yielding an overall export market for livestock products equaling approximately 12% of overall domestic production [2, p. 32]. This suggests programs whose aims are to protect exports at the expense of domestic production have their priorities misplaced.

Agriculture is now developing concentrated "production centers" (parts of the country where a type of production is concentrated and predominates, such as poultry in the Delmarva peninsula, corn in Iowa, or catfish farming in Mississippi), which operate and have resources and skills far beyond what twentieth century farms could imagine. Furthermore, ownership has concentrated, such that now majorities of primary production and processing are owned by a few small groups and companies, allowing for consistent management and rapid communications. Finally, agriculture is now highly integrated. For instance, in the large poultry production centers of the southeastern US, the companies involved in production also operate their own feed processing, transportation, and wholesale or retail divisions. These structural innovations change the risk profiles against which we should be defending.

### 2.3 Threat Profiles of Today

Reviews of recent FMD outbreaks in Taiwan (1997, [3, 4]), United Kingdom (2001, 2007, [5, 6]), plus bovine spongiform encephalopathy (BSE) in Canada (2003), United States (2004, 2005), [7, 8], with added insight from Newcastle Disease and highly pathogenic avian influenza outbreaks in North America (2003–2004, [9, 10]), have uncovered new considerations in regional or state disease control programs.

For instance, the United Kingdom experienced near wholesale destruction of its cattle markets with the 1985 discovery of BSE, and added damage to both cattle and swine with the destruction of over 6 million animals in the 2001 FMD outbreak, third of which were done for "welfare" reasons (Fig. 1, [11, p. 21]). Welfare slaughter occurs when, with markets shut down and animal movement stopped, farms soon run out of space, feed, and/or money, and have no option other than to destroy their animals or let them starve. The United Kingdom has experienced, as a result, a drop in domestic consumption, signaling that severe outbreaks can lead to such changes in demand that attempts to maintain supply are futile. In another example, the Taiwan FMD experiences in the late 1990s (Table 1, [3, 4]), demonstrate that agriculture is actually quite fragile in the face of major supply and demand perturbations. In 1996, Taiwan was one of the largest pork exporters in the Pacific Rim. After FMD, Taiwan became a net pork importer; as of 2009 they had not regained their production or market share.

Lastly, from documents found in Taliban sites in Afghanistan [12], to environmental or animal rights websites, it is apparent that agriculture, though a major critical infrastructure, is seen by its enemies as a large, soft target, susceptible to being a focus of politically motivated economic warfare. While none of the above disease events described were intentional in their origin, the results of the outbreaks are similar to what will be seen in a planned attack to either target an industry (state-level or locally) or a whole production system (nationally). The modern trend involving rapid and distant transportation of animals, feedstuffs, employees, and equipment, factored with collateral movements (wildlife, tourists, etc.), work synergistically to allow a disease agent to enter the production system by accident and create multifocal widespread outbreaks in a very short period of time (hours to days). Thus, accidental introductions of an FAD agent are likely to present the same disease management challenges that are found in intentional introductions.

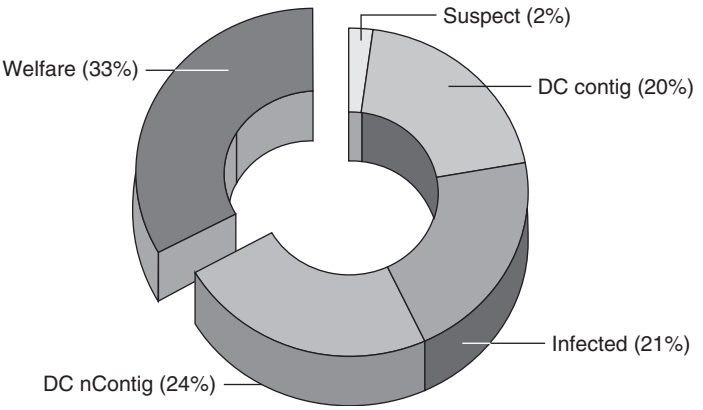



**FIGURE 1** Reasons for animal destruction (UK 2001). In the 2001 FMD outbreak in the United Kingdom, fully one-third of all animals destroyed were killed for "welfare" reasons—the animals had no markets to go to and the farms ran out of money and/or resources. Welfare, destroyed for welfare reasons; Infected, destroyed after confirmation of disease; DC Contig, destroyed as a contiguous dangerous-contact herd; DC nContig, destroyed as a noncontiguous dangerous-contact herd; Suspect, destroyed after classification as suspected of having disease. [Data from: Ref. [11]].

**TABLE 1 Breakdown of Costs As of 3 Years After the Taiwan Foot and Mouth Disease (FMD) Outbreak**

| Item or Activity | Cost | Percentage of Direct Costs (%) |
|---|---|---|
| Indemnity for pigs destroyed | $ 188 million | 49.5 |
| Vaccine costs | $ 14 million | 3.6 |
| Carcass disposal | $ 25 million | 6.5 |
| Miscellaneous | $ 28 million | 7.4 |
| Market value losses | $ 125 million | 33.0 |
| Total direct costs | $ 380 million | 100.0 |
| Total indirect costs (jobs, tourism) | $ 3,650 million | 961.0 |

*Note:* Taiwan used stamping out plus reactive vaccination protocols. Total direct costs of the disease response ($380 million) is only one tenth of the total indirect costs of this event. This means that major foreign animal disease outbreaks are *societal* catastrophes that come to society through agriculture. [Data from: Refs. 3, 4].

## 3 DETAILS AND CHALLENGES IN OPERATING STAMPING OUT/ERADICATION PROGRAMS

SOE programs are initiated to achieve very specific goals, and the prioritization of tools and methods are based on assumptions that are often unstated. However, those assumptions are then left untested, meaning that the outcomes of the program will be very different from what was originally envisioned. To better understand how this can happen, we need to look at the history of SOE: how it works and how it fails.

### 3.1 How Stamping Out Programs Work

Historically, programs for controlling FADs use the standard SOE approaches of quarantine (stop movements) and euthanasia as their primary tools [1]. In such a program,

animal and product movement are stopped, decreasing disease expansion, and allowing time for affected herds or flocks and likely to be affected herds or flocks to be identified. The animals are then destroyed and disposed of, to halt their ability to spread disease. After a period of strict surveillance, official movement permits allow markets to build back. In this way, such programs eradicate FADs by stopping agent replication and shedding, as depicted in the UK FMD 2001-based model shown in Figure 2 [13].

Some new measures have been added to the SOE approach in recent years. Emergency vaccination is one such advancement: "ring" or "fence" vaccination involves identifying an infected premise (IP) and vaccinating herds around the IP to limit opportunities for the agent to spread, analogous to setting backfires to stop forest fires. Interestingly enough, until recently, the SOE perspective limited the best use of vaccine (i.e. vaccine to protect and preserve life) and instead required that vaccinated animals be euthanized even though they were not infected [13, 14]. New technologies can now allow differentiation between vaccinated uninfected animals versus animals that are infected, making such "Vaccinate to Kill" strategies obsolete.

As a result of its long and proven track record in eradicating disease, its conceptual and logistical straightforwardness, and its clearly identifiable outcome, SOE has been the preferred tactic embraced by FMD-free countries since the mid-twentieth century [15]. Additionally, emergency vaccination is seeing increased interest from international FAD programs, and the World Organization for Animal Health (WOAH or OIE Office International des Épizooties), which is changing rules that have previously severely penalized vaccine-using countries [13].

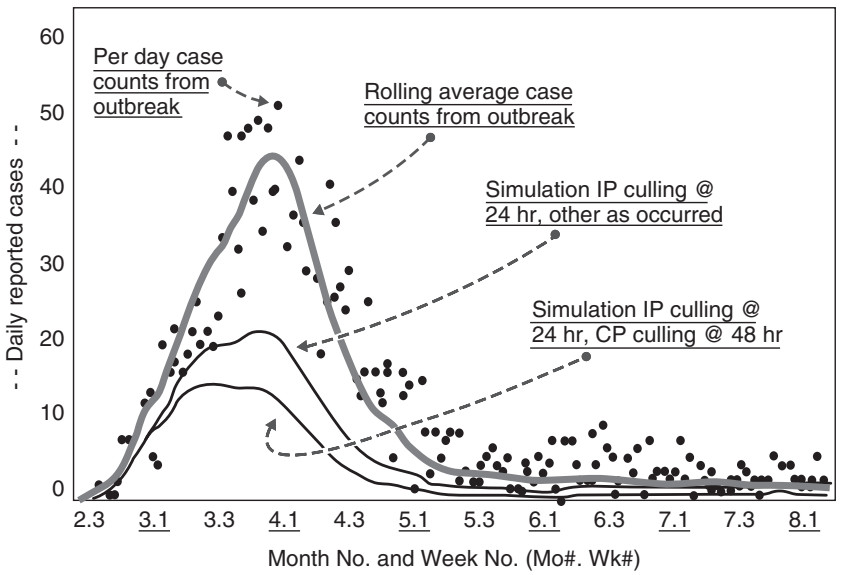



**FIGURE 2** SOE program goals and outcomes. Analysis of actual versus simulated epidemic curve for the 2001 UK FMD outbreak, assuming different levels of goal achievement for detection and slaughter. Actual did not achieve culling goals of infected premises (IPs) within 24 h of diagnosis, and contiguous premises (CPs) within 48 h. [Adapted from: Ref. [13] Chapter 10, Chart A, p. 94, with permission].

### 3.2 How Stamping Out Programs Fail

An SOE approach operated as the sole or primary tool for outbreak control has its problems [16]. For instance, the assumption that outbreaks will start small is likely to be false in today's mobile agriculture. Modeling of FADs suggests that either bioterror events or accidental market-driven outbreaks will not be present as small, local events. As an example, simulations suggest that an FMD outbreak starting in swine in eastern North Carolina (NC) could be in 5–7 states, affecting almost 500 herds in the first 10 days following exposure. Worst-case scenarios suggest an FMD outbreak could require destroying between 30 and 50 million animals, and would take more than 9 months (almost 280 days) to get under control [17, 18]. Thus, if SOE were to be used as the sole response tool, large numbers of animals, both of positive and negative nonexposed herds, will be euthanized. Additionally, to limit scavengers and potential public health concerns from the carcasses of euthanized animals, very rapid carcass destruction and disposal is required, usually by burial, composting or burning [19]. All carry public perception and environmental problems if done on a large scale, further limiting the attractiveness of an SOE approach. In the end, few workers believe that US society would tolerate that level of animal waste and destruction. Fewer still believe the United States could mobilize the necessary personnel to successfully execute and complete such a massive campaign.

Adding emergency vaccine to an already late SOE approach does little to help, because its only response to being "behind the disease curve" is to increase the size of the potential "rings." As shown in Table 2, however, increasing vaccination-ring size increases personnel and supply requirements by a square of the ring's diameter increase, at a time when both are likely to be very limiting.

Another problem is that SMOs required for SOE create massive damage in today's highly mobile "just-in-time" agriculture. Estimates from the NC dairy industry to the authors are that if interstate milk movement is stopped, the entire NC system milk storage capacity would be reached within 48 h—far short of a typical multiday SMO–there would be nowhere for milk to go, even if the state remained FMD-free, thereby jeopardizing a healthy dairy industry.

Even properly managed SMOs can create tremendous damage at the individual farm level. For example, Figure 3 illustrates a simple analysis done by us determining how many non-shipping days a dairy could absorb before its annual profit (measured as returns to management) reached zero. It suggests the average NC dairy in spring 2009 producing between 17,000 and 18,000 lbs of milk per cow, could survive an SMO up to 9–13 days, assuming all else is equal. Should the control and recovery program increase costs (or decrease milk prices) by a mere 3%; however, these farms will have zero returns to management within hours of instituting the SMO. Higher-producing farms, assuming similar debt and externals, survive longer, but the trend is relentless: The longer SMOs last, the more of the industry will fail, *even though they are doing everything right and remain uninfected*.

The SOE/SMO mind-set can permeate other disease control programs. For instance, in spring 2009, a commercial Canadian swine herd was infected with the novel H1N1 influenza virus by a worker. Although the disease ran its course in the herd (no animals died), and recovered animals are not infective, the government stopped all movement of animals from the farm. This introduced welfare degradation, which meant they had to slaughter animals for welfare purposes. Furthermore, animals were kept out of the human food chain, and even rendered product (a process that destroys all viruses) had to be disposed of by one of the most expensive means, landfilling. To explain the reasoning,

**TABLE 2 Demonstration of Logistical Problems with Increasing the Size of a Ring Vaccination Program's Area**

| Default Program | Proposed Program | Factor Increase | Item/Resource Measure/Count |
|---|---|---|---|
| 2 | 6 | 3.0 | Kill zone (KZ) radius (mi) |
| 6 | 18 | 3.0 | Control zone (CZ) radius (mi) |
| 13 | 114 | 8.8 | KZ area (sq. mi) |
| 101 | 905 | 9.0 | CZ area (sq. mi) |
| 26 | 227 | 8.7 | KZ swine farm count |
| 202 | 1810 | 9.0 | CZ swine farm count |
| 50,266 | 452,390 | 9.0 | KZ count pigs |
| 402,124 | 3,619,115 | 9.0 | CZ count pigs |
| 88 | 760 | 8.6 | Kill team personnel count |
| 448 | 4024 | 9.0 | Vaccination team personnel count |
| 9 | 26 | 2.9 | KZ roadblock count |
| 26 | 76 | 2.9 | CZ roadblock count |
| 34 | 101 | 3.0 | KZ roadblock personnel count |
| 101 | 302 | 3.0 | CZ roadblock personnel count |
| 706 | 5289 | 7.5 | Total personnel count |
| 50,266 | 452,390 | 9.0 | Total animal euthanasia sets required |
| 402,124 | 3,619,115 | 9.0 | Total vaccine doses required |

*Note:* Typical eastern North Carolina swine-farm size and density, and roadway density, plus standard response task force/strike team sizes and shift length used for both options. Counts rounded to next whole number.
DEFAULT: Assumes a program with a 2-mile radius for culling KZ, where herd destruction would occur and a 6-mile radius for vaccination CZ, where vaccination would occur;
PROPOSED: Expands KZ to a 6-mile radius, and CZ to an 18-mile radius (i.e. a threefold increase in radii compared to DEFAULT).
The PROPOSED increase results in a 7.5- to 9-fold increase in immediate needs for personnel, eqipment, and supplies. This increase provides a near tripling of the distance the virus must spread to break the ring vaccination program before animals respond to the vaccine, which does not translate to a threefold decrease in risk, let alone a ninefold improvement.

a Canadian official was quoted as saying " . . . The decision to cull the herd was to ease overcrowding . . . This doesn't have anything to do with the flu, . . . It has to do . . . with animal welfare . . . Due to the quarantine, these animals cannot be moved off the farm as they normally would. The living conditions would soon become unacceptable due to overcrowding and they (the pigs) would have been in distress . . . " [20]. As with the discussion of the dairies shut out of their market by SOE/SMO procedures above, we must be honest in recognizing that these animals, and these farms, are destroyed by our *programs*, not by the disease.

Lastly, a strong motivation to transition FAD response away from SOE/SMO policies stems from the observations that historical plans generated numerous unintended consequences beyond the direct market effects mentioned above. Two especially vexing issues include (i) that our programs induce paradoxical motivation for producers to seek ways for their herds or flocks to become infected or to bypass control measures in last-ditch efforts to avoid individual financial ruin by either gaining indemnities or selling product [21] and (ii) that we ignore the socioeconomic and political impacts on nonagricultural facets of communities and economies; impacts that are often several fold greater than the direct impacts on agriculture (see Table 1 as an example).

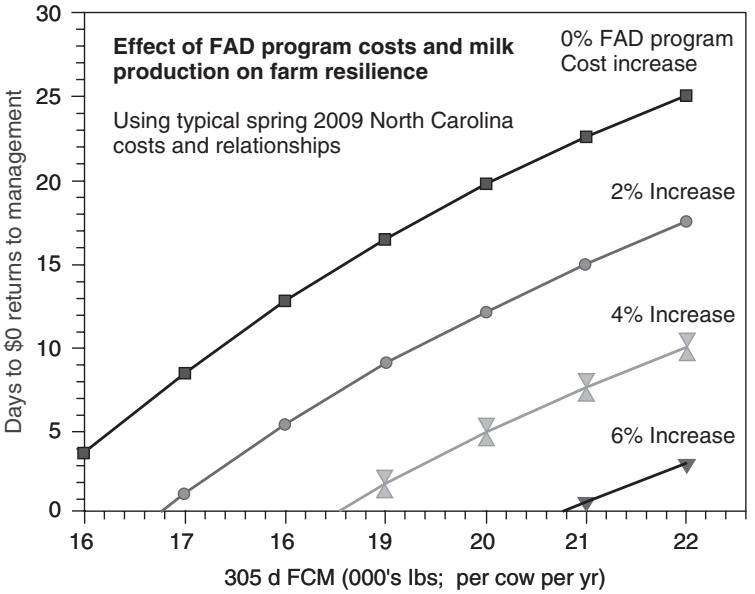



**FIGURE 3** Destroying uninfected farms through SOE programs. Economic prediction for dairies' resilience to stop movement orders (using typical NC dairy cost structures and trends), as a function of per cow milk production and across program-induced cost increases from 0% to 6%. The typical NC dairy produces almost 18,000 lbs FCM, meaning it would have mere days before a stop movement program would erase a total year's profit, assuming the program did not change the dairy's relative costs and income. However, if the SOE program decreased income relative to cost by 2%, its resiliency is halved. Should the SOE program imbalance costs and revenues by 4%; however, the farm will almost immediately become unprofitable. This damage occurs even though the farm is uninfected by the disease. FCM, fat-corrected milk production per cow per lactation.

## 4 KNOWLEDGE ADVANCES ENCOURAGING DEVELOPMENT OF BALANCED EVENT MANAGEMENT STRATEGIES

Many nations and trade blocks have reconsidered their FAD programs, and are considering a more managed strategy. For instance, WOAH/OIE has increased its interest in, and work with (i) regionalization within a country (declaring parts of a country free of disease and open to trade) and compartmentalization within industries (allowing unaffected segments to continue economic activity), (ii) decreasing the time-to-trade-resumption penalties that countries practicing FMD vaccination face, and (iii) updating their rules and policies regarding testing and vaccination technologies [22].

But these changes, though helpful, do not address fundamental issues causing SOE/SMO methods to fail. A major lack is in not recognizing how technologies offer improved methods and tools [23, p. 122]. Following are but a few of the disciplines and technologies that have recently advanced greatly. While many examples could be brought forth, here we only address vaccinology or immune enhancements, disease detection, and information technology. Together, they bring new tools and opportunities for prevention, response, and recovery.

### 4.1 Advances and Tools Ignored by Most Stamping Out Plans

Current vaccine development techniques include functional genomics and gene alteration techniques that produce live vector-based vaccines exploiting important gene expression and genetic recombination techniques to increase their safety and create readily identifiable genetic markers for differentiation from wild virus [24]. Subunit vaccines—products that do not involve the use of live agents—can take vaccine safety margins to levels unattainable by standard killed or attenuated techniques [25]. Novel methods of vaccine delivery—through feed, aerosols, or the previously mentioned vectors—promise to improve the ability to cover disparate populations. Further, improvements in lyophilization and sterilization have enhanced shelf life and stability, making long-term stockpiling of these tools in ready-to-deploy forms more feasible. Nonvaccine immune system enhancement opportunities have been augmented through expanding knowledge of general animal health, nutrition, and stressors. Direct oral or mucosal delivery of interferons have demonstrated themselves to be an effective and fast therapy against viruses, including FMD–without vaccine use. The ability to include such products in feed during an outbreak has experimentally shown efficacy in protecting swine from FMD infection, even without concomitant vaccines [26]. Developments in understanding and manipulating different parts of immune systems (e.g. cell-mediated vs. humoral) to optimize responses to different agents also show highly specific potentials for control applications. Finally, long-term genetic techniques and expanded genome maps promise new opportunities to create more disease resistant livestock.

Modern materials science, biochemistry, nanotechnology, mathematical pattern-recognition, spectroscopy, and molecular imaging systems have recently been combined to optimize approaches to rapid, high resolution, accurate, and efficient diagnostic and biosensor tools. Environmentally stable automated systems that can combine sampling and detection technologies have been commercialized and adapted to business, environmental, and military applications as well. Combined with previously mentioned genetically altered vaccines, these technologies potentially allow rapid and repeatable differentiation of vaccinated, recovering, and recently exposed animals [27].

The last innovation example, information technology, is perhaps the most obvious and socially permeating change that is not recognized in typical SOE plans. Field personnel now access and create information at speeds and distances unheard of only a decade ago. Global positioning systems incorporated into mobile wireless devices are currently in-field for military and government planners and responders. With the advent of national animal identification systems and shared multihazard data structures [28], these systems create new avenues for planning and executing trace-in/trace-out work, for monitoring animal flow, and for serving as the basis for syndromic surveillance systems, distributed databases, and "network aware" activities and coordination, where central decision makers and in-field workers have access to real-time updated data.

## 5 TRANSITIONING TO A STRATEGIC EVENT MANAGEMENT POLICY

Recent catastrophic FAD outbreaks from all parts of the globe have highlighted policy areas we need to improve (e.g. the lack of state or national consideration of business continuity issues for primary production, secondary handling or processing, and support industries) while designing and executing FAD control and eradication programs. A key driver to quickening the transition needed will be the realization that SOE policies as

stand-alone solutions are not the answer to the challenges presented to modern food and agriculture by FADs.

### 5.1 Regionalization, Compartmentalization, Proof-of-Status Testing

Consideration of both sides of a disease event (infected case management and uninfected premises administration) are critical to transitioning between SOE and an event management strategy. Approaches and tactics such as regionalization, compartmentalization, standardized biosecurity, and proof of negative-status testing are all part of a comprehensive managed response, and as mentioned above are experiencing interest internationally [22].

Modern agriculture continues to regionalize and compartmentalize itself into production centers, and will do so in the future due to a number of different factors adding to the validity of the approach [29]. While regionalization refers to geographic separation and specialization of production and processing, compartmentalization capitalizes on breaks that occur naturally in production processes. For example, in swine production many producers have breaks (physical, workforce, and management separations) among sows /pigs, nursery age pigs, and finishing pigs, producing essentially a three-compartment production system. Compartmentalization has been utilized by industry in day-to-day operations to protect the overall health of their animals and the system by safeguarding different segments, and improving organization and efficiency. This same strategy can be used during disease outbreaks to maximize response organization, effectiveness, efficiency and more importantly, to protect uninfected segments of agriculture.

Unfortunately, current SOE/SMO plans treat these densely populated and specialized production centers as if they were small and relatively isolated, that is, as if they were farms and companies from the 1950s. This results in current FAD response plans working against regionalization, and ignoring compartmentalization. However, understanding Production Centers, regionalization, and compartmentalization, can afford response officials the ability to designate zones for infected herds or flocks, as well as for negative herds or flocks. As regionalization and compartmentalization approaches are developed specific to a region and an industry, response actions such as proof-of-status testing and standardized biosecurity can support control activities, so that as response officials in infected states grapple with eradication, response officials in negative states can preserve their food production, processing, and related industries through business continuity efforts.

### 5.2 New Horizon: Programs and Tools That Can Aid the Transition

There are a number of programs and tools in existence or in development that can greatly aid the transition. Existing programs include Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability (CARVER) and Shock (a threat assessment tool that evaluates the vulnerability to, and the shock factor of, a successful attack on an entity) [30] and Food Agriculture Sector–Criticality Assessment Tool (FAS–CAT), a method to assess the subsystems comprising the overall food and agricultural organization [31]. Others in development offer new methods to help responders gauge readiness and develop standardized cross-jurisdictional plans. To insure that efforts are fully integrated, standardized exercises can be conducted in states, regions, and nationally through a program known as Homeland Security Exercise and Evaluation Program (HSEEP) [32]. Finally, recognizing that agriculture and food systems have outgrown local approaches

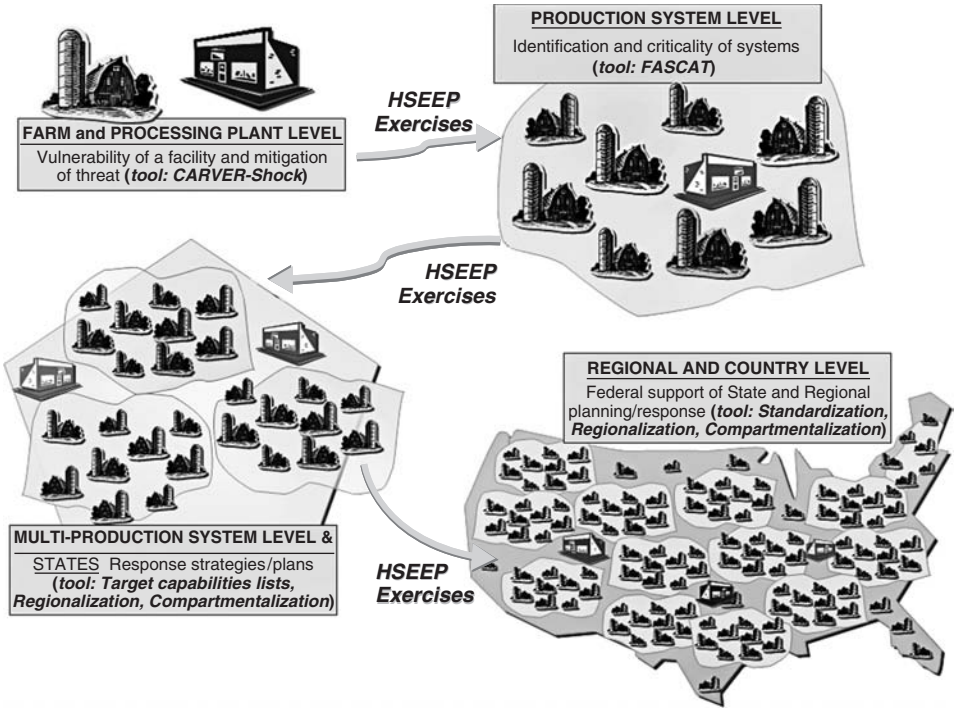



**FIGURE 4** Diagram of "farm to fork" resilience planning. Scalable processes and tools allow vulnerability analyses and prioritization at all levels of food security. However, some tools and methods will be appropriate at some levels, but not others. For descriptions of the tools listed, please see the text.

to FADs has led to regional planning efforts utilizing tools such as compartmentalization and regionalization. The keys will be to develop standardized approaches across states (i.e. regions) for biosecurity measures, proof-of-status testing (surveillance), zoning guidelines, and movement protocols, as illustrated in Figure 4.

## 6 CONCLUSIONS

The combination of new knowledge, tools, and economic environments has given rise to new considerations for disease control programs. It is now evident that the current plans to prioritize FAD eradication by only using strict SOE (Figure 5, [33]) in order to maintain agricultural trade, if applied in the many advanced agricultural regions of the United States, are likely to not only fail to contain the epidemic, but could so damage the industries that they will not recover.

Furthermore, given the concentration of production centers seen in NC swine, California dairies, or High Plains' feedlots, emergency ring vaccination strategies are likely to consume vast amounts of very limited early resources to achieve minimal results. From a systems' perspective, then, the unavoidable conclusion is that historical ideas on control of FADs are counterproductive and could well result in greater net harm to agriculture, to rural communities, and to regional economies, than they will alleviate.

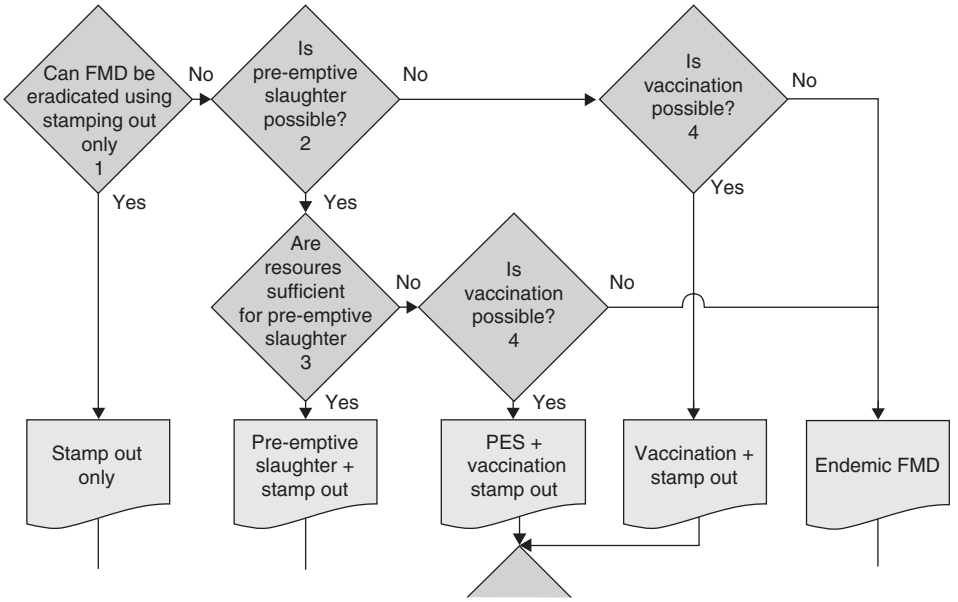



**FIGURE 5** Typical FAD response decision tree for a nonendemic country. Decision tree addressing foot and mouth disease assumes stamping out/eradication, which is the preferred course of action. Only until SOE is deemed infeasible can alternative methods be considered. This disallows risk-based decision processes, and limits decision makers to a single tool, until that tool fails. Such blind rigidity does not belong in decision making within a changing and dynamic event such as an outbreak. [Excerpted from: Ref. [29]].

Finally, in these days of heightened concern for terrorism, we must face the fact that if we can show that even a simultaneous multisite outbreak could be controlled with minimal disruption to production and markets, we will have gone a long way to making these pathogens low-yield tools for those wishing us harm.

Many workers have recognized that new technologies must be incorporated into a comprehensive event management strategy that would prevent and/or limit large-scale outbreaks.

Five characteristics of such a new strategy include the following:

1. *The goal should not be eradication at any cost, but instead, to best assure farm and market survival.* We exist to protect agriculture, not stamp out diseases. Eradication is but one tool we have available in order to accomplish our goals. Managed eradication with attention to business continuity issues regarding production, processing, and transportation will best assure that we protect agriculture and our food supply.
2. *Today's regionalized, compartmentalized, and concentrated production centers should utilize coordinated, facilitated, biosecurity and population health programs. potentially including preventive vaccination.* Production centers represent the largest single points of failure for US agriculture, while at the same time offering us the single best points for establishing targeted prevention and mitigation tools. If we protect production centers (the major population centers) ahead of time, we cut the chances of an uncontrolled epidemic.

3. *We should exploit new means to augment animals' immunities, with or without vaccines.* Using nonvaccine delivery systems will also decrease demands on specially trained personnel and equipment, both of which are always in very limited availability early in any outbreak. Nonvaccine methods also do not trigger trade issues, further helping to assure markets are maintained.
4. *We must minimize SMOs.* They can be minimized through genetically altered or vector vaccines and risk-based differential testing methods, aimed at controlled and permitted market maintenance–that is, we must allow likely negative herds and products to move through markets. A major issue here is in testing capacity, for most state and federal diagnostic laboratories do not have the authority to perform proof-of-status testing, while disallowing private laboratories access and authorities to do the same.

Hence, we must change our formal decision processes to incorporate the new technologies, methods, and opportunities, to better protect agriculture and food security. The decisions cannot presuppose any method as optimal, such as we currently do with SOE. It must be risk-based, with a view toward business continuity, if we are to truly succeed in our goals to protect US food security.

## 7 ABBREVIATIONS

| | |
|---|---|
| BSE | Bovine Spongiform Encephalitis |
| FAD | Foreign Animal Disease |
| FMD | Foot and Mouth Disease |
| IP | Infected Premises |
| OIE | Office International des Epizooties (aka: WOAH/OIE) |
| SMO | Stop Movement Order (aka: Market Standstill) |
| SOE | Stamping-Out / Eradication |
| UK | United Kingdom |
| WOAH | World Organization for Animal Health (aka: WOAH/OIE) |

## REFERENCES

1. Geering, W. A., Penrith, M. L., and Nyakahuma, D. (2009). *Manual of Procedures for Disease Eradication by Stamping Out*, FAO Animal Health Manual No. 12. FAO, Rome, p. 140. Available at http://www.fao.org/docrep/004/y0660e/Y0660E00.htm Accessed 2001 Apr 21.
2. Bange, G. A. (2009). *World Agricultural Supply and Demand Estimates (WASDE-469)*. Table 32: U.S. Meats Supply and Use. Interagency Commodity Estimates Committee, USDA/ERS, Washington, DC, p. 41. Available at http://www.usda.gov/oce/commodity/wasde Accessed 2009 May 09.
3. Anonymous. (1997). Foot-and-Mouth disease spreads chaos in pork markets. *Livestock and Poutlry–World Markets and Trade*. FASonline. USDA/Foreign Agricultural Service, Washington, DC, Updated Dec 2003, p. 4. Available at http://www.fas.usda.gov/dlp2/circular/1997/97-10LP/taiwanfmd.htm Accessed 2009 Apr 20.
4. Huang, S. (2000). Taiwan's hog industry—3 years after disease outbreak. *Agricultural Outlook/October 2000*. Economic Research Service/USDA, Washington, DC, pp. 20–23. Available at http://www.ers.usda.gov/publications/agoutlook/oct2000/ao275h.pdf Accessed 2009 April 20.

5. Anderson, I. (2008). *Foot and Mouth Disease 2007: A Review and Lessons Learned*. Address of the Honourable House of Commons dated 11 March 2008. HC 312. The Stationery Office, London, p. 6. Available at http://archive.cabinetoffice.gov.uk/fmdreview/documents/section_1.pdf Accessed 2009 May 09.
6. Anonymous. (2007). *FMD 2007 Epidemiology Report–Situation at 12:00 Sunday 30 September 2007, Day 58*. Department for Environment, Food and Rural Affairs. London. p. 17 Available at http://www.defra.gov.uk/FootandMouth/ pdf/epidreport300907.pdf Accessed 2009 May 09.
7. Becker, G. S. (2006). *Bovine Spongiform Encephalopathy (BSE, or "Mad Cow Disease'') in North America: A Chronology of Selected Events*. Congressional Research Service, Library of Congress, Order Code RL32932, Washington, DC, p. 35.
8. LeRoy, D., Klein, K. K., and Kivacek, T. (2006). The losses in the beef sector in Canada from BSE. Canadian Agricultural Trade Policy Research Network, Guelph, ON. CATPRN Trade Policy Brief 2006–2004, p. 4. Available at http://www.uoguelph.ca/~catprn/PDF/TPB-06-04-LeRoy.pdf Accessed 2009 Apr 20.
9. Anonymous. *Exotic Newcastle Disease Factsheet (online)*. National Agricultural Biosecurity Center. Kansas State University, Kansas. Available at http://nabc.ksu.edu/content/factsheets/category/Exotic%20Newcastle%20Disease#outbreaks Accessed 2009 Apr 20.
10. Lee, C. W., Swayne, D. E., Linares, J. A., Senne, D. A., and Suarex, D. L. (2005). H5N2 avian influenza outbreak in Texas in 2004: the first highly pathogenic strain in the United States in 20 years? *J. Virol.* **79**(17), 11412–11421. DOI:10.1128/JVI.79.17.11412-11421.2005.
11. Rushton, J., Willmore, T., Shaw, A., and James, A. (2002). *Economic Analysis of Vaccination Strategies for Foot and Mouth Disease in the UK*. Royal Society Inquiry into Infectious Diseases in Livestock, London, p. 95.
12. Friend, M. (2006). Chapter 6 - biowarfare, bioterrorism, and animal diseases as bioweapons. In *Disease Emergence and Resurgence: The Wildlife–Human Connection*, 1st ed., M. Friend, Ed. USGS Circular 1285, Reston, VA, pp. 231–272.
13. Anderson, I. (2002). Chapter 10- pre-emptive slaughter. In *Foot and Mouth Disease 2001: Lessons to be Learned Inquiry Report*, I. Anderson, Ed. The Stationery Office, London, pp. 89–98.
14. Members of the OIE Terrestrial Code Commission (2006–2009). (2008). Glossary. *Terrestrial Animal Health Code 2008*. OIE–World Organization for Animal Health, Paris, p. 12. Available at http://www.oie.int/eng/normes/MCODE/ en_glossaire.htm#sous-chapitre-2 Accessed 2009 May 09.
15. Anonymous. (2009). History of disease control in the UK (On-Line). *Animal Health & Welfare*. Dept of Environment, Food, and Rural Affairs, London. Available at http://www.defra.gov.uk/animalh/diseases/control/history.htm Accessed 2009 Apr 21.
16. Ferguson, N. M., Donnelly, C. A., and Anderson, R. M. (2001). The foot-and-mouth epidemic in Great Britain: pattern of spread and impact of interventions. *Science* **292**, 1155–1160.
17. Anonymous. (2002). *U.S. conducts mock foot-and-mouth outbreak. Animalnet October 1, 2002*. Available at http://archives.foodsafety.ksu.edu/animalnet/2002/10-2002/animalnet_october_1-2.htm#U.S. %20CONDUCTS Accessed 2009 May 9.
18. Reardon, J. W. (2005). *Testimony Before the House Committee on Homeland Security*. Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Washington, DC, p. 16. Available at http://www.globalsecurity.org/security/library/congress/2005_h/050525-reardon.pdf Accessed 2009 May 09.
19. Dörfer-Kreissl, W. (2002). *Report of Measures to Control Foot and Mouth Disease in the European Union in 2001 and Future Measures to Prevent and Control Animal Diseases in the European Union*. [European Parliament Session Document A5-0405/2002]. 28 Nov. pp. 45–52.

20. Strojek, S. (2009). Alberta farm infected with H1N1 culls 500 pigs. *The Canadian Press/CityNews TV*. Rogers Digital Media Co. Toronto. Available at http://www.citynews.ca /news/news_34444.aspx Accessed 2009 May 23.
21. Campbell, D., and Lee, B. (2003). The foot and mouth outbreak 2001: lessons not yet learned. *The UK Foot and Mouth Epidemic of 2001: A Research Resource*. ESRC Centre for Business Relationships, Accountability, Sustainability and Society, Cardiff, p. 27. Available at http://www.fmd.brass.cf.ac.uk/lessonsnotlearnedDCBL.pdf Accessed 2009 May 09.
22. Members of the OIE Terrestrial Code Commission (2006–2009). (2008). Article 8.5. foot and mouth disease. *Terrestrial Animal Health Code 2008*. OIE–World Organization for Animal Health, Paris, p. 23. Available at http://www.oie.int/eng/normes/Mcode/en_chapitre_1.8.5.htm Accessed 2009 May 09.
23. Committee on Assessing the Nation's Framework for Addressing Animal Diseases, National Research Council. (2005). Chapter 4- gaps in the animal health framework. *Animal Health at the Crossroads: Preventing, Detecting, and Diagnosing Animal Diseases*, pp. 118–132.
24. Kitching, P., Hammond, J., Jeggo, M., Charleston, B., Paton, D., Rodriguez, L., and Heckert, R. (2007). Global FMD control–Is it an option?. *Vaccine* **25**, 5660–5664.
25. Moraes, M. P., Chinsangaram, J., Brum, M. C. S., and Grubman, M. (2003). Immediate protection of swine from foot-and-mouth disease: a combination of adenoviruses expressing interferon alpha and a foot-and-mouth disease virus subunit vaccine. *Vaccine* **22**, 268–279.
26. McVicar, J. W., Richmond, J. Y. et al. (1973). Observation of cattle, goats and pigs after administration of synthetic interferon inducers and subsequent exposure to foot and mouth disease virus. *Can. J. Comput. Med.* **37**, 362–368.
27. Pasick, J. (2004). Application of DIVA vaccines and their companion diagnostic tests to foreign animal disease eradication. *Anim. Health Res. Rev.* **5**, 257–262. DOI:10.1079/AHR200479.
28. North Carolina Department of Agriculture (2009). *Emergency Programs - Multi-Hazard Threat Database*. North Carolina Department of Agriculture and Consumer Services, Raleigh, NC. Available at http://www.agr.state.nc.us/oep/MHTD/index.htm Accessed 2009 May 08.
29. MacDonald, J. M., and McBride, W. D. (2009). *The Transformation of U.S. Livestock Agriculture–Scale, Efficiency, and Risks*, Economic Information Bulletin No. 43. Economic Research Service, U.S. Dept. of Agriculture, Washington, DC, 46. Available at http://www.ers.usda.gov/ Publications/EIB43/ Accessed 2009 May 16.
30. Mann, C. J., Acheson, D., and Caverty, J. (2007). Appendix 4: CARVER + Shock Primer. *Agriculture and Food: Critical Infrastructure and Key Resources Sector-Specific Plan*. Food and Agriculture Government Coordinating Council. Washington, DC, p. 250. Available at http://www.cfsan.fda.gov/~acrobat/agfood.pdf Accessed 2009 May 25.
31. The National Center for Food Protection and Defense (2009). *FAS-CAT 1.1*. National Center for Food Protection and Defense, Saint Paul, MN. Available at http://www.ncfpd.umn.edu/ Accessed 2009 May 25.
32. Anonymous. (2007). *Homeland Security Exercise and Evaluation Program - Terminology, Methodology, and Compliance Guidelines*. U.S. Department of Homeland Security, Washington, DC, p. 6. Available at https://hseep.dhs.gov/support/ HSEEP_101.pdf Accessed 2009 May 25.
33. EM/VS/APHIS/USDA. (2005). Appendix 1. vaccine decision tree for a highly contagious disease. *National Animal Health Emergency Management System Guidelines - Response Strategies: Highly Contagious Diseases*, Washington, DC. p. 27, 31.

# INSECTS AS VECTORS OF FOODBORNE PATHOGENS

LUDEK ZUREK

*Kansas State University, Departments of Entomology and Diagnostic Medicine and Pathobiology, Manhattan, Kansas*

J. RICHARD GORHAM

*United States Public Health Service, Food and Drug Administration, Xenia, Ohio*

## 1 INTRODUCTION

Two areas of concern are discussed in this article. One, the major one, has to do with the contamination of food and food-contact surfaces by various insect pests often associated with human or animal foods [1]. The scenarios by which such contaminations occur are well known and are mitigated by strict adherence to sanitation standard operating procedures (SSOPs) and good manufacturing practices (GMPs), by the implementation of the hazard analysis critical control points (HACCP) program, and by the practice of Integrated Pest Management (IPM). We will not describe these four programs. The reader will find abundant resources about these programs on the Internet, from the Land Grant universities, scientific literature, and commercial providers of these programs [2, 3]. The lesser concern, a much less familiar one, deals with intentional food contamination mediated by insect agents. To deal with this threat, an equally proactive approach, similar to SSOPs/GMPs/HACCP/IPM, is essential. It involves a strategy we have termed AIM=F: anticipate, inform, mitigate equals frustrate, that is, the prevention, neutralization or control of intentional acts of food contamination by means of insect agents.

## 2 MUSCOID FLIES AND FRUIT FLIES

Muscoid flies and fruit flies represent a close association of insects with microbes, especially with bacteria originating from human and animal feces and other decaying organic materials. Moreover, muscoid flies have a great potential to contaminate human food and drink with bacteria, including foodborne pathogens, because of their developmental habitats, mode of feeding (regurgitation), unrestricted movement, and attraction to places occupied by humans and domestic animals.

### 2.1 Nutrition and Development

Virtually any environment rich in decaying organic matter harbors a diverse bacterial community and becomes a suitable substrate for development of muscoid flies, such as house flies (*Musca domestica*), stable flies (*Stomoxys calcitrans*), horn flies (*Haematobia irritans*), and face flies (*Musca autumnalis*) [4]. The primary larval developmental sites

for these flies include animal feces/manure and other decaying organic material (human garbage and compost).

The importance of bacteria in the development of muscoid flies has been reported in several studies that show that a live bacterial community is essential for the larval development of these flies. The nature of this symbiosis is unclear. The significance of bacteria for the development of larvae has been examined for house flies [5–7], stable flies [8, 9], horn flies [10], and face flies [11]. Digestibility of bacteria in the intestinal tract was demonstrated in house flies [12], stable flies [13], and blow flies [14, 15]. Other studies of morphological and physiological adaptations of muscoid flies for uptake, storage, and digestion of bacteria also emphasized the importance of bacteria in larval development [12, 16]. In addition, it has been demonstrated that the same bacteria that support the development of stable fly larvae also stimulate oviposition (egg laying) on the specific substrate and therefore indicate the suitability of the substrate for offspring development [9]. Studies on house flies and stable flies have demonstrated that bacteria in the larval gut can survive pupation and can colonize the digestive tract of newly emerged adult flies [17, 18]. This important finding supports the idea that adult muscoid flies serve as vectors of human and animal pathogenic bacterial strains.

Fruit flies do not require bacteria to successfully complete development; however, it has been shown that exogenous bacteria enhance the lifespan of *Drosophila melanogaster*, especially during the first week of adult life [19]; however, a more recent study did not confirm these results [20].

### 2.2 Dissemination of Pathogens and Antibiotic Resistant Strains

House flies and other muscoid (filth) flies are pests of great medical and veterinary significance [21]. House flies are important nuisance pests of domestic animals and people, as well as the main fly vectors of foodborne and animal pathogens [21–23]. Due to their indiscriminate movements, ability to fly long distances, and attraction to both decaying organic materials and places where food is prepared and stored, house flies greatly amplify the risk of human exposure to foodborne pathogens. House flies can transport microbial pathogens from reservoirs (animal manure) where they present a minimal hazard to people to places where they pose a great risk (food) [21, 22]. Stable flies are bloodsucking insects and important pests of domestic animals and people. Stable flies cause great economic losses in the animal industry, primarily in dairy and beef production [24, 25], and they can also play a role in ecology of various bacteria originating from animal manure and other larval developmental habitats [18]. The potential of adult house flies to transmit pathogens such as *Yersinia pseudotuberculosis* [26, 27], *Helicobacter pylori* [28], *Campylobacter jejuni* [29], *Escherichia coli* O157:H7 [30–32], *Salmonella* spp. [33], and *Aeromonas caviae* [34] has been also reported. Recently, it has been demonstrated that house flies are capable of transmitting *E. coli* O157:H7 to cattle, the major reservoir of this human foodborne pathogen [35]. Fruit flies, primarily the Mediterranean fruit fly (*Ceratitis capitata*) and the vinegar fruit fly (*D. melanogaster*), were also reported as potentially competent vectors for *E. coli* O157:H7 and were capable of contaminating fruits with this pathogen under laboratory conditions [36, 37].

Several studies reported a direct positive correlation between the incidence of foodborne diarrheal diseases and the density of fly populations. For example, suppression of flies in a military camp in the Persian Gulf region resulted in an 85% decrease in shigellosis and a 42% reduction in the incidence of other diarrheal diseases [38]. Esrey [39]

reported a 40% reduction of incidence of diarrheal infections in children after suppression of the fly population.

Additionally, the development of antibiotic resistance among clinical bacterial isolates and commensal bacteria of people and animals, as well as bacteria in other habitats, raises a concern that flies may be vector competent not only for specific pathogens but also for nonpathogenic bacteria carrying antibiotic resistance genes. A recent study reported that the majority of house flies collected from fast-food restaurants in the United States carried a large population of antibiotic resistant and potentially virulent *Enterococci*, primarily *Enterococcus faecalis*. The resistance genes were present on mobile genetic elements (plasmids, transposons) with a broad host range [40] that could be potentially transferred by horizontal gene transfer to more pathogenic strains. Additionally, it has been shown that ready-to-eat food in fast-food restaurants is more frequently contaminated by *E. faecalis* and *Enterococcus faecium* in summer months when house flies are more common in restaurants than in winter months [41], indirectly implicating house flies as a potential source of the contamination.

### 2.3 Homeland Security Aspects

It is becoming more apparent that muscoid flies, primarily house flies, and some species of fruit flies have the potential to play an important role in the dissemination of foodborne pathogens in both agricultural and urban environments. Consequently, both preharvest and postharvest food safety strategies will have to include the insect pest management approach. Unfortunately, the current mind set of many farmers and animal production managers is to tolerate insects such as house flies (and other pests that do not have direct and obvious economic impact on animal production) unless residents from surrounding urban sites complain about fly or other insect infestation problems.

House flies and fruit flies can be easily reared in large numbers in laboratory colonies and could be intentionally contaminated on the surface and in the digestive tract by various bacteria, including foodborne pathogens such *E. coli* O157:H7, *Salmonella* spp., and *Campylobacter* spp. Although muscoid flies and fruit flies have been shown to carry these bacteria in nature and have potential to contaminate the surfaces and food they feed on, the relatively short life span of these flies (up to 2–3 weeks) probably does not represent a viable prospect for domestic or international bioterrorist attack that would have serious consequences on a large scale. However, the AIM = F (anticipate, inform, mitigate equals frustrate) strategy has to be ready for this scenario because the typical integrated pest management (lPM) approach would be too slow to protect the public. Immediate quarantine and insecticide measures will have to be in place and ready to be implemented for such situations.

## 3 COCKROACHES

### 3.1 Nutrition and Development

Cockroaches (Blattaria, Dictyoptera) of many species are widely distributed in the natural world, but only a relatively few species have adapted to life within manmade structures or to the habit of frequently invading such structures from the outdoors [42, 43]. Foraging for food generally occurs at night. Cockroaches typically retire to dark, sheltered niches during the hours of daylight. Gradual metamorphosis being the rule in the Blattaria, nymphs

emerging from eggs lack wings and functional reproductive organs, but otherwise they are similar to the adult stage except for being smaller in size. All postegg stages have chewing mouthparts and all utilize similar kinds of food. They are omnivores; virtually any organic material, of either plant or animal origin and either solid or liquid, can be ingested.

Domestic cockroaches tend to require a daily ration of water. This may be supplied as liquid water, as in a floor drain or a puddle under leaky plumbing, or in the form of moist food (anything from food on a hospital food cart to rotting kitchen waste in a garbage can). Moisture, as well as food, may be acquired by ingesting human or animal feces, vomitus, blood, and pus on discarded wound dressings, and moist pet food, to name a few sources. When it comes to food and drink, cockroaches take whatever they can get wherever they can get it. This is where the problem arises for human and animal health: Like flies, cockroaches visit feces (and many other contaminated substrates) and food (that is, edible human or animal food) indiscriminately and their movements from one to the other may contaminate food-contact surfaces.

### 3.2 Dissemination of Pathogens

The cockroach gut is home to a bewildering array of naturally occurring bacteria, most of which are harmless to people and domestic animals [44–46]. But in their visits to substrates laden with pathogens, their exterior surfaces, especially the legs, become laden with pathogenic bacteria. Moreover, they can ingest pathogens, some of which may survive in the gut long enough to be egested with the fecal pellets or, occasionally, regurgitated during feeding. Thus, both clean surfaces and clean food may become contaminated.

Although some doubt about the importance of cockroaches as vectors of foodborne pathogens has been expressed [47], the larger body of published research, some of which is noted here, suggests that cockroaches should be given serious consideration by the public and by the guardians of the public's health. Concern over the role of flies, cockroaches, and ants as potential vectors of microbes pathogenic to humans and animals dates at least from very early in the 1900s and this concern is reflected in the many dozens of scientific papers published during the past century. There is much to be learned from these older papers; many of them are cited in more recent papers and several of them are appended in "Further Reading". For this section on cockroaches, we will bring to the reader's attention a few investigative reports published since the turn of the present century.

The essential thrust of these papers is that pathogens and cockroaches are intimately and consistently associated, a conclusion derived from multiple isolations of pathogens from cockroaches collected in places, such as hospitals and kitchens, generally perceived to be sanitary and sanitized. Cockroaches and their associated pathogens might be implicated in some way, either by direct contact with people (or domestic animals), or by contact with food or food-contact surfaces, is a premise supported by the observations that specific disease outbreaks waned when standard infection control procedures were complemented by elimination of cockroaches [48, 49]. None of these reports conclusively proves that the cockroach committed the "crime," but the correlation of the specific strain of the pathogen taken from the cockroach with the same specific strain taken from the sick patient seems to us to be very compelling circumstantial evidence implicating the cockroach. The authors of virtually every scientific paper on this subject published since 1900 have come to this understanding.

Two other factors add weight to the premise that cockroaches and food (or food-contact surfaces) should not coincide: (i) some strains of pathogens exhibit enhanced virulence, that is, even an immunologically competent host may be susceptible to a much lower than usual infective dose; and (ii) immunocompromised hosts are, of course, susceptible to the supervirulent strains and to lower than usual infective doses of the standard pathogenic strains.

All agree that the cornerstone of personal and community hygiene is hand-washing. Countless incidents of foodborne disease and nosocomial infections have been traced back to a simple behavioral flaw: hand-washing was omitted or done ineffectively. People can be trained to more consistently and effectively wash their hands. Although flies, ants and cockroaches engage in a lot of self-grooming, a behavior vaguely comparable to hand-washing, this does not render them clean in the microbiological sense, as has been graphically demonstrated in at least one instance for cockroaches [50].

We offer here a partial list of pathogens isolated from various species of common domestic cockroaches (locality information, given only after first mention of a given reference, is stated after the reference number); many other pathogen isolation reports may be found in the extensive literature on this subject [51]. Although the status of each of the several pathogens with regard to antibiotic resistance, a very common phenomenon, may be of special interest to clinicians, this information is omitted here because the matter does not seem essential to the purposes of this article.

*Aeromonas* [52 (Libya); 53 (Nigeria)]; *Bacillus* sp. [54 (Botswana)]; *Citrobacter freundii* [53, 55 (Thailand)]; *Enterobacter aerogenes* [56 (Brazil)]; *Enterobacter cloacae* [53, 55, 56]]; *Enterobacter gergoviae* [56]; *Enterobacter* sp. [52, 54]; *Erwinia* sp. [54]; *E. coli* [[53–55] 57 (Taiwan)]: *Hafnia alvei* [56]; *Klebsiella pneumoniae* [48 (South Africa); [53, 55, 56]]; *Klebsiella* sp. [52, 54]; *Mycobacteria* [58 (Taiwan)]; *Proteus mirabilis* [53]; *Proteus* sp. [57]; *Proteus vulgaris* [53]; *Pseudomonas aeruginosa* [53, 57]; *Pseudomonas* sp. [54]; *Salmonella* sp. [53, 54]; *Serratia marcescens* [53, 56, 57]; *Serratia* sp. [52, 54, 56]; *Shigella* sp. [54]; *Staphylococci* (Gram neg.) [56]; *Staphylococcus aureus* [53, 57]; *Staphylococcus epidermidis* [53]; *Staphylococcus* sp. [54]; *Streptococcus faecalis* [53]; *Streptococcus* sp. [52]; *Alternaria* sp. [59 (Brazil)]; *Aspergillus flavus* [54]; *Aspergillus fumigatus* [54]; *Aspergillus parasiticus* [54]; *Aspergillus* sp. [59]; *Candida* sp. [53, 54, 59]; filamentous fungi [56]; *Penicillium* sp. [59]; yeast [56]; *Ballantidium coli* [53]; *Cryptosporidium parvum* [53]; *Entamoeba histolytica* [60 (Taiwan)]; *Ancylostoma duodenale* [53]; *Ascaris lumbricoides* [53]; *Enterobius vermicularis* [53]; *Strongyloides stercoralis* [53]; *Trichuris trichiura* [53].

### 3.3 Homeland Security Aspects

Our primary concern here is to keep our citizens healthy and productive by ensuring that their food is safe to eat. One of the many ways to do that is to prevent the convergence of food and cockroaches, a convergence that is still much too common.

Several species of domestic cockroaches, especially *Blattella germanica* (Blattellidae), *Blatta orientalis* (Blattidae), and *Periplaneta americana* (Blattidae), can be easily reared in huge numbers in the laboratory and are easily contaminated, either superficially or internally, with certain pathogens (such as avian influenza virus, SARS virus, foot-and-mouth disease virus, *E. coli* O157:H7, to name a few) that may cause disease in humans or in domestic animals (and then, in the latter case, may secondarily cause disease in humans). Cockroaches, upon their release from the rearing environment, typically

first seek shelter. As the light of day wanes, the cockroaches will venture forth in search for moisture. Some fall into and drown in the water supplies that serve the chickens, cows, or pigs, inadvertently releasing their burden of pathogens. Others are eaten by pigs or chickens or accidentally ingested by cows as they feed nose-to-nose with the cockroaches. Others seek out the darkness and moisture of the beverage and ice machines in the school, restaurant or company cafeteria. Again, pathogens are deposited on surfaces presumed to be clean. Whether this shotgun type of dissemination will result in human or animal disease, no one can predict. But the level of probability for that eventuality seems to be at least somewhat higher than what might occur during the normal course of farm and food service operations.

Now is the time for the AIM = F strategy to pay off. Thanks to the "A," our farmers, ranchers, factory managers, food service personnel, and school administrators are aware of the inventory of unfriendly interventions that might occur; they have been "I" (Informed) on how to recognize the signs of enemy interventions; they know that IPM is an effective form of "M" (Mitigation); and the combination of AIM results in the "F" (Frustration) of this assault on the public's health. In the bioterrorism scenario, it may not be feasible to wait for the slower pest control measures that are typical of the usual lPM approach. Immediate and thorough application of insecticides and immediate quarantine measures may be essential to quell an obvious threat; protocols for these interventions should be in place, practiced and ready for implementation.

## 4 ANTS

### 4.1 Nutrition and Development

Ants (*Formicidae*, Hymenoptera) are social insects, that is, they live in colonies, each colony responding to the control of (usually) only one queen. The worker ants are females. They are the ones that leave the nest and venture out on food-finding expeditions. Colony size varies greatly according to species and within species. Some are enormous, with thousands of workers; others, only a few dozen. Unlike the cockroaches, ants go through a complete metamorphosis—egg, larva, pupa, adult; but like cockroaches, most kinds of ants live in the natural world; only a relatively few species either nest in manmade structures or routinely forage within such structures [61, 62].

Structure-invading ants are omnivores. The animal proteins and fats in their diet are derived mostly from insects and other arthropods that fall prey to the foraging worker ants. Sugars and starches or foods containing those carbohydrates are often very attractive to ants. Kitchens, bakeries, restaurants, and food factories are typical venues where ants collect a variety of foods that are then held in their chewing mouthparts and transported to the home nest to become essential nutrients for the queen and her brood of larvae. Hospitals too, are often visited. Besides the usual floor feasts of bread crumbs, sugar granules, and fat droplets, ants, especially the pharaoh ant, *Monomorium pharaonis*, may annoy patients by nibbling on food around a patient's mouth; they also feed on exposed pus and dried blood, or they may be found on patient food trays. These ants (*M. pharaonis*) have been found in IV drips and inside packages of sterile dressings [63, 64]. Water is essential and this may be obtained from any exposed source such as floor drains, urinals, patient water flasks, unemptied bedpans, wound dressings, ice machines, plumbing drips, and so forth.

### 4.2 Dissemination of Pathogens

Like cockroaches, ants harbor many kinds of internal bacteria [65, 66], but, with a few exceptions, only the external surfaces, mainly the legs and mandibles, are of concern here [1, 67–69]. These appendages come into contact with substrates, such as the soil and pit latrines outdoors and, most commonly, floors indoors, from which the ants may pick up pathogens. As the ants forage over clean surfaces, such as dishes or cutting boards, or food conveyors in a factory, pathogens may be deposited and eventually become mixed in with a food destined, without a subsequent heat treatment, for human or animal consumption. Ants as pests in hospitals have been reported many times [70–74].

We offer here a partial list of pathogens isolated from various species of common pest ants (locality information, given only after first mention of a given reference, is stated after the reference number); other pathogen isolation reports may be found in the literature on this subject.

*Bacillus cereus* [70 (England)]; bacteria (Gram +) [72 (Brazil)]; *Clostridium perfringens* [70]; *E. coli* [70]; filamentous fungi [72]; *K. pneumoniae* [71 (Trinidad)]; *Micrococcus* sp. [72]; *P. mirabilis* [71]; *Pseudomonas* sp. [71]; *Salmonella* sp. [70]; *S. aureus* [70]; *Staphylococcus* sp. [72]; *Streptococcus pyogenes* [70].

### 4.3 Homeland Security Aspects

Although ants are good candidates for the role of accidental mechanical vectors of pathogens, they are poor candidates as pawns in an act of intentional food contamination. The principal homeland security concern here coincides with the universal objective of operating hospitals and food service facilities, including the home kitchen, in such a sanitized manner that food offered for human consumption is safe to eat, that is, at least it and the surfaces it has touched have been protected from exposure to the pathogens that ants and cockroaches are known to carry.

## 5 PANTRY PESTS

### 5.1 Nutrition and Development

The moths (Lepidoptera) and beetles (Coleoptera) that infest grains, flour, nuts, chocolate, dry dog food, and cereals in the kitchen storage cabinet are referred to as *pantry pests*. They are found in home kitchens, of course, but also in grain storage elevators, huge ships that transport grains, bakeries, restaurants, chicken ranches, dairy barns, food factories, food warehouses, transport trucks, and many other venues both large and small. The pantry pests noted here are holometabolous, that is, their life stages are egg, larva, pupa, and adult. The larva has chewing mouthparts; it is the stage that does the bulk of the feeding and the bulk of the damage to commodities.

### 5.2 Dissemination of Pathogens

Compared to ants and cockroaches, pantry pests are relatively free of pathogens that cause human or animal diseases. They do not usually get out into those venues where bacterial pathogens are common. Unfortunately, they often do not long remain free of pathogens [75] or spoilage organisms [76]. This is because their food sources, in which they live throughout their entire lives, are visited by those pests that commonly visit

pathogen-laden substrates. Cockroaches, ants, flies, rats, and mice bring pathogens to the home territory of the pantry pests. The latter, then, quite inadvertently spread these pathogens here and there as they move about within their food material [77].

The situation is quite different with regard to spoilage molds. The spores of these fungi are ubiquitous; they are produced most abundantly from grain substrates that are damp and deteriorating, that is, "out of condition." Grain spoilage represents economic loss; that explains why managers of grain storages, whether for bulk commodities or retail packages, go to great lengths to maintain a dry environment for these products. But beyond the economic consideration, moldy grain can become a health hazard for both people and domestic animals when certain fungi of deterioration produce aflatoxins.

### 5.3 Homeland Security Aspects

Our concerns here are similar to those faced with ants. The primary goal is to keep susceptible products—nuts, grains, beans, coffee beans, peanuts, and so forth—free of pantry pests, the objective being to produce end-product foods that are safe for human and animal consumption. Generally speaking, the better the storage conditions, the less likely that pantry pests will become established and the less likely that spoilage molds and aflatoxin-producing fungi will proliferate in the commodity. Pantry pests spread the spores of the aflatoxin-producing fungi [78, 79] through the commodity just as they do the spores of common spoilage molds.

Several kinds of pest beetles are easy to cultivate in very large numbers. It would be a simple matter to superficially contaminate adult beetles with some pathogen and release them at a vulnerable location. The sudden increase in the population of a pest around or within a food facility would be the signal to implement AIM = F, with emphasis on immediate, focused insecticidal treatment of the affected facility.

## REFERENCES

1. Gorham, J. R. (1991). Food pests as disease vectors. In *Ecology and Management of Food-industry Pests*, FDA Tech Bull 4, J. R. Gorham, Ed. AOAC International, Arlington, VA, pp. 477–482.
2. Hui, Y. H., Nip, W.-K., and Gorham, J. R. (2003). Sanitation and warehousing. In *Food Plant Sanitation*, Y. H. Hui, B. L. Bruinsma, J. R. Gorham, W.-K. Nip, P. S. Tong, and P. Ventresca, Eds. Marcel Dekker, New York, pp. 373–389.
3. Stanfield, P. (2006). FDA's GMPs, HACCP, and the food code. In *Handbook of Food Science, Technology, and Engineering*, Y. H. Hui, Ed. Vol. **2**, CRC Taylor & Francis, Boca Raton, FL, pp. 73.1–73.14.
4. Spiller, D. (1964). Nutrition and diet of muscoid flies. *Bull. World Health Organ.* **341**, 551–554.
5. Schmidtmann, E. T., and Martin, P. A. W. (1992). Relationship between selected bacteria and the growth of immature house flies, *Musca domestica*, in an axenic test system. *J. Med. Entomol.* **29**, 232–235.
6. Watson, D. W., Martin, P. A. W., and Schmidtmann, E. T. (1993). Egg yolk and bacteria growth medium for *Musca domestica* (Diptera: Muscidae). *J. Med. Entomol.* **30**, 820–823.
7. Zurek, L., Schal, C., and Watson, D. W. (2000). Diversity and contribution of the intestinal bacterial community to the development of *Musca domestica* (Diptera: Muscidae) larvae. *J. Med. Entomol.* **37**(6), 924–928.

8. Lysyk, T. J., Kalischuk-Tymensen, L., Selinger, L. B., Lancaster, R. C., Wever, L., and Cheng, K.-J. (1999). Rearing stable flies larvae (Diptera: Muscidae) on an egg yolk medium. *J. Med. Entomol.* **36**, 382–388.
9. Romero, A., Broce, A., and Zurek, L. (2006). Role of bacteria in the oviposition behavior and larval development of stable flies. *Med. Vet. Entomol.* **20**(1), 115–121.
10. Perotti, M. A., Lysyk, T. J., Kalischuk-Tymensen, L. D., Yanke, L. J., and Selinger, L. B. (2001). Growth and survival of immature *Haematobia irritans* (Diptera: Muscidae) is influenced by bacteria isolated from cattle manure and conspecific larvae. *J. Med. Entomol.* **38**(2), 180–187.
11. Hollis, J. H., Knapp, F. W., and Dawson, K. A. (1985). Influence of bacteria within bovine feces on the development of the face fly (Diptera: Muscidae). *Environ. Entomol.* **14**, 568–571.
12. Espinosa-Fuentes, F. P., and Terra, W. R. (1987). Physiological adaptations for digestion bacteria. Water fluxes and distribution of digestive enzymes in *Musca domestica* larval midgut. *Insect. Biochem.* **17**, 809–817.
13. Rochon, K., Lysyk, T. J., and Selinger, L. B. (2004). Persistence of *Escherichia coli* in immature house fly and stable fly (Diptera: Muscidae) in relation to larval growth and survival. *J. Med. Entomol.* **41**(6), 1082–1089.
14. Greenberg, B. (1968). Model for destruction of bacteria in the midgut of blow fly maggots. *J. Med. Entomol.* **5**, 31–38.
15. Mumcuoglu, K. Y., Miller, J., Mumcuoglu, M., Friger, M., and Tarshis, M. (2001). Destruction of bacteria in the digestive tract of the maggot of *Lucilia sericata* (Diptera: Calliphoridae). *J. Med. Entomol.* **38**(2), 161–166.
16. Dowding, V. M. (1967). The function and ecological significance of the pharyngeal ridges occurring in the larvae of some cyclorrhaphous Diptera. *Parasitology* **57**, 371–388.
17. Greenberg, B. (1959). Persistence of bacteria in the developmental stages of the housefly.4. Infectivity of the newly emerged adult. *Am. J. Trop. Med. Hyg.* **8**(6), 618–622.
18. Rochon, K., Lysyk, T. J., and Selinger, L. B. (2005). Retention of *Escherichia coli* by house fly and stable fly (Diptera: Muscidae) during pupal metamorphosis and eclosion. *J. Med. Entomol.* **42**(3), 397–403.
19. Brummel, T., Ching, A., Seroude, L., Simon, A. F., and Benzer, S. (2004). Drosophila lifespan enhancement by exogenous bacteria. *Proc. Natl. Acad. Sci. U.S.A.* **101**(35), 12974–12979.
20. Ren, C., Webster, P., Finkel, S. E., and Tower, J. (2007). Increased internal and external bacterial load during *Drosophila* aging without life-span trade-off. *Cell Metab.* **6**(2), 144–152.
21. Olsen, A. R. (1998). Regulatory action criteria for filth and other extraneous materials III. Review of flies and foodborne enteric disease. *Regul. Toxicol. Pharm.* **28**(3), 199–211.
22. Greenberg, B. (1971). *Flies and Diseases*, Princeton University Press, Princeton, NJ.
23. Graczyk, T. K., Knight, R., Gilman, R. H., and Cranfield, M. R. (2001). The role of non-biting flies in the epidemiology of human infectious diseases. *Microbes Infect.* **3**(3), 231–235.
24. Campbell, J. B., Berry, I. L., Boxler, D. J., Davis, R. L., Clanton, D. C., and Deutscher, G. H. (1987). Effects of stable flies (Diptera: Muscidae) on weight gain and feed efficiency of feedlot cattle. *J. Econ. Entomol.* **80**, 117–119.
25. Campbell, J. B., Skoda, S. R., Berkebile, D. R., Boxler, D. J., Thomas, G. D., Adams, D. C., and Davis, R. (2001). Effects of stable flies (Diptera: Muscidae) on weight gains of grazing yearling cattle. *J. Econ. Entomol.* **94**(3), 780–783.
26. Fukushima, H., Tsubokura, M., Otsuki, K., and Kawaoka, Y. (1984). Biochemical heterogeneity of serotype 03 strains of 700 *Yersinia* strains isolated from humans, other mammals, flies, animal feed, and river water. *Curr. Microbiol.* **11**, 149–154.
27. Zurek, L., Denning, S. S., Schal, C., and Watson, D. W. (2001). Vector competence of *Musca domestica* (Diptera: Muscidae) for *Yersinia pseudotuberculosis*. *J. Med. Entomol.* **38**(2), 333–335.

28. Grubel, P., Hoffman, J. S., Chong, F. K., Burstein, N. E., Mepani, C., and Cave, D. R. (1997). Vector potential of houseflies (*Musca domestica*) for *Helicobacter pylori*. *J. Clin. Microbiol.* **35**, 1300–1303.

29. Shane, S. M., Montrose, M. S., and Harrington, K. S. (1985). Transmission of *Campylobacter jejuni* by the housefly (*Musca domestica*). *Avian Dis.* **29**(2), 384–391.

30. Kobayashi, M., Sasaki, T., Saito, N., Tamura, K., Suzuki, K., Watanabe, H., and Agui, N. (1999). Houseflies: not simple mechanical vectors of enterohemorrhagic *Escherichia coli* O157: H7. *Am. J. Trop. Med. Hyg.* **61**(4), 625–629.

31. Moriya, K., Fujibayashi, T., Yoshihara, T., Matsuda, A., Sumi, N., Umezaki, N., Kurahashi, H., Agui, N., Wada, A., and Watanabe, H. (1999). Verotoxin-producing *Escherichia coli* O157: H7 carried by the housefly in Japan. *Med. Vet. Entomol.* **13**(2), 214–216.

32. Sasaki, T., Kobayashi, M., and Agui, N. (2000). Epidemiological potential of excretion and regurgitation by *Musca domestica* (Diptera: Muscidae) in the dissemination of *Escherichia coli* O157: H7 to food. *J. Med. Entomol.* **37**(6), 945–949.

33. Mian, L. S., Maag, H., and Tacal, J. V. (2002). Isolation of Salmonella from muscoid flies at commercial animal establishments in San Bernardino County, California. *J. Vector Ecol.* **27**(1), 82–85.

34. Nayduch, D., Noblet, G. P., and Stutzenberger, F. J. (2002). Vector potential of houseflies for the bacterium *Aeromonas caviae*. *Med. Vet. Entomol.* **16**(2), 193–198.

35. Ahmad, A., Nagaraja, T. G., and Zurek, L. (2007). Transmission of *Escherichia coli* O157: H7 to cattle by house flies. *Prev. Vet. Med.* **80**(1), 74–81.

36. Janisiewicz, W. J., Conway, W. S., Brown, M. W., Sapers, G. M., Fratamico, P., and Buchanan, R. L. (1999). Fate of *Escherichia coli* 0157: H7 on fresh-cut apple tissue and its potential for transmission by fruit flies. *Appl. Environ. Microbiol.* **65**(1), 1–5.

37. Sela, S., Nestel, D., Pinto, R., Nemny-Lavy, E., and Bar-Joseph, M. (2005). Mediterranean fruit fly as a potential vector of bacterial pathogens. *Appl. Environ. Microbiol.* **71**(7), 4052–4056.

38. Cohen, D., Green, M., Block, C., Slepon, R., Ambar, R., Wasserman, S. S., and Levine, M. M. (1991). Reduction of transmission of shigellosis by control of houseflies (*Musca domestica*). *Lancet* **337**(8748), 993–997.

39. Esrey, S. A. (1991). *Interventions for the Control of Diarrhoeal Diseases Among Young Children: Fly Control*, World Health Organization, Geneva, Published document WHO/CDD/91.37.

40. Macovei, L., and Zurek, L. (2006). Ecology of antibiotic resistance genes: characterization of enterococci from houseflies collected in food settings. *Appl. Environ. Microbiol.* **72**(6), 4028–4035.

41. Macovei, L., and Zurek, L. (2007). Influx of enterococci and associated antibiotic resistance and virulence genes from ready-to-eat food to the human digestive tract. *Appl. Environ. Microbiol.* **73**(21), 6740–6747.

42. Gurney, A. B., Fisk, F. W. (1991). Cockroaches. In *Agriculture Handbook 655*, *Insect and Mite Pests in Food: An Illustrated Key*, J. R. Gorham, Ed. Superintendent of Documents, U. S. Government Printing Office, Washington, DC, pp. 45–74, 527–544.

43. Robinson, W. H. (2005). *Urban Insects and Arachnids*, Cambridge University Press, Cambridge.

44. Bracke, J. W., Cruden, D. L., and Markovetz, A. J. (1979). Intestinal microbial flora of the American cockroach, *periplaneta American L. Appl. Environ. Microbiol.* **38**(5), 945–955.

45. Cruden, D. L., and Markovetz, A. J. (1987). Microbial ecology of the cockroach gut. *Annu. Rev. Microbiol.* **41**, 617–643.

46. Roth, L. M., and Willis, E. R. (1960). The biotic associations of cockroaches. *Smithson Misc. Coll.* **141**, 1–470.
47. Bennett, G. (1993). Cockroaches as carriers of bacteria. *Lancet* **341**(8847), 732.
48. Cotton, M. F., Wasserman, E., Pieper, C. H., Theron, D. C., van Tubbergh, D., Campbell, G., Fang, F. C., and Barnes, J. (2000). Invasive disease due to extended spectrum beta-lactamase-producing *Klebsiella pneumoniae* in a neonatal unit: the possible role of cockroaches. *J. Hosp. Infect.* **44**(1), 13–17.
49. Graffar, M., and Mertens, S. (1950). Le rôle des blattes dans la transmission des salmonelloses. *Ann. Inst. Pasteur* **79**, 654–660.
50. Gazivoda, P., and Fish, D. (1985). Scanning electron microscope demonstration of bacteria on the tarsi of *Blattella germanica*. *J. N. Y. Entomol. Soc.* **93**, 1064–1067.
51. Roth, L. M., and Willis, E. R. (1957). The medical importance of cockroaches. *Smithson Misc. Coll.* **134**(10), 1–147.
52. Elgderi, R. M., Ghenghesh, K. S., and Berbash, N. (2006). Carriage by the German cockroach (*Blattella germanica*) of multiple-antibiotic-resistant bacteria that are potentially pathogenic to humans, in hospitals and households in Tripoli, Libya. *Ann. Trop. Med. Parasitol.* **100**(1), 55–62.
53. Tatfeng, Y. M., Usuanlele, M. U., Orukpe, A., Digban, A. K., Okodua, M., Oviasogie, F., and Turay, A. A. (2005). Mechanical transmission of pathogenic organisms: the role of cockroaches. *J. Vector Borne Dis.* **42**(4), 129–134.
54. Mpuchane, S., Allotey, J., Matsheka, I., Simpanya, M., Coetzee, S., Jordaan, A., Mrema, N., and Gashe, B. A. (2006). Carriage of micro-organisms by domestic cockroaches and implications for food safety. *Int. J. Trop. Insect. Sci.* **26**, 166–175.
55. Chaichanawongsaroj, N., Vanichayatanarak, K., Pipatkullachat, T., Poirojpanya, M., and Somkiatcharoen, S. (2004). Isolation of gram-negative bacteria from cockroaches trapped from urban environment. *Southeast Asian J. Trop. Med. Public Health* **35**(3), 681–684.
56. Prado, M. A., Gir, E., Pereira, M. S., Reis, C., and Pimenta, F. C. (2006). Profile of antimicrobial resistance of bacteria isolated from cockroaches (*Periplaneta Americana*) in a Brazilian health care institution. *Braz. J. Infect. Dis.* **10**(1), 26–32.
57. Pai, H.-H., Chen, W. C., and Peng, C. F. (2004). Cockroaches as potential vectors of nosocomial infections. *Infect. Control Hosp. Epidemiol.* **25**(11), 979–984.
58. Pai, H.-H., Chen, W. C., and Peng, C. F. (2003). Isolation of non-tuberculous mycobacteria from hospital cockroaches (*Periplaneta Americana*). *J. Hosp. Infect.* **53**, 224–228.
59. Lemos, A. A., Lemos, M. A., Prado, M. A., Pimenta, F. C., Gir, E., Silva, H. M., and Silva, M. R. R. (2006). Cockroaches as carriers of fungi of medical importance. *Mycoses* **49**(1), 23–25.
60. Pai, H.-H., Ko, Y. C., and Chen, E. R. (2003). Cockroaches (*Periplaneta Americana* and *Blattella germanica*) as potential mechanical disseminators of *Entamoeba histolytica*. *Acta Trop.* **87**(3), 355–359.
61. Smith, D. R. (1991). Ants (Formicidae, Hymenoptera). In *Agriculture Handbook 655*, *Insect and Mite Pests in Food: An Illustrated Key*, J. R. Gorham, Ed. Superintendent of Documents, U. S. Government Printing Office, Washington, DC, pp. 297–309, 633–649.
62. Smith, M. R. (1965). *House-infesting Ants of Eastern United States*, Technical Bulletin 1326, U. S. Department of Agriculture, Washington, DC.
63. Beatson, S. (1973). Pharaoh's ants enter giving sets. *Lancet* **1**(7803), 606.
64. Cartwright, R. Y., and Clifford, C. M. (1973). Pharaoh's ants. *Lancet* **2**(7843), 1455–1456.
65. Boursaux-Eude, C., and Gross, R. (2000). New insights into symbiotic associations between ants and bacteria. *Res. Microbiol.* **151**(7), 513–519.

66. Zientz, E., Feldhaar, H., Stoll, S., and Gross, R. (2005). Insights into the microbial world associated with ants. *Arch. Microbiol.* **184**, 199–206.
67. Hughes, D. E., Kassim, O. O., Gregory, J., Stupart, M., Austin, I., and Duffield, R. (1989). Spectrum of bacterial pathogens transmitted by Pharaoh's ants. *Lab. Anim. Sci.* **39**(2), 167–168.
68. Ipinza-Regla, J., Figueroa, G., and Moreno, I. (1984). *Iridomyrmex humilis* (Formicidae) y su papel como possible vector de contaminación microbiana en industrias de alimentos. *Folia Entomol. Mex.* **62**, 111–124.
69. de Zarzuela, M. F. M., Campos-Farinha, A. E. C., and Peçanha, M. P. (2005). Evaluation of urban ants (Hymenoptera: Formicidae) as carriers of pathogens in residential and industrial environments. *Sociobiology* **45**(1), 9–14.
70. Beatson, S. H. (1972). Pharaoh's ants as pathogen vectors in hospitals. *Lancet* **1**(7747), 425–427.
71. Chadee, D. D., and Le Maitre, A. (1990). Ants: potential mechanical vectors of hospital infections in Trinidad. *Trans. R. Soc. Trop. Med. Hyg.* **84**, 297.
72. da Costa, S. B., Pelli, A., de Carvalho, G. P., Oliveira, A. G., da Silva, P. R., Teixeira, M. M., Martins, E., Terra, A. P. S., Resende, E. M., Hueb, C. C., de Oliveira, B., and de Morais, C. A. (2006). Ants as mechanical vectors of microorganisms in the school hospital of the universidade federal do Triângulo Mineiro. *Rev. Soc. Bras. Med. Trop.* **39**(6), 527–529.
73. Edwards, J. P., and Baker, L. F. (1981). Distribution and importance of the Pharaoh's ant *Monomorium pharaonis* (L.) in National Health Service Hospitals in England. *J. Hosp. Infect.* **2**(3), 249–254.
74. Fowler, H. G., Bueno, O. C., Sadatsune, T., and Montelli, A. C. (1993). Ants as potential vectors of pathogens in hospitals in the State of São Paulo, Brazil. *Insect Sci. Appl.* **14**, 367–370.
75. Harein, P. K., and De Las Casas, E. (1968). Bacteria from granary weevils collected from laboratory colonies and field infestations. *J. Econ. Entomol.* **61**(6), 1719–1720.
76. Dunkel, F. V. (1988). The relationship of insects to the deterioration of stored grain by fungi. *Int. J. Food Microbiol.* **7**, 227–244.
77. Husted, S. R., Mills, R. B., Foltz, V. D., and Crumrine, M. H. (1969). Transmission of *Salmonella montevideo* from contaminated to clean wheat by the rice weevil. *J. Econ. Entomol.* **62**(6), 1489–1491.
78. Eugenio, C., De Las Casas, E., Harein, P. K., and Mirocha, C. J. (1970). Detection of the mycotoxin F-2 in the confused flour beetle and the lesser mealworm. *J. Econ. Entomol.* **63**(2), 412–415.
79. Pande, N., and Mehrotra, B. S. (1988). Rice weevil (*Sitophilus oryzae* Linn.): vector of toxigenic fungi. *Nat. Acad. Sci. Lett. (India)* **11**, 3–4.

## FURTHER READING

Agbodaze, D., and Owusu, S. B. (1989). Cockroaches (*Periplaneta Americana*) as carriers of agents of bacterial diarrhoea in Accra, Ghana. *Cent. Afr. J. Med.* **35**(9), 484–486.

Devi, S. J., and Murray, C. J. (1991). Cockroaches (*Blatta* and *Periplaneta* species) as reservoirs of drug-resistant salmonellas. *Epidemiol. Infect.* **107**(2), 357–361.

Foil, L. D., and Gorham, J. R. (2000). Mechanical transmission of disease agents by arthropods. In *Medical Entomology: A Textbook on Public Health and Veterinary Problems Caused by Arthropods*, B. F. Eldridge, and J. D. Edman, Eds. Kluwer Academic Publishers, Dordrecht, pp. 461–514.

Fotedar, R., and Banerjee, U. (1992). Nosocomial fungal infections—study of the possible role of cockroaches (*Blattella germanica*) as vectors. *Acta Trop.* **50**(4), 339–343.

Fotedar, R., Banerjee, U., Samantray, J. C., and Shriniwas, K. (1992). Vector potential of hospital houseflies with special reference to *Klebsiella* species. *Epidemiol. Infect.* **109**(1), 143–147.

Fotedar, R., Nayar, E., Samantray, J. C., Shriniwas, K., Banerjee, U., Dogra, V., and Kumar, A. (1989). Cockroaches as vectors of pathogenic bacteria. *J. Commun. Dis.* **21**, 318–322.

Fotedar, R., Shriniwas, K., Banerjee, U., Sumantray, J. C., Nayar, E., and Verma, A. (1991). Nosocomial infections: cockroaches as possible vectors of drug-resistant *Klebsiella*. *J. Infect.* **18**, 155–159.

Fotedar, R., Shriniwas, K., Banerjee, U., and Verma, A. (1991). Cockroaches (*Blattella germanica*) as carriers of microorganisms of medical importance in hospitals. *Epidemiol. Infect.* **107**, 181–187.

Gorham, J. R. (1981). Filth in foods: implications for health. In *Principles of Food Analysis for Filth, Decomposition and Foreign Matter*, J. R. Gorham, Ed. FDA Technical Bulletin 1, Food and Drug Administration, Washington, DC, pp. 27–32.

Gorham, J. R. (1991). Filth and extraneous matter in food. In *Encyclopedia of Food Science and Technology*, Y. H. Hui, Ed. Wiley-Interscience, New York, pp. 847–868.

Gorham, J. R. (1994). Food, filth, and disease: a review. In *Food-borne Disease Handbook*, Y. H. Hui, J. R. Gorham, K. D. Murrell, and D. O. Cliver, Eds. Marcel Dekker, New York, pp. 627–638.

Gorham, J. R. (1995). Reflections on food-borne filth in relation to human disease. In *Fundamentals of Microanalytical Entomology: A Practical Guide to Detecting and Identifying Filth in Foods*, A. R. Olsen, T. H. Sidebottom, and S. A. Knight, Eds. CRC Press, Boca Raton, FL, pp. 269–275.

Gorham, J. R. (2001). Food, filth, and disease: a review. In *Food-borne Disease Handbook*, Seafood and Environmental Toxins, Vol. **4**, Y. H. Hui, D. Kitts, and P. S. Stanfield, Eds. 2nd ed, Marcel Dekker, New York, pp. 627–637.

Gorham, J. R., Zurek, L. (2006). Filth and other foreign objects in food. In *Handbook of Food Science, Technology, and Engineering*, Y. H. Hui, Ed. Vol. **2**, CRC Press, Boca Raton, FL, pp. 74.1–74.28.

Gratz, N. (2006). *Vector- and Rodent-borne Diseases in Europe and North America*, Cambridge University Press, Cambridge.

Hui, Y. H., Gorham, J. R., Murrell, K. D., and Cliver, D. O., Eds. (1994). *Food-borne Disease Handbook*, *Volume 1, Diseases Caused by Bacteria; Volume 2, Diseases Caused by Viruses, Parasites, and Fungi; Volume 3, Diseases Causes by Hazardous Substances*, Marcel Dekker, New York.

Hui, Y. H., Pierson, M. D., Gorham, J. R., Eds. (2001). *Food-borne Disease Handbook*, Bacterial Pathogens, Vol. **1**, 2nd ed. Marcel Dekker, New York.

Klowden, M. J., and Greenberg, B. (1976). *Salmonella* in the American cockroach: evaluation of vector potential through dosed feeding experiments. *J. Hyg. (Lond)* **77**(1), 105–111.

Klowden, M. J., Greenberg, B. (1977). Effects of antibiotics on the survival of *Salmonella* in the American cockroach. *J. Hyg. (Lond)* **79**, 339–345.

Kopanic, R. J., Sheldon, B. W., and Wright, C. G. (1994). Cockroaches as vectors of *Salmonella*: laboratory and field trials. *J. Food Prot.* **57**(2), 125–132.

Olsen, A. R., Gecan, J. S., Ziobro, G. C., and Bryce, J. R. (2001). Regulatory action criteria for filth and other extraneous materials. V. Strategy for evaluating hazardous and nonhazardous filth. *Regul. Toxicol. Pharm.* **33**, 363–392.

Oothumen, P., Jeffery, J., Aziz, A. H. A., Bakar, E. A., and Jegathesan, M. (1989). Bacterial pathogens isolated from cockroaches trapped from paedriatric ward in peninsular Malaysia. *Trans. R. Soc. Trop. Med. Hyg.* **83**(1), 133–135.

Panhotra, B. R., Agnihortri, V., Agarwal, K. C., and Batta, R. P. (1981). Isolation of salmonellae from hospital food and vermin. *Indian J. Med. Res.* **74**, 648–651.

Rahuma, N., Ghenghesh, K. S., Ben Aissa, R., and Elamaari, A. (2005). Carriage by the housefly (*Musca domestica*) of multiple-antibiotic-resistant bacteria that are potentially pathogenic to humans, in hospital and other urban environments in Misurata, Libya. *Ann. Trop. Med. Parasitol.* **99**(8), 795–802.

Sulaiman, S., Cheon, Y. K., Aziz, A. H., and Jeffery, J. (2003). Isolations of bacteria pathogens from cockroaches trapped in downtown Kuala Lumpur. *Trop. Biomed.* **20**(1), 53–57.

Umunnabuike, A. C., and Irokanulo, E. A. (1986). Isolation of *Campylobacter* subsp. *Jejuni* from Oriental and American cockroaches caught in kitchens and poultry houses in Vom, Nigeria. *Int. J. Zoonoses* **13**(3), 180–186.

Vythilingam, I., Jeffery, J., Oothuman, P., Abdul Razak, A. R., and Sulaiman, A. (1997). Cockroaches from urban human dwellings: isolation of bacterial pathogens and control. *Southeast Asian J. Trop. Med. Public Health* **28**(1), 218–222.

Zerpa, R., and Huicho, L. (1994). Childhood cryptosporidial diarrhea associated with identification of *Cryptosporidium* sp. in the cockroach *Periplaneta Americana*. *Pediatr. Infect. Dis. J.* **13**(6), 546–548.

# FARM LEVEL CONTROL OF FOREIGN ANIMAL DISEASE AND FOOD-BORNE PATHOGENS

GAY Y. MILLER

*University of Illinois, Urbana-Champaign, Illinois*

CHARLES HOFACRE

*University of Georgia, Athens, Georgia*

LINDSEY HOLMSTROM

*Texas A&M University, College Station, Texas*

## 1 INTRODUCTION

Preventing the introduction of diseases, especially foreign animal diseases (FADs) and diseases that could cause food-borne illness, is critically important. Diseases of this type can be devastating to the individual farm, to the industries affected, and also to the overall

**TABLE 1 2002 Census of Agriculture Market Value of Agricultural Products Sold**

| Item | Number of Farms[a] | Sales ($000)[a] | Rank by Sales | Percent of Total |
|---|---|---|---|---|
| Cattle and calves | 851,971 | 45,115,184 | 1 | 22.5 |
| Poultry and eggs | 83,381 | 23,972,333 | 3 | 11.9 |
| Milk and other dairy products from cows | 78,963 | 20,281,166 | 4 | 10.1 |
| Hogs and pigs | 82,028 | 12,400,977 | 8 | 6.2 |
| Horses, ponies, mules, burros, and donkeys | 128,045 | 1,328,733 | 12 | 0.7 |
| Total animal and animal product sales | 1,142,357 | 109,494,401 | — | — |
| Total grain and crop Production | 986,625 | 93,789,281 | | |
| Total agriculture sales | 2,128,982 | 200,646,355 | — | 100.0 |

[a]Numbers may not add due to overlap of some categories.

Source: USDA (200). National Agricultural Statistics Service, *2002 Census of Agriculture, Ranking of 2002 Market Value of Agricultural Products Sold*, http://www.nass.usda.gov/census/census02/topcommodities/topcom_US.htm, and USDA 2002. National Agricultural Statistics Service, *2002 Census of Agriculture*, Table 50, http://www.nass.usda.gov/census/census02/volume1/us/st99_1_050_050.pdf.

economy. The value of US animal production is substantial (Table 1) [1]. In the 2002 census of agriculture, the United States had approximately 1.1 million animal-producing farms with average assets (land, buildings, and equipment) exceeding $500,000 [2]. The market value of agricultural production sold from animal production farms in 2002 was approximately $107 billion, and including crops sold from these farms, the total sales was $109 billion. The animal-producing sector exceeds the crop sector in agricultural value of products sold by several billion dollars.

Current US policy is to have a variety of programs and methods to control the introduction of FADs to the United States by controlling importation of live animals and animal products that can present a risk of introduction of FAD. Science-based rules and regulations established by the United States Department of Agriculture (USDA) govern activities that could present homeland security risks. There are outbreaks of FADs around the world and in many countries diseases foreign to the United States are endemic and present a constant risk of introduction. Trade, movement of people, mechanical means of transmission, and biological vectors between the countries need to be monitored and controlled to decrease transmission risks. This article presents an overview of animal agriculture production in the United States, how animal production practices influence farm-level control of pathogens, how the structure of food animal-producing industries affects prevention and control of the introduction and farm-level vulnerabilities of FADs, and finally, farm-level control of contemporary critical FAD pathogens.

## 2 OVERVIEW OF ANIMAL AGRICULTURE PRODUCTION IN THE UNITED STATES

Agricultural production has increased in efficiency over the last several decades in the United States. Increased efficiency of production has been realized by use of inputs such

as growth promotants and growth promoting antibiotics, as well as changes in the organizational structure of the industries and ongoing improvements in animal genetics and animal husbandry. Many of these changes in animal husbandry practices and organizational structure have grown out of a desire to enhance productivity by limiting the amount of disease and the potential for disease transmission. Additionally, as the profitability per animal declines over time, it becomes uneconomical for smaller producers to be involved in production; hence, through time, the scale of production in the United States has become larger. Simultaneously, we have seen an increasing movement toward so-called intensive agricultural production, where large numbers of animals are located at one geographic site in environmentally controlled and confined housing where capital investment in facilities has replaced labor to the extent economical and possible. These large scale production systems have been made possible because of improvements in disease control, improved water and feed quality, enhanced labor efficiency, and improved technology in housing structures and equipment.

## 2.1 US Beef Industry

Beef production has the highest monetary value and is the most vulnerable of the US animal production sectors. It is also one segment of animal production where a major portion of the industry remains extensive in nature. Cow–calf operations, which are responsible for the breeding and early growing segment of beef cattle occurs typically on small farms on land that is marginal for crop production but which provides good grazing land with associated shelter due to the topography and trees on these premises. In 2002, there were 796,436 beef cow farms with an inventory of 61,413,259 beef cattle and calves [3]. The two herd size categories with the largest number of beef cattle and calves were the 215,320 farms having 20–49 head each and a total of 11,496,796 cattle and calves; and the 23,126 farms having 200–499 head each and a total of 11,852,703 cattle and calves. The largest size category (over 2500 head) had fewer numbers of animals in total than the smallest herd size category of 1–9 head. With such a large number of cow–calf premises, they are more widely geographically dispersed than other less extensive production systems. Annual US beef production is estimated at about 26 billion lb (2006), with an increase of about 2 billion lb from 2005 to 2007 projections [4]. Current projections of production are expected to be stable over the period from 2006 to 2008 [4]. Animals sold from cow–calf premises are typically sold through auction markets, with the larger-scale farms being less likely than smaller-scale farms to sell through auctions [5]. Congregation of animals from previously dispersed geographic areas, as happens at auction markets, increases disease transmission and disease dispersion risks.

Beef calves weaned from cows are typically placed in a stocker or backgrounding operation, which uses production practices and resources to grow calves slowly and inexpensively; or calves may be placed directly into a feedlot. For example, a stocker operation might turn calves onto corn stubble for the winter, or into other grazing environments, which will typically cause slower less expensive growth than in the feedlot. Most (over 80% of inventory) beef calves eventually are placed into large scale (1000+ head) beef feedlots for finishing [5]. The feedlot diet consists of a higher grain content than the previous diets, and animals are usually confined to pens with a high density of cattle.

Veterinary services and biosecurity practices are quite variable premises to premises in beef cow–calf production. Most beef cow–calf operations do not have individual animal

identification [6]. Most beef cow–calf operations have limited or no biosecurity practices, or regular disease prevention programs, have potentially regular contact with wildlife in the area (70% of producers report sightings of wild deer four or more times per month, [7]) and uncontrolled human access to the animals. Additionally, most (85%) cow–calf operations have animals other than beef cattle present [8], and there is regular contact between these different animals/species; not an insignificant percentage (30% in 1997) of cow–calf operations purchase cattle to add to the existing herd [8]. Replacement heifers and cows that calve most typically are raised on the premises where they calve [6]. Since introducing new stock is an important way that new diseases could enter a herd, separating newly purchased stock (quarantine) is important for disease control; within herd quarantines for any newly purchased, cattle and calves are provided by less than 40% of operations [8]. Most cow–calf operators are unaware of the distance to other premises that contain species such as captive *cervidae*, bison, or Mexican-origin cattle [7]. It is not uncommon for cow–calf herds to graze on public or privately leased ground, and to be commingled with herds owned by other individuals [7]. Some vector control is commonly practiced with over 80% of cow–calf premises reporting fly control and 75% reporting rodent control. Carcass disposal is important for disease agent containment; most common methods used are burial, rendering, and incineration [7].

In beef feedlots, most operations use veterinary services [5]. The majority of larger feedlots (8000+ head) have formal quality assurance programs, and collect and test a variety of environmental samples, and have at least some dust control practices in place. Such practices can decrease the transmission of diseases that can be spread by virus or bacterial particles (which can ride on dust plumes carried from a premises). Almost all cattle entering a feedlot are "processed" at or near arrival to the feedlot, using a variety of procedures which can include injections, topical or oral treatments, and implants of various kinds unless they receive such processing (or preconditioning) prior to arrival at the feedlot. The average distance cattle are shipped from the feedlot to a packing plant is shorter (100 miles) for larger feedlots, compared with smaller (144 miles) feedlots, and closer (110 miles) for the central region of the United States versus other regions (179 miles) [9]. The distance that animals travel to packing plants can influence disease transmission, especially in the early stages (prior to diagnosis) of an FAD event.

Biosecurity in beef feedlots is commonly practiced, with some farms restricting the movement of people, and most farms making some effort to control entry of other animals (including horses, dogs, cats, foxes, squirrels, coyotes, raccoons, skunks, rabbits, and birds) to varying degrees [10]. Nearly all (over 95%) feedlots have fly control measures, with most implementing more than one control measure.

In terms of general security, large scale production systems are more likely to have enhanced security with limited (e.g. gated) access to the premises, security cameras, night lights, etc.

### 2.2 US Poultry Industry

The commercial poultry industry in the United States is a fully integrated system of animal agriculture. Each poultry company has control over all fiscal and bird husbandry aspects of production, from the day-old parent breeders to the marketing and distribution of the final products to the retailer. The "poultry industry" is actually three different industries: commercial layers, broilers, and turkeys. Commercial layers are chickens of the leghorn breed that lay table or breaker eggs for human consumption. There are approximately

334 million table egg layers in production in the United States [11]. These birds begin laying eggs for human consumption at 18–19 weeks of age.

The US turkey (272 million) and broiler chicken (9.1 billion) [12] industries are similar to each other, with the company purchasing the parent breeders at one day of age, or hatching eggs from a primary breeder or genetic selection company. These birds are raised on farms contracted by the company under specific company guidelines. The offspring (broiler chickens or commercial turkeys) of these breeders are hatched in company-owned hatcheries, and placed on a contract or company-owned farm, where the farmer must follow strict company guidelines for husbandry. All feed that is fed to the breeders, broiler chickens, or commercial turkeys is manufactured in a company-owned (or contracted) feed mill under specific guidelines of the company. The company nutritionist(s) will specify the nutritional aspects of the feed, and the company veterinarian(s) will determine any vaccine, antibiotic, or anticoccidial usage requirements. The birds will then be slaughtered in the company-owned processing plant.

The typical US broiler chicken farm will have approximately 100,000 chickens, divided equally into four houses. As in a city of 100,000 people, disease prevention becomes imperative for the poultry industry. Poultry veterinarians practice preventive medicine, utilizing two primary tools, biosecurity and vaccination. The US average level of death loss (mortality) in the typical 100,000-bird broiler farm is 4–5% [13]. There is also a loss of approximately 0.5–1.0% of the birds for human consumption in the processing plant, when birds are condemned by the United States Department of Agriculture-Food Safety Inspection Service (USDA-FSIS) inspectors [14].

***2.2.1 Typical Poultry Company.*** A typical broiler (or turkey) company comprises one or more divisions, or in industry jargon "complexes". A complex is a self-contained integrated unit that has broiler birds (or turkeys) breeder birds, a hatchery, a feed mill, and a processing plant. The typical broiler complex will slaughter approximately 1 million broiler chickens per week.

Typically, the manager of a complex of broiler birds will have three to four persons as direct reports who are managing this finely tuned operation on a daily basis (Fig. 1).

The feed mill manager provides all of the feed to all of the immature breeders (pullets), the adult breeders (breeder layers), and the broiler chickens in the complex. The feed is very closely controlled and monitored by the Food and Drug Administration (FDA). All documentation is available for FDA when they inspect each feed mill. It is illegal for any unapproved drugs to be added to the feed or for the level of the drug to be different than the use limitations on the FDA approved label. This means there is no legal means of using any drug in an extra label manner in poultry feed.

The live production manager has the three segments of the business dealing with the live birds. The first direct report is the breeder manager who is responsible for acquiring the day-of-age breeder chicks from the primary breeding company. These chicks are raised by contract pullet growers in specially designed houses from day 1 to sexual maturity (approximately 22–24 weeks of age). At sexual maturity, these pullets are moved in trailers with cages to breeder farms to begin laying fertile eggs. These breeder farms are typically owned by a farmer contracting with the poultry company. These contractors are paid by the dozen for the eggs produced. There are approximately 10,000 hens (plus 1000 roosters) in each house and most typically two houses per farm. The feed for both pullets and breeders is weighed and distributed automatically at a specific time of day. The water is also automatically available to the birds. All of the eggs from

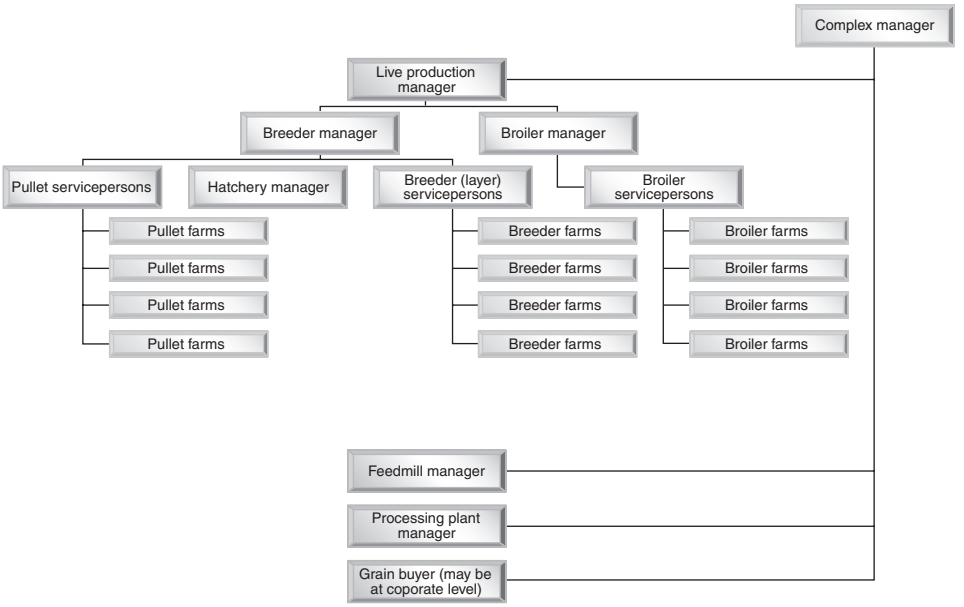



**FIGURE 1** Typical broiler chicken complex management structure.

a breeder farm are held in an environmentally controlled room on the farm for 2–3 days. An environmentally controlled truck goes to the farm, the eggs are loaded on to the truck, and then delivered to the hatchery. The hatchery manager receives the eggs from multiple broiler breeder farms and four times each week, sets eggs into incubators where they have a controlled environment. The broiler chicks hatch in 21 days (28 days for turkeys). These day-of-age chicks are typically vaccinated in the hatchery to help prevent two respiratory diseases, Newcastle disease and infectious bronchitis.

The day-old chicks are then delivered to a contract broiler grower farm where they go into an environmentally controlled house that is on average 40-ft wide and 500-ft long with approximately 25,000 broilers per house. Many of these houses have computers controlling the temperature and ventilation. An automatic feeder system maintains feed available to the birds 100% of their life. Automatic nipple or closed water systems are found in almost 100% of the houses. Fresh water from a municipal system or a potable well flows into the house and can only exit the system when a bird pecks or touches the nipple thus allowing water to go into its mouth.

The contract farmer or "grower" is responsible for the daily care of the birds, providing the building, equipment, heat, electricity, water, and litter handling. The company owns the birds and provides the feed, any medication or vaccines if necessary, and transportation of birds. The growers follow the poultry companies' husbandry guidelines. The broiler manager has many broiler servicepersons, who each have a number of farms where they provide any technical assistance to the contract grower. They visit every farm a minimum of once a week and usually twice a week. If a grower has birds that become sick, or an abnormal number dies ($>1$ bird/day per 1000, i.e. $>25$/day in a 25,000 bird house) then they immediately contact their broiler serviceperson (available 24 h/day). These broiler servicepersons are trained by veterinarians to perform necropsies or they

may deliver diseased or dead birds to a diagnostic laboratory veterinarian in order to identify the cause of excess mortality.

The broiler chicken growers' pay is based on the pounds of broilers delivered to the processing plant utilizing the least amount of feed for growth. They will have any birds that are condemned by the USDA as unwholesome for human consumption deducted from this weight. Therefore, it is important for growers to follow company husbandry guidelines. Also for many poultry company contracts, the use of any medication, insecticides, disinfectants, etc. will be strictly controlled by the company.

The birds on a broiler farm are of the same age (all in at the same time). When the birds reach slaughter age (on average ~49 days old) all birds are caught and loaded on to trucks and delivered to the processing plant (all-out at the same time). At the processing plant, the USDA-FSIS veterinarian is responsible for antemortem and postmortem inspection. The processing plant manager oversees all operations from slaughter to the final product leaving the plant.

### 2.3 US Pork Industry

The US pork-producing industry has also changed dramatically over the past few decades. What was once an industry dominated by small, independently owned operations now comprises fewer, larger operations that are concentrated in certain regions of the United States. In 1995, only 2.6% of swine operations had 2000 or more hogs and held 43% of the inventory. In 2006, 11.8% of swine operations had 2000 or more hogs, holding 80% of the hog inventory. Over 21.1 billion lb of pork was produced in 2006 [15]. As for the poultry industry, decreased production costs and increased efficiency obtained from using new specialized technologies and genetics, among other things, have contributed to the increased pork industry concentration [16].

Many parallels can be seen with the poultry industry as the pork industry becomes more specialized and vertically integrated. A previously open market industry has moved to one dominated by marketing and production contracts. In marketing contracts, producers agree to deliver a certain number and size of hogs to processors at a certain time. Prices received by producers may be determined in advance or be a formula-based price, such as a spot market price. Production contracts are becoming more common and are not dissimilar to production contracts in the broiler industry. In these contracts, an integrator (large producer or processor) provides the inputs such as the hogs, feed, veterinary, and management services. The contractor provides the land, facilities, and labor, and receives a fixed payment. In both types of contracts, premiums may be given for production efficiency or the quality and size of the hogs [16].

Total confinement and multiple-site production are commonly used in US swine production operations. Operations that specialize in a specific phase of production are becoming more common. Such operations take advantage of newer cost efficient technology and improved genetics in many aspects of production. The attractiveness of specialization has caused the number of farrow-to-finish operations to decrease [17]. Farrow-to-finish operations are generally less efficient and have an increased risk of disease introduction and spread due to the wide age range of pigs on a premises, and increased movement of pigs and personnel on and off these sites, as compared to operations that specialize in one phase of production. Farrow-to-wean, nurseries, and grower or finishing operations are three typical phases of specialized production and will be discussed next.

***2.3.1 Farrow-to-Wean.*** Artificial insemination is the primary technique for mating gilts and sows, especially in large and medium size operations. Semen is primarily purchased or collected off-site [18], eliminating the need to keep boars on-site except for checking if the gilt or sow is ready for insemination (in heat). Artificial insemination does reduce the risk of disease transmission. Semen should still be tested for certain diseases (e.g. porcine reproductive and respiratory syndrome; PRRS). In 2006, [18], the average number of piglets per litter was 11.5, with 10.5 being born alive and 9.4 weaned. Preweaning mortalities ranged from 8.5 to 11.3% per litter The most common reason for preweaning deaths is from being crushed by the sow. Piglets are injected with iron when they are 7–10 days old and are sometimes given antibiotics in the feed. Most breeding-age females are culled when there is a reproductive failure or when the age of the female becomes a risk factor. Carcasses are primarily disposed of by rendering or composting on-site [18]. There can be a high flow of new arrivals on farrow-to-wean production sites and proper biosecurity is important to decrease the risk of disease introduction. Isolating or quarantining, and disease testing of new breeding animals before they are introduced into the herd can help prevent the introduction of new pathogens. Newly introduced pigs are isolated for an average of 4–6 weeks. Administering vaccines to new arrivals is the most common acclimation method used. Other acclimation practices include exposing new arrivals to pigs on-site, and less commonly feedback of feces from other swine or feedback of mummies, placentas, or stillborn pigs [18].

Pigs are generally weaned between 16 and 27 days, although larger operations may wean at an earlier age (16–20 days). Pig flow is continuous during gestation phases and primarily continuous or all-in/all-out by room or building during farrowing phases. All-in/all-out management includes cleaning and disinfecting before the room or building is refilled which reduces the risk of disease spread [18].

***2.3.2 Nursery.*** Weaned pigs often move to a nursery, where they will stay for 6–8 weeks. Pigs leaving the nursery will weigh 30–80 lb. Annual mortalities in nurseries are typically 4–5%, with respiratory problems being the most frequent reason for deaths. Most operations use antibiotics in feed and vaccination as disease prevention methods during this phase of production. Nursery pigs are commonly vaccinated for *Mycoplasma* and erysipelas. Pig flow is mainly all-in/all-out. Pigs are primarily obtained off-site from another producer and come from a single producer (i.e. single source), although 25.4% of larger sites obtained pigs from three or more sources [18].

***2.3.3 Grower or Finisher.*** Pigs stay at a grower or finisher site for an average of 16–18 weeks. Annual mortalities and pig flow management are similar to nurseries. Also like nurseries, pigs are primarily obtained off-site from a single source. The most common disease prevention method used during this phase of production is antibiotics in feed [1]. Once they reach market weight (225–300 lb), most hogs will be sold to one or two packers, but may be sold to more depending on the geographic proximity of packers and production sites [19].

Hog production was previously mainly concentrated in the North Central regions of the United States (Iowa, Illinois, Indiana, and Minnesota), but has expanded to include the South Atlantic (North Carolina) and South Central (Oklahoma, Texas) regions [16]. Differences in operation types are seen between regions. For example, weaned pigs are commonly transported from the South Atlantic to the North Central region to be finished [18]. It has been estimated that 3.8 million hogs were shipped out of North Carolina in

2001 [20]. Based on the 2006 National Animal Health Monitoring System (NAHMS) study of the swine industry, 31.6% of sites shipped pigs across state lines [18]. Also, approximately 8% of hogs slaughtered in the United States are of Canadian origin. Most Canadian hogs are imported to the North Central region as feeder pigs, and the rest go directly to slaughter houses [17]. Livestock trucks transporting pigs between the different phases of production, both locally and regionally, can also spread pathogens in the process. Both local and regional animal movements can affect the extent of an outbreak, especially if there is delayed detection of disease. It is believed that a livestock truck that was not properly cleaned and disinfected was responsible for the spread of classical swine fever (CSF) from Germany to The Netherlands during the 1997–1998 outbreak [21].

Feral swine populations continue to grow in the United States, and their distribution is becoming more widespread. Estimates of their numbers are over 4 million, with the majority of feral swine located in Florida, Texas, and California. They pose a serious risk for transmitting endemic diseases of feral swine such as brucellosis and pseudorabies. FADs could also be introduced into the feral swine population and go undetected for some time. An FAD introduced into feral swine could fade out or become endemic. This represents a risk of disease transmission to commercial swine if biosecurity does not prevent direct or indirect contact between feral and commercial swine. In the 2006 NAHMS swine study, 25% of large sites and 12% of medium sites reported the presence of feral swine in their county, especially those facilities located in the southern regions [18].

Rodents can also spread disease, either as hosts or mechanical vectors. Most operations use some method to control rodents; bait or poison is most frequently used. The majority of swine operations only allow employees to come into contact with areas that house the swine. Some companies have their employees sign documents prohibiting them from owning swine of their own. Outside visitors that are allowed in areas where the swine are housed are usually required to put on clean boots and coveralls. Operations may require visitors to be without swine contact from other premises 24 or more hours before entering [18].

## 3 PREVENTING/CONTROLLING INTRODUCTION OF DISEASES AT THE FARM LEVEL

Production practices and the structure of the food animal industries imply many areas of vulnerability. Large numbers of animals are often housed at one geographic site, and often in a shared airspace, or in close confinement. Although such practices enhance the profitability of production and also decrease transaction costs for production companies (costs decreased or avoided with integrated production companies), they can increase disease transmission risk by making a larger number of animals at risk for becoming infected by a contagious disease. However, large integrated companies can also afford to have more stringent biosecurity practices through economies of scale in production. Large companies are more likely to have in-house veterinary staff, written and enforced biosecurity guidelines, in-house diagnostic laboratories, and other production inputs that are not possible for smaller scale production systems. The net impact then for disease risks implied by the current food animal industries' structure and production practices in the United States is unclear; there are forces that could increase disease transmission risks and forces that would decrease such risks. Similarly, the development of appropriate and

protective countermeasures can simultaneously have aspects that are of varying difficulty to implement.

The remainder of this section focuses on production inputs and ways to help harden these as sources of vulnerabilities. Obvious risks include genetic stock (both live animals and semen or eggs/embryos), vectors for disease transmission, feeds, supplements, water, vaccines and pharmaceuticals, and air.

### 3.1 Direct Animal Contact and Genetic Stock Vulnerabilities, Vehicles/Fomites, and Vectors as Sources of Pathogens

Goals for biosecurity of live animals include minimizing opportunities for disease transmission, decreasing sources of infectious agents, using methods such as vaccination and good husbandry to enhance the immune status of animals to prevent disease, and monitoring for the presence of disease while using appropriate diagnostic testing to become aware of the profile of pathogens and immune status. Infected live animals and direct contact are arguably the most likely source for introduction of many FADs to a herd or flock. By appropriately siting production facilities away from neighboring herds and flocks and then maintaining a closed herd/flock (i.e. no animals are admitted from outside sources) sources of infectious agents can be minimized. This means that no animals are admitted from outside sources. This practice may or may not be possible or appropriate.

The next alternative is to identify animals that will come to the farm that are from sources that have high biosecurity and that can certify the disease status of their animals and products (e.g. semen). It is important for farms to use transportation methods and routes that are safe and will limit potential exposure to infectious agents by limiting sources of infectious agents, for example, manure, animal hair, dander, and dust. This means transporting animals using thoroughly cleaned and disinfected trucks, and when possible, company-owned transportation. Quarantine of all newly arrived animals is needed so that there is adequate time for monitoring and testing for diseases that might have been carried to the farm by the new animals. Appropriate vaccination or processing prior to mixing new arrivals with any animals that are on the premises will further ensure the safety of adding new genetic stock to the farm. Biosecurity surrounding the introduction of live animals may be the most important area for protecting the farm from FAD risk.

Additionally, there are many other activities that are important to decrease the likelihood of FAD introduction to a farm. Control of traffic of all types to the premises is critical. Exclusion of unnecessary visitors, pets, and pests will decrease the likelihood that a disease is introduced accidentally. Disease can be introduced by animal or environmental exposure/contamination to vehicles/fomites such as boots or coveralls, pets or pests, or a variety of other mechanisms. Pests include vertebrate animals such as wild birds, rats, mice, and raccoons, as well as invertebrate vectors, which may transmit disease, such as flies and mosquitoes. As examples, poultry production systems and many swine production systems require the use of disposable coveralls, boots, gloves, face masks, and hair bonnets for all people entering the premises. Additionally, many swine production systems require shower in and shower out for all visitors to production facilities. Many systems stipulate and enforce a period of no animal contact prior to visiting the facilities for all noncompany personnel. Maintaining a record of all visitors is also a common practice on poultry and swine production systems.

Cleaning and disinfecting between batches of animals decreases the disease transmission risks between batches. Reporting of abnormal signs of disease and maintaining a veterinary–client relationship are all valuable practices so that if disease is present or introduced, it is treated promptly and when appropriate, the facility is depopulated, infected materials are appropriately disposed of, and the facility and all associated equipment and materials are cleaned and disinfected. These and many similar practices all contribute to enhanced biosecurity for the animals present in production systems.

The description of the goals of biosecurity should make it obvious why much of the US commercial agriculture, as explained in the previous section describing the US animal production sectors, has evolved to its current structures and practices. For example, the current structures and practices in commercial broiler and turkey production and larger-scale swine production have the same age animals that arrive from a single source, into facilities that are managed as all-in–all-out (or batch) production. Companies and production methods have been structured to avoid introduction of disease to the farm.

Genetic stock is an important source for meeting improved product standards driven by industry demands. Today in commercial agriculture, breeding companies develop and maintain pure breeding lines, which are used to create grandparent stock. Grandparent stock are the parents of so-called parent stock. Parent stock are then the parents of the commercial animals. Biosecurity for genetic stock involves similar functions to those applied directly to the commercial animals, except that the standards are even higher.

The use of purchased semen is a common practice to introduce new genetic stock or simply as the standard for parent stock breeding systems. Practices that will enhance biosecurity for semen include obtaining semen from known negative sources, from companies that practice high biosecurity and use extensive surveillance and testing, and ensure the safety and security of transportation and delivery of semen to the farm premises where it will be used. Frequency of disease testing and the openness of semen company records are some of the indicators that can be used to assess the biosecurity of semen providers.

Companies responsible for providing semen to producers must consider a variety of issues beyond the basic biosecurity and surveillance of their animals. For example, sources of equipment and products (e.g. semen extenders) must be thoroughly checked with ongoing methods to detect accidental or potential sabotage to materials that could contribute disease risks to the semen products they produce.

Studies help elucidate the risks for farms and on-farm production practices. For example, a risk analysis for the importation of CSF (also known as *hog cholera* and an FAD that was eradicated from the US swine population in 1976) demonstrated that CSF is spread by movement of live animals, especially wild boars, people, vehicles, equipment, or semen contaminated with virus [22]. These risk factors identified for the importation risk model apply also to potential spread within the US domestic herd.

There is a variety of other practices that can be implemented to help harden on-farm production systems. Examples include the following:

- Background checks for all hired personnel
- Enforcing company biosecurity policies/monitoring employee compliance of company biosecurity requirements
- Anticipating and watching for abnormal signs of disease and abnormal activity of people in and around the production facilities

- Establishing farm-specific emergency response plans
- Identifying animal disposal sites that meet Environmental Protection Agency (EPA) requirements
- Identifying depopulation, disposal, and disinfectant/decontamination methods and partner companies that could be worked with if needed
- Siting facility locations to minimize exposure to other herds/flocks including siting away from major roads/freeways
- Participating in and practicing with industry and local county animal response team (CART) and state animal response team (SART)
- Structuring the farm and animal production sector to provide for agility of response to outbreaks from a variety of considerations

### 3.2 Feeds/Supplements and Water Vulnerabilities

Feeds/supplements and water will be discussed from the perspective of the poultry industry, but the concepts and vulnerabilities identified apply generally to animal agriculture production. The two primary sources of water for poultry are also the same sources for the human population: municipal water and well water. Both sources should be potable drinking water. If a farm is near a municipal/local government water system, it may source from that system. However, because of the large amount of water usage, especially in the summer to aid in cooling birds, and because the location of production systems does not normally allow accessing municipal water systems, the source of water for the majority of farms is wells. Commonly, more than one well is required to supply water to a farm. In most cases, the well water would have been tested for potability when the well was first opened but may not be tested again unless a problem is suspected.

Many turkey farms and some broiler breeder farms have water treatment systems, primarily chlorinators. Few broiler or layer farms have any consistent water treatment occurring. Many newer farms have water meters in each house/barn and the farmer/grower/company will monitor water consumption.

From a biosecurity perspective, the water system is an area of vulnerability. Some diseases and chemicals could be transmitted by contaminating the water system. This can occur both naturally and by intentional introduction. The testing for potability is typically limited to looking at organisms that are indicators of fecal contamination, nitrates, and ion levels including sodium, chloride, sulfate, iron and manganese. For livestock, testing may also include pH, conductivity, potassium, total dissolved solids, and hardness. Potability testing does not generally indicate the presence of other disease agents, toxins, or chemicals that could cause a disease.

The water source should be secured and regularly checked. This will mean locking the well heads, and controlling the source, storage, and use of any chemicals and water processing systems that may be used. Water that is obtained from a municipal system, while perhaps more secure, can also be potentially contaminated. Given the ease of distribution and wide exposure contaminated water could cause, ensuring quality water in animal agriculture production is important.

The majority of feed provided to all segments of the poultry industry in the United States is obtained from large centralized feed mills specific to that location/company. Nearly all of the broiler chicken and turkey feed mills provide feed for only broilers or turkeys of that company. However, many of the commercial table egg-producing feed

mills are multiple species mills, producing feed for dairy cattle, beef cattle, etc. The ingredients are primarily corn (energy) and soybean meal (protein) with added vitamins, minerals, and any medications. The feed accounts for as much as 60% of the cost of producing the poultry or eggs, so feed ingredient prices significantly affect which ingredients are used. For example, as the price of soybean meal increases, more rendered by-products derived from animal processing plants are used as a protein source. Routinely now, ruminant rendered product (meat and bone meal) is used as a cheaper source of protein to add to poultry diets in addition to soybean meal.

The major raw ingredients arrive at the feed mill either by train or by truck in bulk. These will be offloaded and stored in large silos. The minor raw ingredients such as minerals, vitamins, or medications come in bags and these are stored usually in the warehouse section of the mill.

Feed mills will normally produce feed for 16+ h/day and feed is delivered in bulk tanker trucks which augers the feed into storage bins on the farm. The system on the farm is a closed auger system from the bin which supplies one to two houses (i.e. barns). The feed mills are an area of vulnerability for animal agriculture. Feed mills are operating 16+ h and have feed being delivered from the finished feed storage bins almost 24 h/day. Feed mills are usually open with few locks or security systems. Employees, feed trucks, raw ingredient vehicles, etc. are coming and going on an almost continuous basis. Thus, intentional introduction of pathogens, toxins, or chemical contaminants is possible.

Feeds have been shown to be a risk recently with the melamine contamination of poultry and pig feeds [23]. This contamination occurred through the use of feed ingredients imported from China used in producing pet foods. Left over pet food ingredients were then purchased by animal feeds manufacturers and used in the production of animal feeds. The contamination was traced to the use of a rice protein concentrate, wheat gluten, and corn gluten that evidently had melamine used to increase the apparent protein content of the feed. Hogs that fed the melamine were initially quarantined. They were eventually allowed to go to slaughter after a holding period and testing revealed they were safe for human consumption. There was significant market disruption and concern generated for the producers directly involved in this event and for the industries generally. Undoubtedly, there will be increased guidance and potentially increased regulations from the FDA, the agency responsible for oversight of animal feeds.

Animal feeds have a history of being a target for a terrorist attack [23]. Many poisonings have been accidental [23, 24]. Still these incidents are informative about the potential risk and the needs for improving feed security.

The use of garbage feeding of pigs is forbidden by federal law unless the garbage is treated (usually by cooking) to kill disease organisms. Garbage can be a source of transmission of animal diseases including FADs, such as foot-and-mouth disease (FMD). Additionally, human pathogens found in garbage can be transmitted to pigs if not killed by cooking the garbage, and might form the basis for a zoonotic cycle of disease transmission.

Salmonella is a zoonotic pathogen that can be transmitted in feeds. In poultry, it has been well documented that feed can be a source of salmonella [25, 26]. The primary source of salmonella introduced into feed is from a contaminated raw ingredient with animal protein sources often having high levels of salmonella [27]. Additional sources of salmonella introduction into finished feed can be from residual feed in the mill from passage of previously contaminated feed, from rodents living in or near the feed mill, and from wild birds [26].

### 3.3 Vaccine and Pharmaceutical Vulnerabilities

Vaccines and pharmaceuticals are a source of vulnerability for food animal production. These materials need to be kept in a secure location which holds the materials at appropriate conditions needed for the materials. Materials must be procured from reputable sources that conduct assessments for quality and safety of product. Clean injection equipment needs to be used with new needles used for each animal, or at least changed frequently if new needles are not used on every animal. Records need to be kept of all use of vaccines and pharmaceuticals.

### 3.4 Air Contaminants and Airborne Spread of Pathogens

Aerosol transmission of certain pathogens and contaminants can occur within and between farms. Successful transmission depends on many farm-level factors. Host factors include the animals' health status, species, age, density, and their behavior and interaction. Management factors include the building type (layout, floor type, dimensions, ventilation system), feeding system (equipment, time and duration, feed type), waste removal system, and bedding type. Environmental factors include temperature, relative humidity, concentration of gas, and the direction and speed of air [28, 29].

For airborne spread of pathogens, a sufficient amount of infectious particles must be generated by infectious animals and transported and inhaled by susceptible animals [30]. Infectivity must be maintained in order for susceptible animals to become infected. Airborne particles originating from droplets stay in the air for longer periods of time than particles originating from dry matter, such as dust. A high amount of aerosolized particles are generated from animals that sneeze or cough, and a lower amount from normally exhaled breath [28]. Aerosols can also be generated from urine or feces, especially from spraying slurry [31, 32], and from bedding and feed [33]. Airborne FMD viral particles may originate from incinerating infected carcasses [34]. Once in the air, pathogens undergo decay that is related to the amount of time they remain in the air, particle size, temperature, and relative humidity [35]. Influenza viruses are most stable in dry air, whereas FMD virus is most stable in moist air [28]. Airborne particle concentration has been shown to increase at lower temperatures [33], but this can be influenced by the type of farm management. Building design and ventilation systems are equally important as animal activity and density in determining airborne particle concentrations [36]. Cool and damp environments that are flat, with little to no wind and sunlight, favor the travel and survival of airborne particles over long distances [28].

Airborne disease transmission depends on the minimal infective dose of the agent needed to cause infection, as well as farm-level factors such as herd size and type/susceptibility of animals. Transmission is more likely to occur as herd size increases. Larger animals and older animals have a higher risk of becoming infected because they breathe in more air than smaller and younger animals. For example, there is lower risk of transmitting airborne FMD virus to hog farms than to cattle farms [37].

Airborne disease transmission risk can be reduced. Reducing dust, where feed is a major source, greatly reduces aerosol particles [28]. Dust can be reduced from feed by adding tallow, soybean oil, or water [38]. The amount of animal activity and movement should be decreased, when possible. Slurry and manure spreading should be done appropriately to limit the production of aerosol particles as much as possible. Facilities should be designed to allow for proper ventilation and space between animals; the relative humidity to decrease airborne transmission risk is 60% or above [39]. Strategically

placed air inlets can also be beneficial [40]. Although expensive, combining air filtration and positive pressure ventilation has also been suggested [28].

Facility dispersion (i.e. more space between facilities) will help decrease airborne disease transmission risk. However, appropriate spacing of housing is not always feasible, and this alone is not enough to prevent aerosol transmission [36]. Personnel on farms should always be vigilant and follow appropriate biosecurity protocols when entering and exiting animal houses. Movement between infected and noninfected houses by the same person should be minimized or avoided. Depending on the disease, vaccination as part of an overall animal health plan can also help prevent diseases caused by airborne pathogens.

## 4 PATHOGENS OF CURRENT CRITICAL IMPORTANCE FOR FOOD-PRODUCING INDUSTRIES

Infectious diseases and emerging pathogens are of critical importance in today's food animal-producing industries. Even endemic diseases have become of increased importance. For example, low pathogenic avian influenza (LPAI) is a disease which is endemic with periodic regional epidemics being experienced (for example in the turkey industry). However, LPAI has become of critical importance because of the potential for mutation to highly pathogenic avian influenza (HPAI). There are many endemic diseases of importance for food animal-producing industries. Indeed, there are so many that whole books are written on such topics. In this section, three FADs of contemporary importance are discussed: HPAI FMD, and CSF

### 4.1 Highly Pathogenic Avian Influenza

The two most important poultry FADs are exotic Newcastle disease (END) and HPAI. Since there is minimal zoonotic potential with END, the focus here is HPAI. However, END is a potentially devastating disease to the poultry industry as evidenced by the outbreak in Southern California, Nevada, Texas, and Arizona in 2002–2003 that cost an estimated $198 million [41]. This END outbreak was limited to a small segment of the commercial poultry industry and was primarily in game fowl and backyard flocks.

The last major outbreak of HPAI in the United States occurred in 1983–1984 in Pennsylvania [42]. This outbreak, caused by an H5N2 virus, affected 448 flocks with more than 17 million birds destroyed in Pennsylvania and Virginia. The virus began as an LPAI subtype H5N2 and then quickly mutated to the highly pathogenic form. The USDA spent over $63 million in 1983 to eradicate this virus from these two states and prevent further spread. This amount does not include the cost to the individual farmer (except indemnity for the affected flock), the losses for the poultry industry in lost revenue, and the many other costs that are not easily calculated.

In general, influenza viruses are very host specific; however, there have been some occasions when the virus has crossed between species as has been seen in the recent H5N1 in Asia crossing from poultry to humans [43]. The recent viruses that have been associated with bird to human transmission are of the H7 and H5 hemagglutination type. It is because of the recent Asian outbreak and concerns for a further change in the virus that many states have now begun programs for containment of low pathogenic H5 or H7 avian influenza viruses.

HPAI is a reportable disease [44]. The USDA is designated with the authority for containment, destruction, and indemnity. However, successful control of an outbreak will require close cooperation among the USDA, the state(s) where the outbreak is occurring, and the poultry industry. HPAI outbreaks also include notification of the US Department of Health and Human Services and the US Centers for Disease Control and Prevention.

There is a federal program for monitoring for LPAI called *US Avian Influenza Clean* for layer and broiler breeding birds. This is administered by the USDA's National Poultry Improvement Plan (NPIP) [45]. This program requires that a minimum of 30 birds be tested and antibody negative for avian influenza when more than 4 months of age. To retain negative classification, a breeder flock must have a minimum of 30 birds tested negative at intervals of 180 days. Also, before these birds are slaughtered, 30 days prior to the end of the laying cycle, 30 birds must be tested and antibody negative.

The USDA-NPIP also has recently begun a special program for the meat-type (broiler) chicken industry to monitor for H5/H7 subtypes prior to slaughter. This program requires a negative antibody test for H5/H7 subtypes of avian influenza from a minimum of 11 birds per flock no more than 21 days prior to slaughter.

In most states with large numbers of commercial poultry, there are also active surveillance of live bird auctions and markets, as well as passive surveillance programs. Passive surveillance programs include serological testing of all live birds submitted to state diagnostic laboratories for avian influenza.

In the event of a positive serological result, the confirmation of subtype will be done by a USDA authorized laboratory, frequently the USDA National Veterinary Services Laboratories (NVSL) in Ames, Iowa. NVSL will immediately report the results to the proper state authority. If it is an H5/H7 subtype of LPAI, then the state veterinarian will quarantine the farm and implement that state's avian influenza (AI) response plan. It should be noted that a serological surveillance program is not necessary in the event of an introduction of HPAI since there are normally morbidity and mortality rates approaching 100% [46]. In this event, the poultry producer will immediately notify either a company veterinarian or a local diagnostic laboratory.

HPAI can be readily diagnosed and would result in an immediate quarantine and depopulation of the affected premises by a cooperative effort of federal, state, and local authorities working closely with the poultry producers. The size of the affected premises or number of premises affected will determine the size of a testing and/or depopulation zone around the index premises. All of this will be decided by the response (also called *the incident command*) team of the federal, state, and poultry industry cooperators. LPAI cannot be clinically distinguished from other respiratory diseases. Therefore, the USDA and state programs for active serological surveillance are necessary and have been shown to be effective in identifying H5/H7 subtype affected flocks as seen in 2007 in West Virginia and Virginia. These birds were identified and depopulated. The virus did not spread.

The method of mass depopulation of floor reared poultry that is being developed is using foam [47]. Foam has been shown to be a faster depopulation method as group size increases and is no more stressful for the birds than $CO_2$ depopulation. Speed of response in an FAD event is critical to a successful response. Foam has the added advantage of needing fewer humans to depopulate larger houses, and thus may be preferred for HPAI.

Proper handling of depopulated birds and infected materials such as litter is also important for a successful response. Natural decomposition by on-site composting was the method used for the 2007 LPAI events in West Virginia and Virginia. The biosecurity

of on-site composting needs more research, but appears to have good potential for meeting the biosecurity goals of appropriate and safe carcass disposal [48].

### 4.2 Foot-and-Mouth Disease

A major epidemic of FMD in Taiwan in 1997 caused the death of approximately 184,000 pigs; additionally, almost 4 million hogs were slaughtered in the eradication program [49]. The previously robust Taiwanese pork industry has been restructured and downsized [50]. The FMD outbreak in the United Kingdom in 2001 had an estimated economic impact of £8.6 billion (equivalent to $17.4 billion US) [51]. There has been a second outbreak in 2007 in the United Kingdom that is substantially smaller, although still costly. Both of these economies suffered in major ways because of FMD. Additionally, there was serious animal suffering and human psychological problems, as well as serious restriction of a variety of activities. For example in the UK outbreak in 2001, the most important economic impact was associated with loss of tourism and recreational use of agricultural lands and the countryside.

FMD is considered an important contemporary FAD because of ease of access to the virus (there are many countries where FMD is endemic), extremely contagious nature of the agent and its ability to spread rapidly, the affect on multiple species (all cloven-hooved animals are affected, including dairy cattle, beef cattle, pigs, goats, and sheep to name a few), the high potential impact on international trade, and the potentially severe economic, social, and political consequences of the disease [52]. Epidemiological models have suggested that as many as 17% of all herds could become infected during a hypothetical outbreak of FMD in California [53]. Total eradication costs from the simulated FMD outbreaks ranged from $61 million to $551 million with mean herd indemnity payments estimated to be $2.6 million and $110,359 for dairy and nondairy herds, respectively [54]. Wind-borne spread of the virus contributes to a higher potential for more rapid spread since it can spread to 20 km [55].

The National Center for Animal Health Emergency Management (NCAHEM) has plans for handling an outbreak of FMD should it occur in the United States. Similarly, there are many states and state animal or agricultural response teams that have plans and have conducted exercises around FMD scenario outbreaks. The United States also maintains the North American FMD Vaccine Bank which provides ready access to FMD vaccine should this be needed as part of mounting appropriate countermeasures during the face of an outbreak of FMD should one occur. This vaccine bank contains contemporary FMD strains with sufficient cross strain immune protection to cover virtually any strain that might occur, either from a natural introduction or bioterrorist introduction of FMD. Additionally, it has been shown that use of an emergency vaccine will prevent or reduce virus replication dramatically reducing the amount of virus released into the environment [56]. This is critically important in the early stages of an outbreak, and suggests that vaccination can be used as an appropriate countermeasure even if animals receiving vaccine will be diverted to depopulation later in managing the outbreak. Animals might be diverted to depopulation rather than being sent through market channels because the rules established by the OIE (World Organization for Animal Health) currently require a longer period of time to elapse, from the identification of the last known infected animal, in order to be listed as disease free, if vaccination has been used as a part of the control measures employed during an outbreak. Since the OIE-disease free status provides access to markets which exchange at a premium rate over markets which involve other

designations, there might be times at which the most epidemiologically and economically sound decision would be to use vaccination to slow disease spread because depopulation could not proceed as rapidly as desired. This would make time for later depopulation, while simultaneously preventing the negative impact of having used vaccination as a part of the control strategy (since the vaccinated animals do not enter market channels).

### 4.3 Classical Swine Fever

CSF, also known as *hog cholera*, is a highly contagious disease of swine. CSF was first recognized in the United States in 1833. The United States was declared free of CSF in 1978 following an intensive 16-year eradication campaign, which cost $140 million. A similar eradication effort would have cost approximately $525 million in 1997 [57, 58]. The virus remains widespread throughout the world and is well established in the Caribbean basin and regions of Mexico despite extensive control and eradication efforts. Outbreaks continue to be reported in countries with control programs, while other countries simply consider the disease endemic. In many counties in Europe, CSF has become endemic in large wild boar populations [59]. The ease of access to the CSF pathogen in the Caribbean basin represents a significant threat to the United States for both intentional and nonintentional introduction. Any introduction of CSF could result in significant economic loss due to the subsequent need for massive control and eradication efforts, and the resulting loss of access to foreign markets. An outbreak in The Netherlands in 1997, for example, resulted in the destruction of almost 11 million pigs, of which almost 9.2 million were slaughtered for welfare reasons [60]. The cost of this epidemic has been estimated at US $2.3 billion, which included both direct costs and the consequential losses to farms and related industries [61].

Infected pigs shed virus in all excretions and secretions including blood, semen, urine, feces, and saliva. Oronasal is the most important route of transmission between pigs [62]. Transmission of CSF may occur through direct contact between domestic and wild/feral pigs, by feeding pig carcasses or infective pig products (especially swill feeding) to susceptible animals, or indirectly via contaminated clothing or equipment [63]. During the 1997–1998 CSF outbreak in The Netherlands, 17% of transmission was due to direct animal contact. The rest of transmission was due to indirect contact, primarily from transport lorries [64]. Illegal swill feeding is responsible for many outbreaks as the virus survives very well in meat. The virus has been shown to survive up to 4 years in frozen pork [65].

Clinical signs of CSF can be variable and depend on many factors, the most important factor being viral virulence. Although outbreaks of highly virulent strains characterized by high mortalities were common in the past, currently circulating strains are predominately mild to low virulence [66]. Introduction into the United States of low virulence CSF may delay detection. Such was the case in Europe. The approximate time from viral introduction until detection of CSF outbreaks was 3 weeks in Belgium (1993), 4 weeks in the UK (1986), 6 weeks in The Netherlands (1992 and 1997–1998 outbreaks), 8 weeks in Germany (1997), and 9 weeks in Spain (1997) [64]. Many other diseases in swine have clinical signs indistinguishable from these low to moderate CSF strains. These diseases include PRRS, erysipelas, *Salmonella*, *Pasteurella*, postweaning multisystemic wasting syndrome (PMWS) (all endemic in US commercial swine), and any enteric or respiratory disease with fever that is unresponsive to antibiotics [62]. Floegel-Niesmann et al. [66] evaluated the virulence of recent CSF strains and concluded that clinical diagnosis would

be difficult up to 14 days post infection. Still, 75% or more of outbreaks in Germany and The Netherlands were detected by clinical signs [67]. Fever and apathy or fever and ataxia were the most prominent clinical signs reported by veterinarians and farmers during the Netherland outbreak [64].

The United States does have a CSF surveillance plan. The objectives are to allow for rapid detection, monitor the risk of introduction and CSF status in other countries, and to demonstrate freedom of disease, which is especially important for trading purposes. A passive surveillance plan relies on reporting by veterinarians, producers, diagnostic labs, and slaughter plants of pigs with clinical signs similar to CSF. Once the area veterinarian in charge (AVIC) is notified, a foreign animal disease diagnostician (FADD) will be sent to investigate and collect appropriate samples which will then be shipped to the Foreign Animal Disease Diagnostic Laboratory (FADDL) at Plum Island, New York. The United States also actively performs surveillance of high-risk swine populations, such as waste feeding operations, condemned pigs at slaughter facilities and periodically, feral swine. Twenty-six high-risk states and Puerto Rico have been identified for sample collection. Eligible samples from sick pigs received by a CSF-approved National Animal Health Laboratory Network (NAHLN) laboratory can be tested [68].

## ACKNOWLEDGMENTS

The authors thank Peter Bahnson, University of Wisconsin, for early discussions and ideas about the overall chapter structure and content.

## REFERENCES

1. USDA, National Agricultural Statistics Service (2002). *2002 Census of Agriculture, Ranking of 2002 Market Value of Agricultural Products Sold*. http://www.nass.usda.gov/census/census02/topcommodities/topcom_US.htm.
2. USDA, National Agricultural Statistics Service (2002). *2002 Census of Agriculture, Table 50. Selected Characteristics of Farms by North American Industry Classification System*, http://www.nass.usda.gov/census/census02/volume1/us/st99_1_050_050.pdf.
3. USDA, National Agricultural Statistics Service (2002). *2002 Census of Agriculture, Table 16. Beef Cow Herd Size by Inventory and Sales*, http://www.nass.usda.gov/census/census02/volume1/us/st99_1_014_016.pdf.
4. USDA, ERS, WASDE (2002). www.usda.gov/oce/commodity/wasde/ –accessed 10-12-06 and 06-26-07.
5. NAHMS (1999). *Part 1. Baseline Reference of Feedlot Management Practices*, http://www.aphis.usda.gov/vs/ceah/ncahs/nahms/feedlot/.
6. NAHMS. (1997). *Part 1: Reference of 1997 Beef Cow-Calf Management Practices*, http://www.aphis.usda.gov/vs/ceah/ncahs/nahms/beefcowcalf/beef_cowcalf_other.
7. NAHMS (1997). *Part 3: Reference of 1997 Beef Cow-Calf Production Management and Disease Control*, http://www.aphis.usda.gov/vs/ceah/ncahs/nahms/beefcowcalf/beef_cowcalf_other.
8. NAHMS. (1997). *Part 2: Reference of 1997 Beef Cow-Calf Health and Management Practices*, http://www.aphis.usda.gov/vs/ceah/ncahs/nahms/beefcowcalf/beef_cowcalf_other.
9. NAHMS (1999). *Part II: Baseline Reference of Feedlot Health and Health Management*, http://www.aphis.usda.gov/vs/ceah/ncahs/nahms/feedlot/.

10. NAHMS (1999). *Part III. Health Management and Biosecurity in U.S. Feedlots*, http://www.aphis.usda.gov/vs/ceah/ncahs/nahms/feedlot/.
11. www.nass.usda.govpublication/statistical highlights.
12. Pedersen, J. (1999). By the Numbers. Poultry USA, February, 2007:12–64.
13. Agri Stats, Inc. (2007). Fort Wayne, Agri Stats Inc., Indiana, Jan.–June 2007, 317–319.
14. Agri Stats, Inc. (2007). Agri Stats Inc., Indiana, Jan.–June 2007, 336–339.
15. USDA, National Agricultural Statistics Service (2007). *Statistical Highlights 2006/2007*, http://www.nass.usda.gov/Publications/Statistical_Highlights. Accessed November 11, 2007.
16. Martinez, S. W. USDA, Economic Research Service (2002). *Current Issues in Economics of Food Markets: A Comparison of Vertical Coordination in the U.S. Poultry, Egg, and Pork Industries*. Agriculture Information Bulletin 2002 No. 747-05.
17. Haley Mildred, M. (2007). USDA, Economic Research Service. *Market Integration in the North American Hog Industries*, http://www.ers.usda.gov/publications/ldp/NOV04/ldpm12501/ldpm12501.pdf. Accessed July 22, 2007.
18. NAHMS (2007). *Part 1: Reference of Swine Health and Management Practices in the United States, 2006*, http://nahms.aphis.usda.gov/swine/swine2006/Swine2006_Pt1.pdf. Accessed November 1, 2007.
19. Lawrence, John D., and Glenn, G. (2007). *Production and Marketing Characteristics of U.S. Pork Producers, 2006*. Working Paper 07014, Iowa State University. http://www.econ.iastate.edu/research/publications/viewabstract.asp?pid = 12828. Accessed November 1, 2007.
20. Shields Dennis A., and Mathews , Kenneth H. USDA, Economic Research Service (2003). *Interstate Livestock Movements*, http://www.ers.usda.gov/publications/ldp/jun03/ldpm10801/ldpm10801.pdf. Accessed July 23, 2007.
21. Meuwissen , Miranda P. M., Horst , Suzan H., Huirne , Ruud B. M., and Dijkhuizen, A. A. (1999). A model to estimate the financial consequences of classical swine fever outbreaks: principles and outcomes. *Prev. Vet. Med.* **42**, 249–270.
22. USDA, National Center for Import and Export (2007). http://www.aphis.usda.gov/vs/ncie/swine_manual/exe-summary.html-accessed 9-4-07.
23. National Institute for Animal Agriculture (2007). *Swine Health Report*, Summer.
24. Kosal, M. E., and Anderson, D. E. (2004). An unaddressed issue of agricultural terrorism: a case study on feed security. *J. Anim. Sci.* **82**, 3394–3400.
25. Schleifer, J. H., Juven, B. J., Beard, C. W., and Cox, N. A. (1984). The susceptibility of chicks to Salmonella Montevideo in artificially contaminated poultry feed. *Avian Dis*. **28**(2), 497–503.
26. McIlroy, G. S. (1998). Control of salmonella contamination of poultry feeds. In *Proceedings of International Symposium on Food-Borne Salmonella in Poultry*, R. K. Gast, and C.L. Hofacre, Eds. July 25-26, 1998, Baltimore, MD, pp. 83–87.
27. Hofacre, C. L., White, D. G., Maurer, J. J., Morales, C., Lobsinger, C., and Hudson, C. (2001). Characterization of antibiotic-resistant bacteria in rendered animal products. *Avian Dis.* **45**, 953–961.
28. Stärk, K. D. C. (1999). The role of infectious aerosols in disease transmission in pigs. *Vet. J.* **158**, 164–181.
29. Radostits, O. M. (2001). Health and production management in swine herds. *Herd Health: Food Animal Production Medicine*, 3rd ed. WB Saunders, Philadelphia, PA, pp. 635–764.
30. Winkler, K. C. (1973). The scope of aerobiology. In *Airborne Transmission and Airborne Infection. IVth International Symposium on Aerobiology*, J. F. Ph. Hers, and K. C. Winkler, Eds. Oosthoek Publishing Company, Utrecht, pp. 1–11.
31. Rankin J. D., and Taylor, R. J. (1969). A study of some disease hazards which could be associated with the system of applying cattle slurry. *Vet. Rec.* **85**, 578–581.

32. Boutin, P., Torre, M., Serceau, R., and Rideau, P. J. (1988). Atmospheric bacterial contamination from land-spreading of animal wastes: evaluation of the respiratory risk for people nearby. *Agric. Eng. Res.* **39**, 149–160.
33. Fišer, A., and Král, F. (1969). Air temperature and air humidity effect on number of air bacteria in piggeries with a different feed technology. *Acta Vet.* **38**, 579–587.
34. Smith, L. P., and Hugh-Jones, M. E. (1969). The weather factor in foot and mouth disease epidemics. *Nature* **223**, 712–715.
35. Cox, C. S. (1989). Airborne bacteria and viruses. *Sci. Prog.* **73**, 469–500.
36. Smith, J. H., Boon, C. R., and Wathes, C. M. (1993). Dust distribution and airflow in a swine house. In *Livestock Environment IV. 4th International Symposium*, E. Collins, and C. Boon, Eds, Amercian Society of Agricultural Engineers, pp. 657–662.
37. Sellers, R. F. (1971). Quantitative aspects of the spread of foot-and-mouth disease. *Vet. Bull. Weybridge* **41**, 431–439.
38. Heber, A. J., Stroik, M., Nelssen, J. L., and Nichols, D. A. (1988). Influence of environmental factors on concentrations and inorganic content of aerial dust in swine finishing buildings. *Trans. Am. Assoc. Agric. Eng.* **31**, 875–881.
39. Hartung, J. (1994). The effect of airborne particulates on livestock health and production. In *Pollution in livestock production systems*, I. Ap Dewi, R. F. E. Axford, I. F. M. Marai, and H. M. E Omed, Eds. CAB International, Oxon, pp. 55–69.
40. Amass, S. F. (2005). Biosecurity: reducing the spread. *Pig. J.* **56**, 78–87.
41. Whiteford, A. M., and Shere, J. A. (2004). California experience with exotic newcastle disease: a state and federal regulatory perspective. *Proceedings of 53rd Western Poultry Disease Conference*. Sacramento, CA, March 7–9, 2004, 81–84.
42. Fichtner, G. J. (1986). The Pennsylvania/Virginia experience in eradication of avian influenza (H5N2). *Proceedings of the 2nd International Symposium on Avian Influenza*. Athens, GA, Sept. 3–5, 1986, 33–40.
43. Perdue, M. L., and Swayne, D. E. (2005). Public health risk from avian influenza viruses. *Avian Dis.* **49**, 317–327.
44. Cooperative Control and Eradication of livestock or poultry diseases. Code of Federal Regulations:9. subsection 53.1.
45. Poultry Improvement – Sub Chapter G. National Poultry Improvement Plan. Code of Federal Regulations:9. subsections 145, 146, 147.
46. Swayne, D. E., and Halvorson, D. A. (2003). Influenza. In *Diseases of Poultry*, 11th ed., Y. M. Saif, Ed. Iowa State Press, pp. 135–160.
47. Benson, E., Malone, G. W., Alphin, R. L., Dawson, M. D., Pope, C. R., and Van Wicklen, G. L. (2007). Foam-based mass emergency depopulation of floor-reared meat-type poultry operations. *Poult. Sci.* **86**, 219–224.
48. Wilkinson, K. G. (2007). The biosecurity of on-farm mortality composting. *J. Appl. Microbiol.* **102**, 609–618.
49. Knowles, N. J., Samuel, A. R., Davies, P. R., Midgley, R. J., Valarcher, J. F. (2005). Pandemic strain of foot-and-mouth disease virus serotype O. *Emerging Infect. Dis.* **11**(12), 1887–1892.
50. USDA, Economic Research Service (2000). *Taiwan's Hog Industry –3 Years After Disease Outbreak; Agricultural Outlook*, October 2000, pp. 20–23.
51. DEFRA (2007). http://www.defra.gov.uk/animalh/diseases/fmd/pdf/economic-costs_report.pdf, accessed 9-4-07.
52. National Science and Technology Council, Subcommittee on Foreign Animal Disease Threats, Committee on Homeland and National Security February 16, (2007). *Protecting Against High Consequence Animal Diseases: Research and Development Plan for 2008-2012*.

53. Bates, T. W., Thurmond, M. C., and Carpenter, T. E. (2003). Results of epidemic simulation modeling to evaluate strategies to control an outbreak of foot-and-mouth disease. *Am. J. Vet. Res.* **64**(2), 205–210.

54. Bates, T. W., Carpenter, T. E., and Thurmond, M. C. (2003). Benefit-cost analysis of vaccination and preemptive slaughter as a means of eradicating foot-and-mouth disease. *Am. J. Vet. Res.* **64**(7), 805–812.

55. Sellers, R. F., and Gloster, J. (1980). The northumberland epidemic of foot-and-mouth disease, 1966. *J. Hyg.* **85**(1), 129–140.

56. Cox, S. J., Voyce, C., Parida, S., Reid, S. M., Hamblin, P. A., Paton, D. J., and Barnett, P. V. (2005). Protection against direct-contact challenge following emergency FMD vaccination of cattle and the effect on virus excretion from the oropharynx. *Vaccine* **23**, 1106–1113.

57. Dahle, J., and Liess, B. (1992). A review on classical swine fever infections in pigs: epizootiology, clinical disease and pathology. *Comp. Immunol. Microbiol. Infect. Dis.* **15**(3), 203–211.

58. United States Animal Health Association (USAHA) (1998). Hog Cholera In *Foreign Animal Diseases*. Pat Campbell & Associates and Carter Printing Co., Richmond, VA., pp. 273–282.

59. Artois, M., Depner, K. R., Guberti, V., Hars, J., Rossi, S., and Rutili, D. (2002). Classical swine fever (hog cholera) in wild boar in Europe. *Rev. Sci. Tech.* **21**(2), 287–303.

60. Dijkhuizen, A. A. (1999). The 1997-1998 outbreak of classical swine fever in The Netherlands. *Prev. Vet. Med.* **42**(3-4), 135–137.

61. de Vos, C. J., Saatkamp, H. W., and Huirne, R. B. M. (2005). Cost-effectiveness of measures to prevent classical swine fever introduction into The Netherlands. *Prev. Vet. Med.* **70**(3-4), 235–256.

62. Moennig, V., Floegel-Niesmann, G., and Greiser-Wilke, I. (2003). Clinical signs and epidemiology of classical swine fever: a review of new knowledge. *Vet. J.* **165**, 11–20.

63. Straw, B. E. (2006). *Diseases of swine*, 9th ed. Blackwell Publishers (US), Ames, IA.

64. Elbers, A. R. W., Stegeman, A., Moser, H., Ekker, M. H., Smak, J. A., and Pluimers, F. H. (1999). The classical swine fever epidemic 1997–1998 in The Netherlands: descriptive epidemiology. *Prev. Vet. Med.* **42**, 157–184.

65. Edwards, S. (2000). Survival and inactivation of classical swine fever virus. *Vet. Microbiol.* **73**, 175–181.

66. Floegel-Niesmann, G., Bunzenthal, C., Fischer, S., and Moennig, V. (2003). Virulence of recent and former classical swine fever virus isolates evaluated by their clinical and pathological signs. *J. Vet. Med.* **B 50**, 214–220.

67. Elbers, A. R. W., Bouma, A., and Stegeman, J. A. (2002). Quantitative assessment of clinical signs for the detection of classical swine fever outbreaks during an epidemic. *Vet. Microbiol.* **85**, 323–332.

68. USDA (2007). *Procedure Manual for Classical Swine Fever (CSF) Surveillance*, http://www.aphis.usda.gov/vs/nahss/swine/csf/CSF_procedure_manual_2007.pdf. Accessed November 2, 2007.

## FURTHER READING

Iowa State University *The Center for Food Security and Public Health website*, http://www.cfsph.iastate.edu/

National Research Council of the National Academies (2005). *Animal Health at the Crossroads: Preventing, detecting and diagnosing animal diseases*. The National Academies Press, Washington, DC.

# RISK ASSESSMENT, RISK MANAGEMENT, AND PREVENTIVE BEST PRACTICES FOR RETAILERS AND FOODSERVICE ESTABLISHMENTS

JULIE A. ALBRECHT
*University of Nebraska-Lincoln, Lincoln, Nebraska*
CATHERINE H. STROHBEHN
*Iowa State University, Ames, Iowa*

## 1 INTRODUCTION

Projected sales for the foodservice industry for 2007 were $537 billion with $1.5 billion of food sold on a typical day. There is a great deal of concentration of ownership within the food industry at all levels: production, processing, distribution, and retail sales. With the population of Americans shifting from rural to urban locations, the majority of consumers' food is purchased from retail and foodservice establishments, which rely on food wholesalers to procure food from food manufacturing plants. These food facilities are inspected at least once per year, but potential for intentional contamination through physical or chemical agents can occur at any time.

The restaurant industry employs an estimated 12.9 million people, 9% of the US workforce, making it the largest employer outside of government [2]. The foodservice industry is expected to add two million jobs over the next decade, with total employment projected to reach 14.8 million in 2017. The majority of foodservice workers (83%) are employed in privately owned eating and drinking establishments.

The largest category of commercial eating places is restaurants, with projected market sales of $491 billion in 2007. Although more than 7 out of 10 eating and drinking places are single unit, independently owned operations [3], those establishments that are part of multiunit or chain organizations are serving food to greater numbers of people.

Census data from 2000 showed increasing diversity in the US population with an increase of 30% for Hispanics and growth in the other races of 29%. Data from the National Restaurant Association (NRA) in 2006 found about one of every four restaurant employees (26%) was reported as speaking a foreign language at home (predominately Spanish) compared to 18% of the overall population [4]. Foreign born workers represented 21% of foodservice employees in 2004 [2] Because the foodservice industry hires a large diverse population, reaches a large number of customers and generates a large market share, this industry may be potential target of intentional contamination of the United States food supply.

The World Health Organization [4] identified food terrorism as an act of deliberate contamination of food for human consumption with chemical, biological, or radionuclear

agents for the purpose of causing injury or death to civilian populations, and/or disruption to social, economic and political stability.

In a keynote address at Institute of Food Technologists (IFT's) Fourth Research Summit in April of 2005, Hedberg from the University of Minnesota's School of Public Health detailed challenges of defending global food systems from terrorist attacks: global sourcing, increased fresh produce consumption from nondomestic sources, increased number of meals consumed away from home, increased centralization of production (with larger batch sizes and distribution networks) [5]. Hedberg also commented on the paradigm shift from a food safety focus (which relies on forensic review of events) to a food defense approach (which predicts risks and implements prevention steps). Another speaker at the conference, Shaun Kennedy from the National Center for Food Protection and Defense, noted that terrorists do not fear retribution as many are committed to sacrificing their own lives to achieve their aims. Multiple detection techniques are being developed, which may provide methods to prevent catastrophic consequences of a terrorist attack on the food supply, yet there are limitations with these techniques [5].

These threats can be presented through physical infrastructures or through humans. The reality of potential threats to our food and water was intensified after the terrorist attacks of September 11, 2001. Federal legislation has been enacted to provide some degree of protection through the ability to trace back food products, as this has been identified as a critical step to mitigate public health impacts. The Bioterrorism Act of 2002 required those involved in the food chain (producer, processor, wholesaler, or retailer) to be able to identify their food sources, minimally to the immediate past link. The final rule issued in December, 2004, required establishment and maintenance of records by those who manufacture, process, pack, transport, distribute, receive, hold or import food in the United States. Country of origin labeling (COOL) legislation was passed to ensure that provenance of meat items was communicated to consumers.

Motivations to harm food include purposes of terrorism or criminal activity, such as corporate sabotage, yet results of causing harm or creating an atmosphere of fear and panic are the same. There are 15 reports of serious attacks on the food chain from 1961 to 2005. These have been limited in the United States with only two occurrences [6]. The most serious attack on the food chain in the United States was due to Rajneeshees (an Oregon-based cult) contaminating food at 10 restaurants with *Salmonella typhimurium*, causing 751 illnesses in 1984 [7]. Another attack was the intentional poisoning by a supermarket employee 250 lb of ground beef in 2002 which caused 111 cases of illness [6]. The scope of the threat to agriculture from bio- or chemical attacks. particularly for livestock producers, was illustrated in the United Kingdom with cases involving food-and-mouth disease (FMD) and oovine spongiform encephalopathy (BSE). Although uniteritional, the impact on the food producer and the food industry was wide spread.

Operators in the retail food industry need to assess risks, implement strategies to manage these risks, and identify the best practices that will prevent threats to food while in their custody. Organizational policies and written standard operating procedures (SOPs) can provide internal guidance. The food and drug administration (FDA) has developed an educational program to raise awareness among government agency and industry representatives about food defense issues and emergency preparedness. The ALERT program title is based on the acronym of key elements assure, look, employees, reports, and threats [8].

## 2 RISK ASSESSMENT

Emergency management literature emphasizes the importance of assessment as a means of developing response scenarios. These vulnerability assessments are a critical part of a food defense plan and several tools are available within sectors of the industry. One tool used is the CARVER+Shock process that can help organizations focus on intentional system vulnerabilities, which was discussed in an earlier article.

A traditional supply chain is the integrated network of entities involved in the manufacture of goods (which includes procurement of raw materials and assembly into final product), transportation to distributors, and ultimately preparation and/or sale to final customers. Multiunit corporate foodservice chains are coordinating their own supply chains as a control measure to ensure security and safety of the food product. The intention is to protect the safety, quality, and quantity of products. This includes maintaining product integrity so that it is tamper resistant and that substitution of ingredients or final products is prevented. Larger food-related organizations may be better positioned to implement assessment and prevention steps, yet their investment is likely to be driven by potential widespread impact and economic consequences should an attack occurs. Parallels can be drawn with outbreaks of food borne illnesses within one specific restaurant chain, and its resultant destruction [9].

Terrorists may not attack smaller food industry organizations as resultant impact would be low, both in terms of public health and economics. However, an orchestrated simultaneous attack on multiple, smaller food industries could achieve the same outcomes as one large attack on a multinational company. Thus, all food industries are advised to consider potential threats. For wholesale and retail (foodservice and grocery stores) links of the food chain, the focus should consider physical and human elements [10, 11, 12].

Foodservices vary considerably with regards to market niche, menu items and needed raw ingredients, amount of preparation required, hours of operation and service, access to storage and production areas, frequency of deliveries and regularity of these, and number of employees on any one shift. Generally, all employees receive some basic food safety training and are aware of some security issues. Enhancing the training to consider food defense is needed [13].

### 2.1 Perceptions of Risk

In an assessment conducted by one of the authors [14] at three Midwest supplier food shows 393 respondents representing a variety of institutional and commercial foodservices or retail grocery stores indicated their levels of concern about an attack on their food supply, their perceptions of the likelihood of this occurring, and whether any changes had occurred in the past year. Approximately 82% indicated they were very or somewhat concerned about intentional food contamination, although only 35% thought something could happen in their businesses. Approximately 25% reported that their organization conducts background checks on prospective employees, limits employee access within physical structures, and inspects their facilities. About 12% (50 of 393 respondents) reported that an identification system for employees is in place and 55 said that changes had been made in reporting systems, such as installation of security cameras and locks. Of the 393 respondents, 43 indicated that changes had been made with regard to customer access.

Food security practices in Kansas schools and health care facilities were investigated for foodservice directors' perceptions of their operations' risk of bioterrorism [15]. The

authors found that limited access to chemicals and storage was perceived as the most important practice to protect operations from food defense threats. The least important practices perceived by these foodservice directors to protect their facilities from possible food threats were updating contact information and building a network outside of their operation. In addition, Yoon and Shanklin reported that foodservice operators implemented preventative measures where they perceived a risk, that is, chemical use and storage. In their study, the largest gap between perception and practice was communication.

## 2.2 Assessment Steps

As part of the risk assessment phase, organizations are encouraged to (i) develop a response team, (ii) review and develop written policies and SOPs (focus on human element), (iii) assess vulnerabilities of physical elements (facility, equipment, utilities, and infrastructure), and (iv) review and develop a training program for all organizational staff.

***2.2.1 Response Team.*** It is recommended that a team should be formed representing all functional areas of the organization and all levels of employees. Team members should be knowledgeable about the operation and trustworthy, as risk assessments and management plans are considered confidential and available on a need-to-know basis. The team for smaller organizations might consist of three or four members. Infusion with an organization's food safety plan has been suggested [10]. Larger organizations have established Hazard Analysis Critical Control Points (HACCP) plans, albeit frequently only seen at the management level.

***2.2.2 Review Policies and Procedures.*** The foundation for any food safety plan is written policies and SOPs. Foodservice SOPs are available from a number of sources in the public domain, such as the National FoodService Management Institute and Iowa State Universities Food Safety Project (See www.nfsmi.org and www.iowahaccp.iastate.edu for SOPs available in Microsoft Word format so that organizations can easily modify as needed). Written documentation is needed for food defense as well. Current hiring procedures should be reviewed and job descriptions be updated to include responsibilities for food defense and safety. Documentation of current practices should also be reviewed, such as sign-in sheets and building entry logs. Restriction of employee access to designated work areas is suggested. Written policies and SOPs should also consider customers. The review should consider access by those internal (i.e. employees) and external (delivery personnel, repair workers and contract personnel, and customers) to the organization, and screening practices.

***2.2.3 Access.*** A photo identification badge easily seen on uniforms of employees is one way to verify access is valid. Job descriptions should include the statement that photo identifications are worn all the time while at work. Some organizations may issue color-coded uniforms to designate areas of operation the employee should be. Wholesalers who supply foodservice operations should have their own controls to ensure that employees are screened before hiring. A wholesale food distributor would want to limit access to inventory only to screened and bonded employees. Identification as an employee of the wholesaler company is frequently achieved with use of uniforms and wholesale company vehicles. However, because these could be hijacked, the use of photo identification is also recommended. Deliveries should occur ONLY while employees are present. In some

smaller school districts, the dairy vendor may request a key to make milk deliveries early in the morning before the opening of the building. This practice is not recommended.

Repair personnel and contractors should stop at the organizational office for check-in and be escorted to the work area by a supervisory employee. Their presence should be monitored while at the work site. Subcontractors, suppliers, repair persons, and others should not be given unrestricted access while on a wholesale or retail foodservice organizations' premises.

***2.2.4 Screening.*** As part of the selection process, employees should be screened for any physical or mental characteristics that may present a threat to the organization. The selection process should be documented so that the desired employee characteristics are tied to the job description and are a bona fide occupational qualification. Thus, the job description should include a statement regarding employee's responsibility in risk assessment. Often a financial background check is conducted on a person who will work with money just as organizations may periodically screen e-mail messages and internet traffic on workplace computers to ensure that inappropriate websites are not visited.

***2.2.5 Facility Assessment.*** An assessment of the operation considering the facility and property itself, layout and design of the building that allow for unchecked access, and infrastructure, such as utilities or transportation vehicles, should be conducted. Potential risks should be identified and procedures be developed to mitigate these risks [16]. All properties of the organization, including parking lots should be reviewed on a regular basis. Although there are governmental regulations that provide some safeguards, industry organizations should recognize the inherent benefits of regularly reviewing operations. Wholesalers and foodservices should incorporate risk assessments into the daily operational regime. Emergency contact information should be readily available in each work area for management fire, FEMA, police, building security, and so on, so that employees are knowledgeable about response authorities and response procedures.

***2.2.6 Facilities.*** Access onto the grounds of the retail foodservice and wholesaler should be screened so that only necessary individuals or vehicles are allowed to enter. Perimeter fencing should be in place and be regularly checked. Exterior lighting of the grounds and parking areas should be in place, particularly by entry areas. Access to facility grounds and to facilities should be restricted to individuals with a legitimate reason for their presence. Physical barriers, such as locked doors and keys restricted to a few screened individuals, can protect against tampering with equipment, theft or substitution of product, or adulteration of the food products. Unlocked doors during operation provide open access in many food and chemical storage areas and in the food production and service areas.

***2.2.7 Layout and Design.*** Identify areas for restricted access, such as food or chemical storage areas. In many organizations, access to these is open during working hours. Often, surplus inventory (food and chemicals) is kept in areas hard to monitor. It is recommended that employees, customers, and contractors/repair persons have access ONLY to areas necessary to complete their work. Addition of doors, security gates, or other physical barriers can help prevent transition. Reconfiguration of product flow may also improve work efficiencies and product safety.

***2.2.8 Infrastructure.*** Vehicles are used in transporting food ingredients and menu items to and from foodservices. All retail food operations need a potable water supply and an energy source (gas or electric). Mail and computer systems are other potential attack points.

***2.2.9 Training.*** In the food security plan, management needs to identify training needs (annual or semiannual of key points of the plan). The training program could include introduction and implantation of new policies and procedures that are made because of the food security plan, simulation of what to do in a tampering event, emergency procedures/evacuation simulations, and so on.

***2.2.10 Monitoring.*** Continual assessment of potential risks from employees, contractors, customers, or the public is needed. Some organizations utilize third party monitoring programs, such as undercover patrons, and receive reports on potential risks. The use of security cameras has also increased. These can be a valuable tool to document compliance and assess future training needs.

A checklist format can be used on a daily or weekly basis by rotating key personal to ensure that vulnerabilities have not been attacked and ownership is spread among all staff members (Table 1). Employees should be aware of any existing vulnerabilities and trained to report any observations. Responsibility to continually observe for vulnerabilities should be included in job descriptions and as part of the review process. These reports should be formalized with a written plan. Physical vulnerabilities can be minimized with prompt attention.

## 3 RISK MANAGEMENT

Many food defense action steps mirror those in place to ensure the safety of food products, such as a HACCP plan and SOPs. Although the food security and HACCP plans are similar in nature and development process, two separate documents should be prepared. The food security plan needs to be individualized for each organization. Foodservice and grocery store managers need to prepare for the possibility that tampering or other criminal and terrorist attacks could occur. A food security plan needs to be in place as a proactive measure—including elements for evacuation, segregation of affected products, local response network, and availability of emergency contact information as well as training for staff about communications internally and externally during a crisis. Retail food managers need to have a broader perspective—should think all possibilities and methods that can compromise integrity of products and facilities.

### 3.1 Plan Development

Managers should select a team of knowledgeable individuals to develop the food security plan and conduct assessments of food security procedures and operations. It is recommended that the plan be kept confidential, but the strategies for employee training and communication, both internal and external, should be included in the plan.

***3.1.1 Communication.*** The food security plan should lay out a strategy for internal and external communication.

**TABLE 1 Food Defense Checklist for Retail Foodservice Operations**

| | Yes | No | N/A |
|---|---|---|---|
| Facility security | | | |
| Facility has a written food defense plan | | | |
| A designated person or team plans and implements food defense policies | | | |
| Food defense practices are evaluated and documented at least annually | | | |
| Emergency contact list is available to all employees | | | |
| Managers conduct a daily walk-through inspection of the operation | | | |
| The outside of facility is adequately lighted | | | |
| Facility is locked and secured when closed | | | |
| Exterior doors are locked at all times (except customers' entrance) | | | |
| Keys to access kitchen and food and chemical storage areas are restricted to foodservice management staff | | | |
| Access to food preparation areas is controlled for all visitors and nonfoodservice employees, including cleaning crews, delivery vendors, and contractors | | | |
| Visitors are required to sign in at the main office, show picture ID, and explain the purpose of their visit. A visitor badge is worn | | | |
| Personnel | | | |
| References for new employees are verified and backgrounds are checked | | | |
| Managers are alert for unusual employee and customer behavior (i.e. workers staying after shift and arriving early) | | | |
| Personnel have been trained in food defense policies and procedures | | | |
| Customers are restricted from entering storage and preparation areas | | | |
| Visitors are supervised while in food production areas | | | |
| Terminated employees lose all means of access to facility (keys and passwords); this may mean locks are rekeyed and passwords are changed | | | |
| Storage is provided for employees' personal items so that these are not allowed in food preparation areas | | | |
| Receiving | | | |
| Food is purchased only from approved vendors | | | |
| A delivery schedule is maintained | | | |
| Deliveries are verified against purchase orders | | | |
| Delivery personnel are monitored while at the facility | | | |
| Packaging integrity of received products is verified | | | |
| Food and supplies are placed immediately in appropriate storage upon receipt | | | |

**TABLE 1 (*Continued*)**

| | Yes | No | N/A |
|---|---|---|---|
| Food preparation areas | | | |
| Self-service stations (such as food bars and buffets) are monitored at all times by foodservice employees | | | |
| Employees are trained to check ingredients before use to note unusual smells, defective products, and expiration dates, and to know appropriate actions to take if there is a problem | | | |
| Records are maintained to ensure traceability of raw ingredients back to suppliers | | | |
| Procedures are in place for safely handling and disposing of contaminated products | | | |
| Storage areas | | | |
| Access to all food product and chemical storage areas is secured and controlled | | | |
| Chemicals are stored in a locked area, outside of food preparation areas | | | |
| Chemical use is monitored to prevent deliberate food contamination | | | |
| Employees are trained to properly use chemicals to prevent food contamination and protect human safety | | | |

*Food Defense* in foodservice operations refers to the process of guarding the operation against intentional acts of contamination or tampering. This checklist will help you assess the security of your operation. Check YES, NO, or N/A (not applicable) for each practice in your operation. Develop a plan for addressing practices that were marked NO.

The *internal communication plan* should include training of supervisory staff to be observant of signs of tampering or unusual behavior. A clear reporting system of such events needs to be established so that information is transferred to the proper channels and appropriate actions can be taken in a timely manner. An updated list of key contacts (fire, police, etc.) should be maintained and readily available to key personnel. Employee training should include awareness about suspicious activity, the appropriate reporting channel, and response required of employees for the operation. Who and what will be communicated internally to employees should be included if an event occurs that jeopardizes the integrity of the facility or food products. In addition, signage at designated points to restrict access to employees, delivery and repair personnel, and the public should be an integral component of the communication plan.

The *external communications* section should identify a designated spokesperson knowledgeable about the organization and the plan. This person should be capable of effective communication with press and authorities. This part of the food security plan should include a crisis management strategy to prepare for and respond to any suspicious activity. This crisis management strategy may be similar to an existing natural disaster plan already in place in the food establishment.

***3.1.2 Procedures to Ensure Security.*** The food security plan should include procedures to ensure security of the physical facility and human elements.

*Facility security* should include access limited to only authorized personnel. At some locations, this may mean perimeter fencing and/or security guards and check-in stations or designated employee entrances. Lighting of outside areas should be evaluated and changes be made to provide adequate lighting for high visibility in parking lots, delivery areas, and other access area.

Designated parking areas for staff should be available. Swipe cards or pass codes should be used at employee entrances. Security badges with codes (uniform colors, electronic bar codes, etc.) to restrict access to only necessary areas. Use of security cameras external to the building and internally in staff and public areas is encouraged. These can be useful as a deterrent and as a reconstruction aid in the event of an incident and may lower insurance premiums. Door locks with limited distribution of keys is also recommended.

What we often see at retail foodservices, particularly those not part of multinational chains, is open access to food storage and production areas during hours of operation. Those intended for direct harm or theft can often easily enter the facility and access food and/or chemical storage areas. Posing as a customer, delivery or repair person, or new employee is a way by which access to vulnerable areas can be gained.

A defined product recall plan should be identified for any product that is considered unusual or suspicious. This recall plan may be similar to an existing policy for a product that is a food safety concern.

The food security plan should include routine security checks of facilities and of procedures established by the team and a third party may be employed to conduct such an audit.

***3.1.3 Training Programs.*** Training plans should raise awareness in staff about potential risks, and that natural hazards, such as a fire which would cause an evacuation, might be part of an intentional attack on the organization.

Management should provide training to all staff about need for building and product security. Part of the training should include importance of restriction to work areas, reasons for background checks and employee screening, and need to follow policy with regards to security measures (no loaning of keys or passwords). The job description should include a statement with regards to compliance with all operational policies, including consequences identified for noncompliance. Staff should also be provided with storage areas for personal items to limit what is brought into the production areas. Management should encourage all staff to be alert to actions of others and to report any unusual or suspicious behavior—such as reporting early or staying late without any reason, accessing files or information about areas outside of their work zones, asking questions about security measures or other sensitive issues, or bringing cameras to work. Management is advised to consider restricted use of cell phones during work day due to the ability to take photos.

***3.1.4 Implementation and Evaluation.*** After training, new policies and procedural changes can be implemented with subsequent changes introduced as steps are added to the food security plan. It is not necessary to have a complete plan in place with one rollout.

The team should consider an annual review of the food security plan. Reports of concern (inventory records, supplier receipts, etc.) should be evaluated by the appropriate management staff on a regular basis to verify that the plan is working. If the plan is not

working, the plan needs to be modified and changes be implemented to ensure the security of the facility and food products. The team should meet on a quarterly basis or as needed to consider events or changes noted/needed. An event that occurs nationally, such as a tampering activity in a similar industry, should trigger a review of the existing plan. Management should consider instituting a reward system for employee compliance.

## 4 PREVENTATIVE BEST PRACTICES

The Food Security Plan development should include the areas listed in Table 2. To aid in the development of your food security plan, current organizational policies and procedures should be reviewed. HACCP Plans and SOPs are important to review as part of the Food Security Plan development phase, and for continuous improvement of the plan.

**TABLE 2 Components of the Food Security Plan**

| Area of Concern | Check for Inclusion in Plan |
|---|---|
| *Human Element* | |
| Management | |
| Assemble a team | |
| Determine a designated spokesperson. Assign responsibilities for security to authorized personnel and incorporate into job descriptions | |
| Develop a crisis management strategy | |
| Review existing facility layout/design, policies and procedures, including food safety plans (i.e. HACCP) and SOPs | |
| Examine existing records related to security issues, such as receiving and purchasing. Establish appropriate records and/or revise existing records to be able to track previous link of the food chain | |
| Develop a system for reporting suspicious behavior | |
| Develop a plan for evacuation in light of various scenarios—fire, water outages, and so on | |
| Maintain a current list of emergency response organizations in the community | |
| Develop and post signage in facility restricting access as appropriate | |
| Provide training for employees at least annually | |
| Staff and employees | |
| Review existing policies and procedures about hiring practices including background checks, job descriptions, performance appraisals, reward systems, training logs, sign-in sheets, and so on | |
| Provide recognizable forms of identification for employees. These forms should include name badges with photo identification and may include specific uniforms | |

(*continued overleaf*)

**TABLE 2 (*Continued*)**

| Area of Concern | Check for Inclusion in Plan |
|---|---|
| Provide storage for employees' personal items. Restrict types of items that employees can bring to work | |
| Change locks, keys, combinations, codes, passwords, and so on, when employees discontinue employment | |
| Restrict access of employees, delivery, and repair personnel to areas of work | |
| Require annual training for employees, document training, and develop a reward system for application of training content | |
| Public | |
| Restrict access to nonpublic areas | |
| Monitor public areas | |
| *Physical Element* | |
| Physical facility | |
| Provide protection of nonpublic perimeter of facility | |
| Monitor access to nonpublic areas of facility | |
| Use lighting for perimeter of premises, such as parking, delivery areas, and so on | |
| Inspect and evaluate HVAC system, water, and utilities on a regular basis by screened personnel | |
| Operations | |
| Evaluate inspection procedures of incoming products, deliveries, supplies, mail, and so on | |
| Evaluate records for receiving | |
| Monitor food storage areas so access is restricted to authorized personnel only | |
| Monitor chemical storage areas so access is restricted to authorized personnel only. Implement security measures. MSD Sheets should be accessible to all employees | |
| Evaluate vulnerabilities of foodservice and/or retail display areas regularly | |
| Review potential vendors, suppliers, and contractors. Maintain an approved list and monitor access to operation to those on list | |
| Develop security for your computer system. Limit access by nonscreened personnel | |
| Develop a method to validate your program | |

## ACKNOWLEDGMENTS

Table 1 was developed as part of a project funded by the USDA Cooperative States Research, Education and Extension Service, Project No. 2005-51110-03282. The mention of trade or company names does not mean endorsement. The contents are solely the responsibility of the authors and do not necessarily represent the views of USDA.

Prepared by Catherine Strohbehn, PhD, Iowa State University (ISU) Extension specialist; Jeannie Sneed, PhD, former ISU HRIM professor; Paola Paez, M.S., ISU HRIM graduate student; Sam Beattie, PhD, ISU Extension specialist; and Janell Meyer, ISU HRIM Food Safety Project Coordinator. Reviewed by Julie A. Albrecht, Extension specialist, University of Nebraska-Lincoln.

## REFERENCES

1. Food Marketing Institute. Trends 2008. Food Marketing Institute, Aslington, VA.
2. National Restaurant Association (2006b). *State of the Restaurant Industry Workforce: An Overview*, June 2006. Restaurant and Information Services Division. Retrieved December 1, 2006 www.restaurant.org/pdfs/research/workforce_overview.pdf.
3. National Restaurant Association (2006a). *Restaurant Industry Facts*, Accessed December 14, 2006 www.restaurant.org/research/ind_glance.cfm.
4. World Health Organization (2002). *Terrorist Threats to Food: Guidelines for Establishing and Strengthening Prevention and Response Systems*. Retrieved May 10, 2007 www.who.int/foodsafety/publications/fs_management/terrorism/en.
5. Bryant, C., McEntire, J., and Newsome, R. (2005). Defending the Food Supply. Food Technology, August. In *Proceedings of the Terrorism, Pandemics, and Natural Disasters: Food Supply Chain Preparedness, Response, and Recovery Conference*, University of Minnesota, Minnesota, pp. 64–73, November 1, 2006.
6. Mohtadi. H., and Murshid, A. P. (2005). Analyzing Catastrophic Terrorist Events with Application to the Food Industry. *Proceedings of the Terrorism, Pandemics, and Natural Disasters: Food Supply Chain Preparedness, Response, and Recovery Conference*, University of Minnesota, Minnesota, November 1, 2006.
7. Carus, S. W. (2002). *Bioterrorism and Biocrimes: The Illicit use of Biological Agents Since 1990*, Fredonia Books, Amsterdam, the Netherlands.
8. FDA (2006). *ALERT*. Retrieved January 16, 2007. www.cfsan.fda.gov/alert.
9. Lockyer, S. E. (2004). *Chi-Chi's shuts all units: Outback buys site rights: Mexican chain, in Chapter 11, retains brand, operations, recipes, trade secrets*, National Restaurant News. Retrieved June 20, 2007 http://findarticles.com/p/articles/mi_m3190/is-40-38/ai-n6232955.
10. Powitz, R. W. (2007). Food Defense for the Small Retail Operation. *Food Saf. Mag.* **12**(6), 28–33. Retrieved April 15, 2007 www.iowafoodsafety.org.
11. Barringer, A. A. (2007). Staying ALERT about Food Defense. *Food Saf. Mag.* **13**(1), 26–30.
12. FDA (2004). *Guidance for Industry Retail food stores and Foodservice Establishments: Food Security Preventive Measures Guidance*, Retrieved June 20, 2007 http://www.cfsan.fda.gov/guidance.html.
13. NFSMI (2005). *How to Develop a Plan*, Retrieved May 31, 2007. http://foodbiosecurity.nfsmi.org/DevelopingPlan.php.
14. Albrecht, J. A. (2007). Food Biosecurity Eduation, Extension Accomplishments Reporting System, Retrieved september 8, 2008 http://citnews.unl.edu/etension/eass/lib/showReport.cgi?RECORD=4323 up. Unpublished data.
15. Yoon, E., and Shanklin, C. W. (2007). Food Security Practice in Kansas Schools and Health Care Facilities. *J. Am. Diet. Assoc.* **107**, 325–329.
16. Sayer, S. (2006). Think Like a Terrorist. *Food Qual.* **13**(5), 26–28.

## FURTHER READING

National Restaurant Association Educational Foundation (2003). *Food Security: An Introduction*.

NFSMI (2005). *How to Develop a Plan*. Retrieved May 31, 2007 http://foodbiosecurity.nfsmi.org/DevelopingPlan.php.

National Restaurant Association Educational Foundation (2003). *Food Security: An Introduction*. Retrieved October 30, 2008.http://www.nreaf.org/foodsecurity/foodsecurity.asp.

Bruemmer, B. (2003). Food biosecurity. *J. Am. Diet. Assoc.* **103**(6), 687–691.

Sayer, S. (2006). Food Defense at the Federal Level. *Food Qual.* **13**(5), 29–35.

Simmons, K., Harrison, M. A., Hurst, W. C., Harrison, J., Brecht, J., Schneider, K., Simonne, A. and Rushing, J. (2007). Survey of food defense practices in produce operations in the southeast. *Food Prot. Trends* **27**(3), 174–184.

USDA (2004). *Food Defense Strategies–A Self-Assessment Guide for Foodservice Operators*, Retreived May 31, 2007. http://www.health.state.ny.us/enrionmental/indoors/food_safety//food_defense_strategies.

## ADDITIONAL RESOURCES

South Dakota State University (2006). *Food Defense: Security in a Foodservice Operation. An educational video for foodservice managers*.

# RISK ASSESSMENT AND SAFETY OF THE FOOD SUPPLY

LORNA ZACH AND VICKI BIER

*Center for Human Performance and Risk Analysis, University of Wisconsin-Madison, Madison, Wisconsin*

## 1 BACKGROUND

In their seminal paper, Kaplan and Garrick [1] define risk as involving both uncertainty and some kind of loss or damage. Moreover, Zimmerman and Bier [2] state that "Risk assessment is a means to characterize and reduce uncertainty to support our ability to deal with catastrophe through risk management." Thus, we view risk assessment as "a *decision-directed activity*, directed toward informing choices and solving problems," as suggested by the National Research Council [3].

Sometimes, the available choices include waiting for additional information before making a final decision; likewise, effective problem-solving can involve doing additional

research to identify the best solution. Therefore, assessing the uncertainties about the results of a risk assessment can be useful in determining whether additional information is needed, and if so, which information would be most helpful in making a good decision. In fact, the American Industrial Health Council and others [4] have stated that a good risk assessment "explicitly and fairly conveys scientific uncertainty, including a discussion of research that might clarify [and reduce] the degree of uncertainty." Likewise, the National Research Council [5] has recently gone further, recommending that risk assessments should "*characterize and communicate uncertainty and variability in all key computational steps of risk assessment—for example, exposure assessment and dose-response assessment"* (emphasis in original).

As Phillips [6] notes, "Quantifying uncertainty does not create uncertainty. It merely measures and reports the uncertainty that is always there . . . quantified uncertainty better describes what we know, and thus can facilitate better decisions, suggest improvements in our methods, and help direct new research to where it will provide the most benefit." In other words, if a particular risk is highly uncertain, then a good and accurate risk assessment should have large uncertainty bounds. While a lesser degree of uncertainty might be preferable, decision-makers faced with highly uncertain risks are not well-served by focusing on a single best estimate, since this can lead to undesirable "after-the-fact surprises" [4]. Rather, once the nature and magnitude of the uncertainties are known, this knowledge can help decision-makers prioritize not only which protective measures (if any) should be taken in the short term, but also how best to spend their research dollars to reduce risk in the long term, by considering whether the value of additional information [7] in supporting better decisions would outweigh the cost of collecting such information.

This article discusses one particular approach to characterizing uncertainty and variability, as recommended by the National Research Council [5] namely, the use of so-called "two-dimensional" or "second-order" Monte Carlo simulation. We also discuss applications of this method to food safety and related issues, such as agricultural animal disease. Two-dimensional Monte Carlo simulation is typically used in applications of risk assessment to health, safety, and environmental problems, to assess the desirability of possible preventive and/or mitigating measures to help reduce risk. However, it can also be used to assess the desirability of preventive and mitigating measures for intentional threats to homeland security (e.g. intentionally introduced foot-and-mouth disease or food contamination), as will be discussed below.

### 1.1 Uncertainty Versus Variability

When the National Research Council [5] talks about the need to "characterize and communicate uncertainty and variability," they have specific definitions of these terms in mind. For example, Kaplan [8] describes uncertainty assessment as characterizing the scientific "state of knowledge" about an uncertain quantity of interest (e.g. uncertainty about the *average* effectiveness of a vaccine that has not yet been fully characterized), and distinguishes this from "population variability" (e.g. differences in vaccine effectiveness from one person or animal to another). Similarly, Paté-Cornell [9] draws a distinction between "epistemic uncertainty" (i.e. "Uncertainties about fundamental phenomena reflecting incomplete knowledge") and the randomness or "aleatory uncertainty" used to represent "variations in samples (e.g. of temperature readings at a precise moment of the year over several years)."

It is, in principle, possible to have uncertainty with little or no variability; for example, if all people are believed to be equally susceptible to a particular disease agent, but little is known about their level of susceptibility. Similarly, it is possible to have variability without uncertainty; for example, if the dose of some microbial toxin required to cause disease is known quite accurately, but is known to vary based on the age or weight of the exposed individual. However, most real-world situations exhibit both state-of-knowledge uncertainty and population variability.

The distinction between variability and uncertainty is not necessarily fundamental. For example, some sources of uncertainty might be treated as (effectively irreducible) randomness if a decision has to be made in the short term (e.g. in less than a year), but could be researchable through programs that would yield answers in five to ten years. However, if uncertainty and variability are not clearly separated, analysis results can be misunderstood, and options for risk reduction overlooked. For example, for motor vehicles, as Thompson [10] points out, "simply saying that airbags save approximately 3000 lives each year fails to capture the significant threat that airbags pose to children and small-stature adults. Once this variability is acknowledged, however, opportunities for reducing the risks to those groups may be recognized and implemented."

Many current models analyze variability and randomness (e.g. using Monte Carlo simulation), but unfortunately omit any formal consideration of epistemic uncertainty about the parameter values of the simulation. Thus, Paté-Cornell [9] notes that randomness "is generally more easily acknowledged and integrated in mathematical models," while epistemic uncertainties "are sometimes ignored and tend to be under-reported, especially in public policy studies of controversial or politically sensitive issues." For example, epidemiological models of foot-and-mouth disease may devote a great deal of computation time to simulating the progression of an outbreak as a function of random fluctuations in the number of infectious contacts an animal may have per day and so on, but treat key uncertain quantities (such as the infectivity and latent period of the disease, or even the level of public and stakeholder cooperation with mitigation measures such as movement restrictions [11]) as if they were known constants.

Of course, sensitivity analysis [12] is often used to investigate the effect of key parameter uncertainties on the results of epidemiological models. However, sensitivity analysis on the effects of individual parameters or model assumptions does not yield an integrated statement on the level of uncertainty about the model results.

### 1.2 Two-Dimensional Monte Carlo Simulation

Monte Carlo simulation [13] is a mathematical tool commonly used to help predict what might happen in disease outbreaks or situations where the population is exposed to a disease or toxic agent. Two-dimensional Monte Carlo analysis [14–18] is a variation of this method, designed to create a single, overall statement of uncertainty, including not only the types of randomness and variability that are commonly taken into account in simulations, but also systematic scientific uncertainties (such as lack of knowledge about disease infectiousness).

The basic idea of two-dimensional Monte Carlo is similar to that of sensitivity analysis (namely, varying key parameters over their credible ranges). However, instead of doing a separate set of sensitivity runs for each parameter individually, two-dimensional Monte Carlo does this in an integrated manner, sampling randomly from the probability distributions for all uncertain input parameters before initiating any given simulation

run. In this manner, the methodology makes it possible to quantify and characterize the combined effects of numerous different uncertainties at the same time.

The fact that two-dimensional Monte Carlo analysis explicitly recognizes the uncertainty about key input parameters to the simulation is important in part because randomness and variability have different implications for policy than broader scientific uncertainties. So, while it is useful to have a single overall statement of uncertainty, it is also important to distinguish variability from scientific uncertainty in order to understand their policy implications. In the next section, we discuss several real-world applications of two-dimensional Monte Carlo analysis and their policy recommendations.

## 2 APPLICATIONS OF TWO-DIMENSIONAL MONTE CARLO SIMULATIONS TO FOOD SAFETY AND ANIMAL DISEASE

### 2.1 Fumonisin Toxin in Corn

One example of the use of two-dimensional Monte Carlo analysis from the food-safety literature [17] analyzes a naturally occurring toxin (fumonisin, a type of mycotoxin) in corn and corn products, and explores the associated potential for health concerns. This analysis addressed the uncertainty about the exposure to this toxin (both the quantity of the toxin in corn-based food products, and how much corn people in the United States consume), and also the variability in human susceptibility to the toxin (accounting for variability of response between individuals, and the inadequacy of the data on dose-response relationships).

Humphreys et al. [17] treated the uncertainty about the exposure of the US population to fumonisin as the "outer loop" in the two-dimensional Monte Carlo analysis. In the problem being described here, the lack of knowledge about both, corn consumption levels and the presence of fumonisin in corn, could result in up to 3 orders of magnitude of uncertainty about individual dietary exposure to fumonisin.

Figure 1 shows the concentrations of fumonisin that have been measured in different types of corn products in the United States [17]. Corn meal, for example has relatively high levels of fumonisin contamination, while popcorn, corn chips, and corn flakes have much lower levels.

Figure 2 shows fumonisin exposure per person per day as a function of both, the level of corn consumption (measured in a country-wide dietary survey) and several possible levels of a maximum allowable concentration of fumonisin in corn. The solid black line at the top of the figure shows the toxin consumption under circumstances with no regulatory limit on fumonisin concentration in corn products. As the limit of allowable fumonisin concentration in corn is reduced (from no limit to 2.0 ppm, down to 0.5 ppm), the exposure to the toxin decreases, as expected). However, reducing the allowable concentration level of the contaminant may not substantially reduce the exposure levels of individuals with extremely high levels of corn consumption. This suggests that those individuals with high levels of corn consumption may still be heavily exposed to fumonisin, even if the corn itself is less heavily contaminated.

Given these uncertainties, Humphreys et al. [17] compared two alternative policy measures for dealing with fumonisin toxins namely, limiting the allowable concentrations of fumonisin, and issuing consumption advisories (i.e. advising people to restrict their intake of certain corn products). Figure 3 illustrates the effects of differing consumption advisories on total fumonisin intake, as a function of people's (original) levels of corn

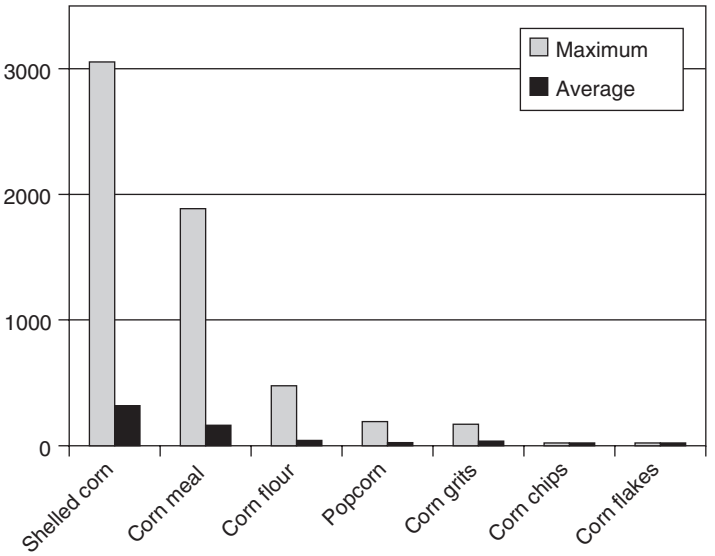



**FIGURE 1** Average Presence of Fumonisin B in U.S. Corn (based on surveillance data from the U.S. Food and Drug Administration, 1994–1995) and based on data published in Reference 17.

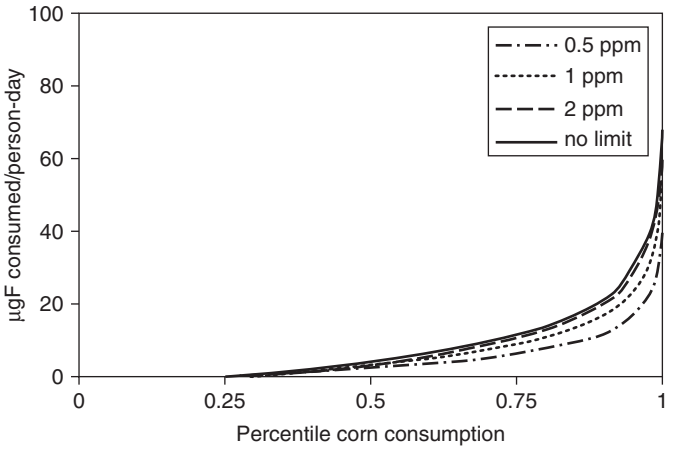



**FIGURE 2** Effects of Different Concentration Limits on Fumonisin Exposure per Person per day (in micrograms) as a Function of the Percentile of Corn Consumption, based on Data in Reference 17.

consumption. The solid black line at the top again shows the extent of fumonisin intake with no consumption advisory. As the recommended consumption limit in the advisory decreases, from no limit to 100 g of corn per day down to 25 g of corn per day, the daily toxin intake is markedly reduced. Thus, consumption advisories would seem to have a greater effect on reducing peak levels of fumonisin intake than contamination limits, because consumption advisories specifically address risks to those individuals who consume large amounts of corn.

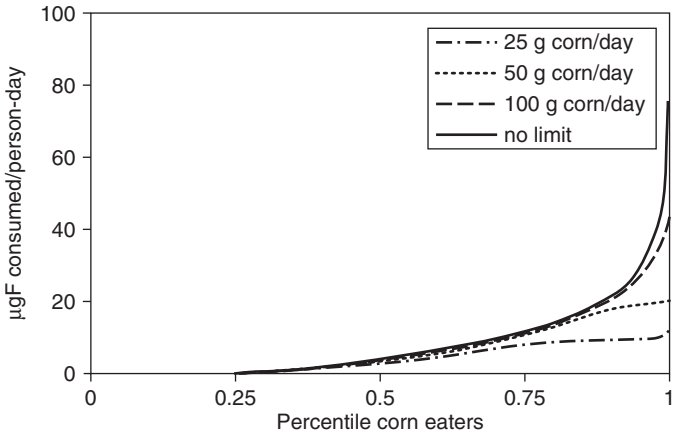



**FIGURE 3** Effects of Differing Consumption Advisories on Total Fumonisin Intake per Person per Day (in micrograms) as a Function of the Original Percentile of Corn Consumption, based on Data in Reference 17.

Humphreys et al. [17] also studied the effects of variability, or the "inner loop" of the Monte Carlo simulation. As noted above, the model input parameters designated as representing variability included different responses between individuals (for example, due to different body weights) and the inadequacy of the data available for characterizing the dose-response relationship to fumonisin.

Figure 4 illustrates the contributions of both uncertainty and variability, as defined by Humphreys et al., to human kidney toxicity in response to a variety of simulated regulatory scenarios. (The graph is dimensionless, because the units can be difficult to interpret.) In Figure 4, the black bars represent the effects of uncertainty with no variability; the gray bars represent variability with no uncertainty; and the white bars represent the effects of both uncertainty and variability. Thus, the black bars show the estimated health risk if both corn consumption and the levels of fumonisin concentration (treated as aspects of "uncertainty" in this study) were at relatively high levels. Conversely, neglecting the uncertainty (or "outer loop" of the Monte Carlo simulation) and setting only those factors treated as variability to high levels would give us the gray estimates of risk (rather than the white-colored estimates). This could result in estimates of risk that are low by about a factor of 10.

Thus, the results in Figure 4 demonstrate the value of two-dimensional Monte Carlo analysis: for example, by highlighting cases in which uncertainty is high, so that it may be worthwhile to conduct additional research before making a final decision. In this particular case, those factors categorized as "variability" appear to contribute more to the overall risk than those categorized as "uncertainty" (although, as noted earlier, there is reason to dispute the categorization of these terms). In any case, all of the risk estimates were low enough that no further regulatory action was judged to be necessary. However, in cases where the overall risk estimates were higher, it could be important to take uncertainty into account in order to avoid underestimating peak risks.

Moreover, in this case study, consumption advisories appeared to be more effective at controlling peak exposures than regulatory limits (presumably because of the wide variability in consumption levels within the population), although it is worth noting that

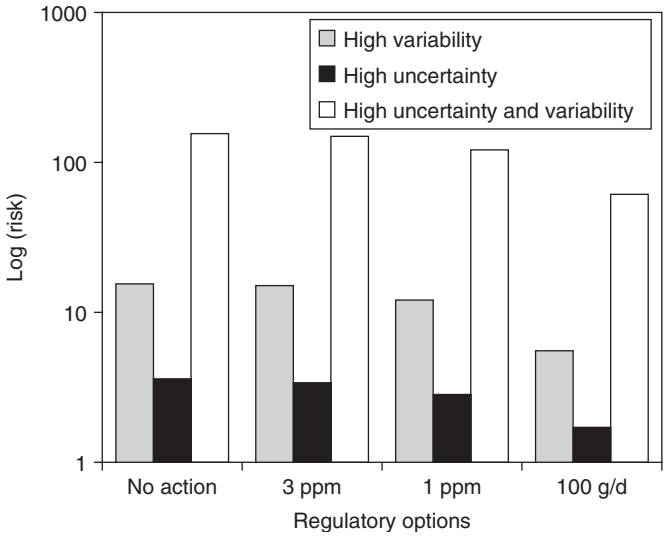



**FIGURE 4** Effects of Uncertainty and Variability on Risk as a Function of Regulatory Option (no action, 3 ppm limit on fumonisin concentrations, 1 ppm limit on fumonisin concentrations, and 100 grams/day consumption advisory), based on Data in Reference 17.

they put the burden of risk reduction on consumers rather than producers. If consumption advisories were to be adopted, it might be desirable to identify which population subgroups are most vulnerable to fumonisin, as well as collecting data on consumption levels by ethnicity and region. By contrast, if regulatory concentration limits were adopted, then additional information on toxin concentrations by production region might be more useful, along with information on how contaminated corn might flow through the supply chain.

To summarize, Humphreys et al. [17] found only low levels of risk in the United States, and therefore little reason for concern about fumonisin levels in the US corn supply. However, risks may not be as low as indicated above if the data on corn consumption were not representative of the entire country (for example, if high-consumption regions were omitted), and if the measured levels of fumonisin in corn crops did not include data obtained under drought conditions (under which fumonisin contamination is more likely). Finally, while Humphreys et al. [17] assumed that kidney lesions were the most sensitive toxicity endpoint in humans, the risks could turn out to be higher than indicated in their analysis if some other endpoint turned out to be more important clinically.

### 2.2 Patulin Toxin in Apple Juice

A similar analysis was performed by Baert et al. [15] to characterize variability and uncertainty regarding children's exposure to patulin toxin from consuming three types of apple juice in Belgium: organic; handcrafted; and conventional. Based on a survey of juice consumption in preschool children, and measured values of patulin in the three types of apple juice, they considered variability in both consumption and contamination levels, as well as uncertainty about these parameters due to lack of data. The resulting analysis showed that variability in the type of juice consumed did have a significant

effect on risk in this case, even considering the confidence intervals reflecting lack of knowledge.

In particular, patulin exposure was found to be higher in children consuming only organic apple juice, with 0.9% of children (90% confidence interval of 0.3% to 1.8%) estimated to exceed the tolerable daily intake of patulin. By contrast, 0.1% of children consuming conventional apple juice (90% confidence interval of 0–0.3%) and no children consuming handcrafted apple juice (90% confidence interval of 0–0.2%) were estimated to exceed the tolerable daily intake. The results reflect both the high variability of juice consumption between individuals, and the high variability of contamination levels in apple juice.

The use of two-dimensional Monte Carlo provided a significant methodological advance in the study of this risk. In particular, the authors noted that "a tendency exists to overestimate mean exposures when a deterministic approach is used." Thus, the probabilistic uncertainty analysis performed by Baert et al. [15] arguably provided a more realistic assessment of the range of exposures, and avoided unnecessarily conservative modeling assumptions and approaches.

The two risk mitigation strategies considered by Baert et al. [15] to reduce patulin intake were similar to the strategies evaluated in the fumonisin example above: either to reduce the allowable levels of contamination in juice, or to reduce juice consumption. Unlike in the fumonisin example, however, here the analysis concluded that regulatory limits would be more effective than consumption advisories. Presumably, this was because the variability of patulin concentrations in organic apple juice was sufficiently high that even with reduced consumption, some children could still be exposed to hazardous levels. In particular, the authors concluded that "a reduction of the consumption has more effect when the patulin contamination is lower."

### 2.3 Escherichia coli O157:H7 on Beef Trimmings

Cummins et al. [16] illustrate a slightly different approach to characterizing the role of variability and uncertainty in food contamination, focusing on the process of food preparation in the supply chain, rather than food consumption. In their work, a model was developed to estimate the prevalence of *E. coli O157:H7* on beef trimmings in Irish slaughterhouses by considering: initial contamination levels on hides; cross-contamination events; process steps at which microbial growth could occur; the results of decontamination efforts; and steps undertaken to reduce bacterial numbers. The output of the model was a distribution of the prevalence of *E. coli O157:H7* on beef trimmings, and also a distribution of the number of organisms on contaminated beef trimmings. The purpose of the model was to identify critical points in the process, and assess the impact of various process mitigations for this bacterial disease agent.

Variability and uncertainty were separated in this analysis in order to identify future data requirements and research needs for model improvements, and also to identify those input parameters that had a significant effect on risk, and should therefore be monitored. A total of 19 input parameters were categorized as representing uncertainty (e.g. test sensitivity, which was assumed to be constant but unknown), variability (e.g. number of contaminated carcasses, which was assumed to fluctuate from day to day), or both (e.g. *E. coli* counts on contaminated hides).

The results showed that uncertainty dominated the results, with variability having relatively little impact on model outputs. In fact, Cummins et al. [16] compared the results of

their two-dimensional Monte Carlo simulation (reflecting both uncertainty and variability) with empirical survey results (reflecting variability alone), and concluded that "the confidence bounds for the simulation are much wider due to parameter uncertainty." Thus, the use of two-dimensional Monte Carlo again arguably resulted in a more accurate statement of the true level of uncertainty about meat contamination in this instance, and avoided providing misleading results, indicating that the true prevalence of *E. coli* O157:H7 on beef trimmings could be almost twice as large at some slaughterhouses as would have been indicated by the results of the surveillance survey at a single slaughterhouse.

The results of the analysis indicated that uncertainty about microbial test sensitivity contributed significantly to the overall uncertainty about model results, and therefore required further experimental work to characterize it. However, the results also supported recommendations about specific risk-reduction measures that could be undertaken in the interim, such as minimizing hide contamination before slaughter and reducing cross-contamination during hide removal.

### 2.4 Application of Two-Dimensional Monte Carlo Simulation To Homeland Security

The above examples were primarily concerned with food safety. However, two-dimensional Monte Carlo can also be used to analyze problems of homeland security, such as intentionally introduced contamination. For example, consider an intentionally introduced outbreak of foot-and-mouth disease. An analysis of such outbreaks should ideally address not only the effects of variability and randomness (for example, due to differences in weather conditions and disease transmission contacts from day to day under various cattle-management strategies), but also key scientific uncertainties (such as lack of knowledge about the infectivity of the disease agent, or the effectiveness of proposed vaccines).

We have undertaken such an analysis [19], using expert opinion to quantify the uncertainty about simulation inputs such as disease infectivity, and differences in infectivity between species. This reflects the fact that such parameters are not known constants, and therefore are better represented by probability distributions rather than point estimates. As in Cummins et al. [16], we found that the results of the two-dimensional Monte Carlo simulation (taking into account the uncertainty about simulation inputs) were much broader than the results of a one-dimensional simulation (reflecting variability alone). For example, in one scenario, the 90% confidence interval for the duration of possible disease outbreaks increased from 1–2 months due to variability alone, to 0.5–4 months taking uncertainty into account, and up to 4 times wider.

In fact, for some input parameters, the ranges of values considered credible by the experts we surveyed were so broad that the inner loop of the simulation would not run for some combinations of parameter values, necessitating significant revisions to the computer code (AusSpread) that was used to model the spread of foot-and-mouth disease. Thus, the discipline imposed by the rigorous quantification of uncertainty and the use of expert opinion arguably helped to overcome any biases or overconfidence that could have resulted from relying on the opinion of a single expert or model developer, leading to a more accurate assessment of the possible extent of disease spread.

Of course, care must be taken in representing intentional malicious acts using probability distributions. Clearly, we do not have perfect information about what a potential attacker might do, so some representation of uncertainty is important. However, the

uncertainties about intentional acts will not necessarily follow the same probability distributions as uncertainties about the same parameters in an unintentional outbreak. For example, while various strains of foot-and-mouth disease may differ in their infectivity, potential attackers will not necessarily choose randomly among them, but may prefer to use strains that are believed to be more infectious. Similarly, the progression of an unintentional outbreak may vary significantly depending on whether the disease happens to emerge shortly before cattle are transferred to an auction barn (and commingled with large numbers of other animals); by contrast, intentional introduction of foot-and-mouth disease may be deliberately performed shortly before transfer to an auction barn, in order to maximize the likelihood of rapid disease transmission.

With such caveats in mind, though, uncertainty can be just as important in homeland security as in health and safety, if not more so. Critical uncertainties related to security might include factors such as how the food system (and consumers) would respond if an incident of intentional food contamination drastically reduced confidence in the security of imported food products, whether the public and stakeholders would cooperate with recommended mitigation measures [11] (such as movement controls, in the case of foot-and-mouth disease), and the secondary economic impacts of terrorism events (e.g. whether consumers resume buying products affected by contamination after the crisis is over, whether import or export markets suffer lasting losses after a contamination incident).

Moreover, variability and uncertainty still have different implications for decision-making in the homeland security context, as in the other examples discussed in this article. For instance, further research on issues such as whether foot-and-mouth disease is amenable to airborne spread could help to determine how severe an outbreak is likely to be, and hence how much effort is justifiable to reduce the risk of disease introduction. Likewise, if the severity of an outbreak of foot-and-mouth disease is found to be significantly affected by vaccine effectiveness, then further research to verify effectiveness might be desirable before committing to vaccination as a mitigation strategy. By contrast, if the severity of an outbreak is found to be influenced primarily by random fluctuations (such as differences in weather conditions at the time of disease introduction), that would argue for committing to a specific mitigation policy sooner, rather than waiting for further research results.

## 3 THE EFFECTS OF MODEL UNCERTAINTY

The applications described above consider primarily the effects of variability and uncertainty in the parameters of a single model. However, in some cases, there is also significant uncertainty about which model is most appropriate, especially if different models give quite different results. In fact, Box [20], an eminent statistician, pointed out that "All models are wrong, but some are useful."

A study by Linkov and Burmistrov [21] investigated model uncertainty in the context of radioactive contamination on fruit (such as strawberries) in the aftermath of a nuclear power plant accident. The authors found radically different predictions for the cesium concentrations in strawberries from the different models they considered. In fact, the results from the six different models initially varied by as much as 7 orders of magnitude.

Figure 5 shows the ratio of the individual model results to the median output of all six models for four different iterations of modeling effort. The iterations represent

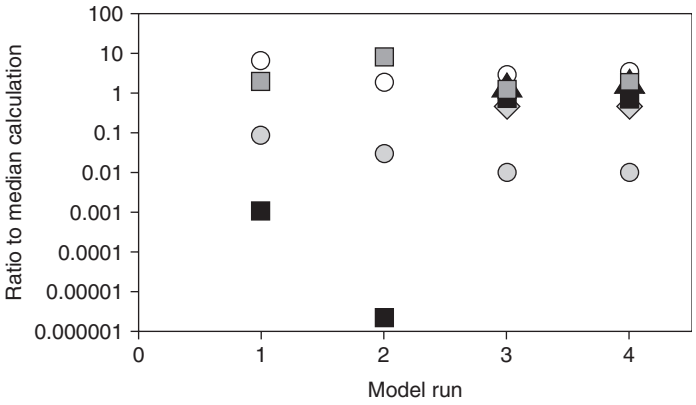



**FIGURE 5** Effects of Model Uncertainty for Strawberry Contamination (based on Data in Reference 21).

meetings in which the modelers discussed and agreed on their assumptions, and attempted to standardize modeling methods in order to achieve greater consistency. As shown in Figure 5, it was not until the third meeting that major disagreements among the results of the various models were substantially reduced. By iterations three and four, there was much closer agreement among most of the models, but one model still gave much lower predictions than the other five. Thus, even extensive interactions among the modelers did not completely eliminate model-to-model differences.

The above results suggest that model uncertainty can be a significant consideration in practice. In some cases, it may still be possible to address model uncertainty within the context of a two-dimensional Monte Carlo simulation. For example, if there is scientific uncertainty about whether foot-and-mouth disease is amenable to airborne spread, this could perhaps be treated as one of the uncertain parameters in the outside loop of a two-dimensional Monte Carlo, with some simulation runs being done under the assumption of airborne spread and others not (depending on how plausible airborne spread is considered to be). In other cases, however, model uncertainty may need to be treated merely as a caveat, or through more traditional sensitivity analysis, for example, if some models are too computation-intensive to be run numerous times, or if the researchers do not have access to all relevant models.

## 4 SUMMARY AND CONCLUSIONS

In summary, methods such as two-dimensional Monte Carlo uncertainty analysis [14, 18] can be a useful adjunct to more traditional Monte Carlo simulation in supporting decision-making. In particular, uncertainty analysis can help identify which areas are the most important focus for future research and data collection, and moreover avoids the problem of inadvertently claiming more than is actually known (which can occur if Monte Carlo simulation is used with point estimates rather than probability distributions for key input parameters).

The implementation of two-dimensional Monte Carlo can be mathematically complex, but ideally, the results should be communicated to decision-makers and stakeholders in

a form that is both informative and easy to understand [10]. This can be done by using probability distributions to show the overall uncertainty about the outcome of the analysis; for example, probability distributions for the number of infected animals in an outbreak of foot-and-mouth disease might be useful in understanding the range of possible scenarios that could occur, and hence how seriously to take the threat [19]. Graphics could also assist in risk communication by showing which sources of uncertainty contribute the most to the overall uncertainty about the outcome. This kind of information can shed light on the value of additional information, thereby helping to improve decisions about which uncertainties are the most important to study and resolve.

Eventually, the results of a risk assessment could be used as input to a formal decision analysis [example Refs. 3, 5, 13], in which stakeholder values are quantified as a basis for identifying the most desirable risk management options. However, in practice (as in several of the examples discussed in this article), it is often straightforward to identify the best (i.e. most effective and cost-effective) risk-reduction options once the risks have been thoroughly characterized. In that case, a formal decision analysis may never be necessary.

## REFERENCES


1. Kaplan, S., and Garrick, B. J. (1982). On the quantitative definition of risk. *Risk Anal.* **1**(1), 11–27.
2. Zimmerman, R., and Bier, V. M.(2002). Risk assessment of extreme events. *Columbia-Wharton/Penn Roundtable on Risk Management Strategies in an Uncertain World*. Palisades, New York, April 12–13. Available at http://www.ldeo.columbia.edu/chrr/documents/meetings/roundtable/white_papers/zimmerman_wp.pdf.
3. National Research Council. (1996). *Understanding Risk: Informing Decisions in a Democratic Society*. National Academy Press, Washington, DC.
4. American Industrial Health Council, U.S. Environmental Protection Agency, U.S. Department of Health and Human Services, and Society for Risk Analysis. (1989). *Presentation of Risk Assessments of Carcinogens: Report of an Ad Hoc Study Group on Risk Assessment Presentation*. American Industrial Health Council, Washington, DC.
5. National Research Council. (2008). *Science and Decisions: Advancing Risk Assessment*. National Academy Press, Washington, DC.
6. Phillips, C. V. (2003). Quantifying and reporting uncertainty from systematic errors. *Epidemiology* **14**(4), 459–466.
7. Yokota, F., and Thompson, K. M. (2004). Value of information analysis in environmental health risk management decisions: past, present, and future. *Risk Anal.* **24**(3), 635–647.
8. Kaplan, S. (1983). On a 'two-stage' Bayesian procedure for determining failure rates from experiential data. *IEEE Trans. Power Apparatus Syst.* **PAS-102**(1), 195–202.
9. Paté-Cornell, M. E. (1996). Uncertainties in risk analysis: six levels of treatment. *Reliab. Eng. Syst. Saf.* **54**(2), 95–111.
10. Thompson, K. M. (2002). Variability and uncertainty meet risk management and risk communication. *Risk Anal.* **22**(3), 647–654.
11. Anthony, R. (2004). Risk communication, value judgments, and the public-policy maker relationship in a climate of public sensitivity toward animals: revisiting Britain's foot and mouth crisis. *J. Agric. Environ. Ethics* **17**(4–5), 363–383.
12. Frey, H. C., and Patil, S. R. (2002). Identification and review of sensitivity analysis methods. *Risk Anal.* **22**(3), 553–578.

13. Morgan, M. G., and Henrion, M. (1990). *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*. Cambridge University Press, Cambridge.
14. Vicari, A. S., Mokhtari, A., Morales, R. A., Jaykus, L. A., Frey, H. C., Slenning, B. D., and Cowen, P. (2007). Second-order modeling of variability and uncertainty in microbial hazard characterization. *J. Food Prot.* **70**(2), 363–372.
15. Baert, K., De Meulenaer, B., Verdonck, F., Huybrechts, I., De Henauw, S., Vanrolleghem, P. A., Debevere, J., and Devlieghere, F. (2007). Variability and uncertainty assessment of patulin exposure for preschool children in Flanders. *Food Chem. Toxicol.* **45**(9), 1745–1751.
16. Cummins, A., Nally, E. P., Butler, F., Duffy, G., and O'Brien, S. (2008). Development and validation of a probabilistic second-order exposure assessment model for *Escherichia coli O157:H7* contamination of beef trimmings from Irish meat plants. *Meat Sci.* **79**(1), 139–154.
17. Humphreys, S. H., Carrington, C., and Bolger, M. (2001). A quantitative risk assessment for fumonisins B1 and B2 in US corn. *Food Addit. Contam.* **18**(3), 211–220.
18. Vose, D. (2008). *Risk Analysis: A Quantitative Guide*, 3rd ed. John Wiley & Sons, Chichester.
19. Zach, L., and Bier, V. M. *Manuscript in preparation. An alternative to sensitivity analysis for understanding uncertainty: analyzing uncertainty and variability in the risk of foot-and-mouth disease*.
20. Box, G. E. (1979). Robustness in the strategy of scientific model building. In *Robustness in Statistics*, R. L. Launer, and G. N. Wilkinson, Eds. Academic Press, New York, pp. 201–236.
21. Linkov, I., and Burmistrov, D. (2003). Model uncertainty and choices made by modelers: lessons learned from the international atomic energy agency model intercomparisons. *Risk Anal.* **23**(6), 1297–1308.

# MICROBIOLOGICAL DETECTORS FOR FOOD SAFETY APPLICATIONS

EVANGELYN C. ALOCILJA AND SUDESHNA PAL
*Biosystems and Agricultural Engineering, Michigan State University, East Lansing, Michigan*

## 1 BIOSECURITY AND FOOD SAFETY THREATS

The complexity of the US food supply chain from cradle to grave provides numerous entry points and routes in which (inadvertent and intentional) contaminants and pathogens can be introduced into the nation's food system. For example, a simple hamburger, consisting of a bun, a beef patty, tomato, lettuce, cheese, and onion, is made of at

least 50 ingredients which could include hundreds of sources when we consider the raw materials, processing, transportation, and finished product. Furthermore, these ingredients may come from across the globe, crossing the US border in less than 24 h. The recent scandal on melamine-tainted pet foods (and maybe human food through melamine-tainted animal feed) is one example of how the food supply can potentially be sabotaged.

The use of microorganisms as biological weapons has long been reported in history. One of the first major attacks that have been reported occurred in the 14th century with *Yersenia pestis* during the siege of Kaffa [1]. The most recent was the deliberate release of *Bacillus anthracis* spores through the postal system in the United States in October 2001, shortly after the terrorist attack, resulting in 22 cases of anthrax and five deaths [2]. Inhalational anthrax has a high mortality rate of about 100% and the spore forms of the bacteria are very stable under harsh environmental conditions. The Centers for Disease Control and Prevention (CDC, http://www.bt.cdc.gov/agent/agentlist.asp) and the National Institute of Allergy and Infectious Diseases (NIAID, http://www3.niaid.nih.gov/topics /BiodefenseRelated/Biodefense/ research/CatA.htm) have classified *B. anthracis* as a Biodefense Category A agent because it can be easily transmitted from person to person, can cause high mortality with potential for major public health impact, may cause public panic and social disruption, and requires special action for public health preparedness. It is estimated that the release of 50 kg of dried anthrax spores for 2 h can lead to a complete breakdown in medical resources and civilian infrastructure in a city of 500,000 inhabitants [3].

*B. anthracis* is a gram-positive, nonmotile, facultatively anaerobic, spore-forming, rod-shaped bacterium and is the etiological agent of anthrax. Anthrax is primarily a zoonotic disease but all mammals, particularly humans, are prone to this disease. The spore forms of *B. anthracis* are highly resistant to adverse environmental conditions, such as heat, ultraviolet and ionizing radiation, pressure, and chemical agents. They are able to survive for long periods of time in contaminated soils and this account for the ecological cycle of the microorganism. The vegetative cells of the bacterium are square-ended and capsulated having a size range of 3 to 5 μm while the spores are elliptical with a size range of 1 to 2 μm [4].

The primary virulence factors of *B. anthracis* are toxin production and capsule formation. Virulent strains of the microorganism carry two large plasmids pXO1 and pXO2 which encode these virulence factors. The plasmid pXO1 carries the structural genes for the anthrax toxin proteins *pagA* (protective antigen), *lef* (lethal factor), and *ef* (edema factor); two *trans*-acting regulatory genes *atxA* and *pagR*; a gene encoding type I topoisomerase, *topA*; and a three gene operon, *gerX*, which affects germination. Plasmid pXO2 carries three genes which encode capsule synthesis: *capA, capB*, and *capC*; a gene associated with capsule degradation, *dep*; and a *trans*-acting regulatory gene *acpA* [5]. None of the three toxin proteins are toxic separately. Toxicity is associated with the formation of binary exotoxins. The association of *pagA* and *lef* results in the formation of lethal toxin (LTx), which provokes lethal shock in animals, while the association of *pagA* and *ef* forms the edema toxin (ETx), which produces edema in the skin [6].

*B. anthracis* spores can enter the human host through the skin (cutaneous route), ingestion (gastrointestinal route), and inhalation (pulmonary route). Ingesting food products contaminated with the spores can lead to gastrointestinal anthrax. In this manner, anthrax spores may cause lesions from the oral cavity to the cecum [7]. Cases of gastrointestinal anthrax have been reported through ingesting undercooked meat from animals [8]. The disease is characterized by fever, nausea, vomiting, abdominal pain, and bloody

diarrhea [8]. Gastrointestinal anthrax has been reported to cause fatalities in 25-60% of cases (CDC, 2001). In some community-based studies, cases of gastrointestinal anthrax outnumbered those of cutaneous anthrax [7]. Awareness of gastrointestinal anthrax in a differential diagnosis remains important in anthrax-endemic areas but now also in settings of possible bioterrorism.

The inhalational form of anthrax is considered the most dangerous among the three routes, having a mortality rate close to 100% (CDC, 2001). The inhaled spores reach the alveolus where they are phagocytosed by macrophages and transported to the mediastinal lymph nodes, where spore germination can occur in up to 60 days. Following germination, the disease progresses rapidly resulting in the production of exotoxins that cause edema, necrosis, and hemorrhage [4]. Diagnosis is difficult in both gastrointestinal and inhalational forms, resulting in the disease rapidly becoming treatment-resistant and fatal.

In addition to intentional contaminations, we have recently faced unintentional food poisoning through pathogen-tainted products which caused recalls on these products. In September 2007, a major meat processing company recalled up to 9,843 mt (21.7 million lb) of ground beef due *E. coli* O157:H7 contamination; it was one of the largest meat recalls in US history. This contamination sickened 30 people in eight states. On October 5, 2007, that company announced that it was closing its business.[1] Contamination of meat products by foodborne pathogens is increasingly a major food safety and economic concern. Billions of dollars are lost every year in medical costs, productivity, product recalls, and jobs as a result of pathogen-contamination outbreaks. In the United States, there are up to 33 million cases of human illness each year from microbial pathogens in the food supply with an associated cost of $2–4 billion in 2006.[2]

NIAID has identified the following microbes as foodborne and waterborne pathogens: diarrheagenic *Escherichia* coli, *Salmonella* species, pathogenic *Vibrio*s, *Shigella* species, *Listeria monocytogenes*, *Campylobacter jejuni*, *Yersinia enterocolitica*, caliciviruses, Hepatitis A, *Cryptosporidium parvum*, *Cyclospora cayatanensis*, *Giardia lamblia*, *Entamoeba histolytica*, *Toxoplasma*, and *Microsporidia*. These organisms are classified as Category B because they are moderately easy to disseminate, result in moderate morbidity rates, and require specific enhancements of CDC's diagnostic capacity and enhanced disease surveillance (http://www.bt.cdc.gov/agent/agentlist.asp). In general, the causes of foodborne illness include viruses, bacteria, parasites, fungi, toxins, and metals with the symptoms ranging from mild gastroenteritis to life-threatening neurological, hepatic, and renal problems. It is estimated that foodborne diseases cause approximately 76 million illnesses, including 325,000 hospitalizations and 5000 deaths in the United States each year [9]. Of these, known pathogens account for an estimated 14 million illnesses, 60,000 hospitalizations, and 1800 deaths indicating that these pathogens are a substantial source of infectious diseases [9]. Researchers at the Economic Research Service (ERS) of the US Department of Agriculture (USDA) estimate that the total annual medical cost associated with foodborne illness caused by pathogens is $6.5–9.4 billion.

Recent foodborne disease outbreaks involved *E. coli* O157:H7 in spinach in 2007, and cookie dough in June 2009, and *Salmonella* in peanut butter in January 2009. *E. coli* are bacteria that naturally occur in the intestinal tracts of humans and warm-blooded animals

[1]http://www.msnbc.msn.com/id/21149977/

[2]http://www.ers.usda.gov/Data/FoodborneIllness/

to help the body synthesize vitamins. A particularly dangerous type is the enterohemorrhagic E. coli O157:H7 or EHEC. In 2000, EHEC was the etiological agent in 69 confirmed outbreaks (twice the number in 1999) involving 1564 people in 26 states [10]. Of the known transmission routes, 69% were attributed to food sources, 11% to animal contact, 11% to water exposures, and 8% to person-to-person transmission [10]. *E. coli* O157:H7 produces toxins that damage the lining of the intestine, cause anemia, stomach cramps, and bloody diarrhea, and a serious complication called hemolytic uremic syndrome (HUS) and thrombotic thrombocytopenic purpura (TTP) [11]. In North America, HUS is the most common cause of acute kidney failure in children, who are particularly susceptible to this complication. TTP has a mortality rate of as high as 50% among the elderly [12]. Recent food safety data indicates that cases of *E. coli* O157:H7 are rising in both the United States and other industrialized nations [13].

Human infections with *E. coli* O157:H7 have been traced back to individuals having direct contact with food in situations involving food handling or food preparation. The most recent *E. coli* O257:H7 outbreak covering 29 states involved eating raw refrigerated prepackaged cookie dough [14]. In addition to human contamination, *E. coli* O157:H7 may be introduced into food through meat grinders, knives, cutting blocks, and storage containers. *E. coli* O157:H7 has also been found in drinking water that has been contaminated by runoff from livestock farms as a result of heavy rains. Regardless of source, *E. coli* O157:H7 has been traced to a number of food products including meat and meat products, apple juice or cider, milk, alfalfa sprouts, unpasteurized fruit juices, dry-cured salami, lettuce, game meat, and cheese curds [11, 15]. Possible points of entry into the food supply chain include naturally occurring sources from wild animals and ecosystems, infected livestock, contaminated processing operations, and unsanitary food preparation practices.

*Salmonella enterica* serovar Typhimurium and *Salmonella enterica* serovar Enteritidis are the most common *Salmonella* serotypes found in the United States. According to CDC, salmonellosis is the most common foodborne illness [16]. Over 40,000 actual cases are reported yearly in the U.S. [17]. Approximately 500 [9] to 1,000 [18] persons die annually from *Salmonella* infections in the United States. The estimated annual cost of human illness caused by *Salmonella* is $3 billion [9]. *Salmonella* Enteritidis has frequently been observed as a contaminant in foods such as fresh produce, eggs, and poultry products. While various *Salmonella* species have been isolated from the outside of egg shells, presence of *Salmonella* Enteritidis inside the egg is of great concern as it suggests vertical transmission, that is, deposition of the organism in the yolk by an infected hen (prior to shell deposition) [19]. The recent outbreak of Salmonella involving peanut butter in January 2009 hit almost every state in the United States.

Human *Salmonella* infection can lead to enteric (typhoid) fever, enterocolitis, and systemic infections by non-typhoid microorganisms. Typhoid and paratyphoid strains are well-adapted for invasion and survival within host tissues, causing enteric fever which is a serious human disease. Non-typhoid *Salmonella* causes salmonellosis, which is manifested as gastroenteritis with diarrhea, fever, and abdominal cramps. Severe infection could lead to septicemia, urinary tract infection, and even death in at-risk populations (young, elderly, and immunocompromised individuals). Raw meats, poultry, eggs, milk and dairy products, fish, shrimp, frog legs, yeast, coconut, sauces and salad dressing, cake mixes, cream-filled desserts and toppings, dried gelatin, peanut butter, cocoa, and chocolate are some of the foods associated with *Salmonella* infection.

## 2 DETECTION

The detection and identification of these foodborne pathogens in raw food materials, ready-to-eat food products, restaurants, processing and assembly lines, hospitals, ports of entry, and drinking water supplies continue to rely on conventional culturing techniques. Conventional methods involve pre-enrichment, selective isolation, and biochemical screening, as well as serological confirmation for certain pathogens. Hence, a complex series of tests is often required before any identification can be confirmed. These methods are laborious and may require a certain level of expertise to perform. Though these methods are highly sensitive and specific, they are elaborate, laborious, and typically require 2–7 days to obtain conclusive results [15]. Their results are not available on the time-scale desired in the food quality assurance or clinical laboratory, which has safety, cost, and quality implications for the food, medical, and biodefense sectors. Rapid detection methods for pathogens have hence become a necessity.

Currently, the three most popular methods for detecting pathogens are: microbial culturing followed by biochemical identification, enzyme-linked immunosorbent assay (ELISA), and polymerase chain reaction (PCR) assay. Conventional microbial culturing techniques are very sensitive; however, they include multiple steps in the assay and require pre-enrichment steps and time consuming processes. For example, conventional detection and specific identification of *B. anthracis* require complex techniques and laborious methods because of the genetic similarities among various *Bacillus* species as well as their existence in both spore forms and vegetative state. *B. anthracis* is identified using standard biochemical techniques, such as its sensitivity to penicillin, nonmotility, non $\beta$-hemolytic behavior on sheep or horse blood agar plates, and its susceptibility to lysis by gamma phage. It has been reported that identification of *B. anthracis* by initial blood culturing requires 6–24 h for growth, which is followed by morphological and biochemical identification that requires an additional 12–24 h, and finally, definitive identification that requires an additional 1–2 days [20]. *B. anthracis* is also shown to selectively grow on polymyxin-lysozyme EDTA-thallous acetate (PLET) agar which requires 1–2 days for growth followed by further confirmation [21].

ELISA is a diagnostic tool to detect the presence of antibody-antigen reaction in a sample. An unknown amount of antigen is affixed to a surface, and then a specific antibody is washed over the surface so that it can bind to the antigen. This antibody is linked to an enzyme, and in the final step a substance is added that the enzyme can convert to some detectable signal. ELISA is becoming very popular for food safety monitoring.

PCR is gaining popularity in non-culture-based detection schemes. It is highly sensitive and able to detect the presence of just one cell. However, PCR technology has some disadvantages such as the requirement of expensive equipment, skilled personnel to perform assays, DNA extraction stages which increase the detection time, and prior information of target DNA sequences.

Biosensors can play a role in the rapid test market. Biosensor technology is emerging as a promising field for rapid detection of microbial pathogens. A biosensor is an analytical device that integrates a biological sensing element with an electrical transducer to quantify a biological event (e.g. an antigen-antibody reaction) into an electrical output. The basic concept of operation of a biosensor is illustrated in Figure 1. The biological sensing element may include enzymes, antibodies, DNA probes, aptamers, molecularly imprinted polymers, and whole cells. Depending on the transducing mechanism, biosensors can be electrochemical, electrical, optical, mechanical, and magnetic. They can be operated in a

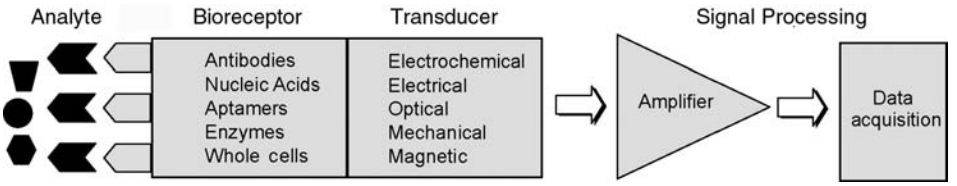



**FIGURE 1** Schematic representation of a biosensor.

reagent-less process enabling the creation of user-friendly and field-ready devices. Some of the major attributes of biosensor technology are its specificity, sensitivity, reliability, portability, real-time analysis, and simplicity of operation. Biosensors are needed to quickly detect disease-causing agents in food, in order to ensure continued safety of the nation's food supply.

Biosensors show high sensitivity and specificity to targets and can be used as simple one-step measurement tools or as multimeasurement devices. Moreover, biosensors can be designed to be operated on-site or at point of care, eliminating the need of expensive lab-based testing. The miniaturization ability of biosensors and their compatibility with data processing technologies, allow them to be integrated into small portable devices. This versatility in biosensors has prompted worldwide research and commercial exploitation of the technology. Recent trends (Fig. 2) indicate that biosensors are the fastest-growing technology for rapid detection of pathogens [22].

## 3 BIOSENSORS FOR MICROBIAL PATHOGEN DETECTION

In this section, we describe different types of biosensors for pathogen detection based on their transduction mechanism such as mechanical, optical, electrochemical, and magnetic approaches.

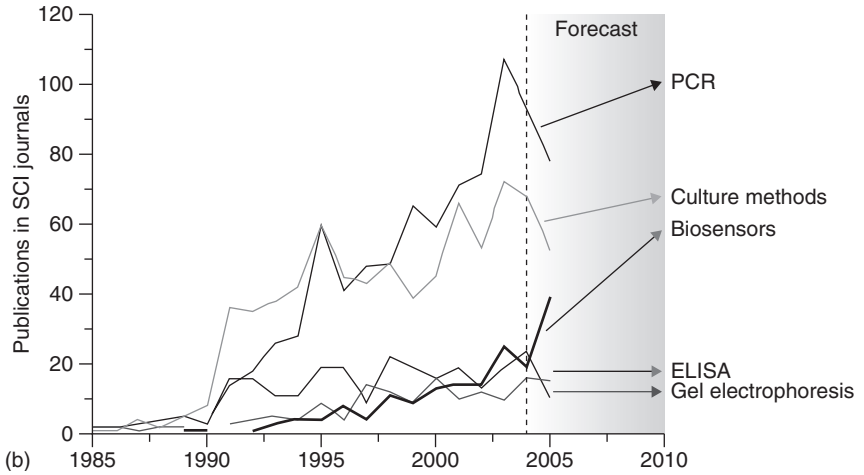



**FIGURE 2** Recent trends in pathogen detection [adapted from Lazcka et al. [22]].

### 3.1 Mechanical Biosensors

***3.1.1 Quartz Crystal Microbalance (QCM) Biosensors.*** Quartz crystal resonators form the basis of Quartz Crystal Microbalance (QCM) sensors. The term "QCM" is used collectively for bulk acoustic wave (BAW), quartz crystal resonance sensors (QCRS), and thickness shear mode (TSM) acoustic sensors [23]. QCM sensors are comprised of a thin quartz disc with electrodes plated on it. When an oscillating electric field is applied across the disc, an acoustic wave with a certain resonant frequency is induced. The disc can be coated with a sensing layer of biomolecules based on the analyte to be detected. The interaction of the analyte with the biomolecules on the disc surface causes a change in mass and a concurrent change in resonant frequency that can be directly correlated to the biomolecular interactions [24]. The relation between mass and the resonant frequency is given by the Sauerbrey equation:

$$\Delta F = \frac{-2.3 \times 10^6 F_0^2 \Delta m}{A} \tag{1}$$

where, $\Delta F$ is the change in frequency (Hz), $F_0$ is the resonant frequency of the crystal (MHz), $\Delta m$ is the deposited mass (grams) and $A$ is the coated area ($cm^2$). The quartz crystals are inexpensive, easily available, and robust, thus making them suitable for chemical sensors and biosensors. In addition, QCM-based sensors provide great flexibility, wide dynamic range of frequency measurements, and label-free detection [24].

A wide range of nonlabeled QCM biosensors have been reported in the literature for the detection of pathogenic bacteria and viruses. QCM sensors based on lectin recognition systems for bacterial identification have been studied by Shen et al. [25], Safina et al. [26]. Shen et al. have used a combination of mannose self-assembled monolayer (SAM) and lectin concanavalin A for the detection of *E. coli* W1485 in a linear range of $7.5 \times 10^2$ to $7.5 \times 10^7$ cells/ml. Safina et al. utilized lectin reporters to develop a flow injection QCM biosensor for detection of *Campylobacter jejuni* and *Helicobacter pylori*. The authors were able to detect $10^3$ to $10^5$ cells/ml in 30 min. A SAM based QCM immunosensor was developed for the detection of *E. coli* O157:H7 by Su and Li [27]. The immunosensor was able to detect the target bacteria in the range of $10^3$ to $10^5$ CFU/ml in 30–50 min. Detection of *B. subtilis* spores as a surrogate to *B. anthracis* was achieved by Lee et al. utilizing a QCM immunosensor to a detection limit of 450 spores/ml [28]. Furthermore, virus (dengue virus and hepatitis B virus) detection with QCM immuno- and nucleic acid- based sensors has been reported by Wu et al. [29] and Yao et al. [30].

QCM biosensors for the detection of DNA sequences have also been developed using nanoparticle labels as amplifiers. Mao et al. [31] reported the use of streptavidin conjugated $Fe_3O_4$ nanoparticles (NPs) for the detection of *E. coli* O157:H7 *eaeA* gene. The NPs acted as 'mass enhancers' and amplified the change in frequency. The biosensor could attain a sensitivity of $10^{-12}$ *M* synthetic oligonucleotides and $2.67 \times 10^2$ CFU/ml *E. coli* O157:H7 cells [31]. Similarly, Au NPs were employed by Wang et al. for real-time bacterial DNA detection in a circulating flow QCM biosensor. The authors reported a sensitivity of $2.0 \times 10^3$ CFU/ml for *E. coli* O157:H7 *eaeA* gene [32].

A QCM-based biosensor was used to detect *Salmonella* sp. in milk samples with detection limits around $10^6$ CFU/ml [33]. Tombelli et al. [34] developed a DNA piezoelectric biosensor for the detection of bacterial toxicity based on the detection of PCR amplified *aer* gene of *Aeromonas hydrophila*. The biosensor was applied to vegetables,

environmental water, and human specimens. The biosensor was able to successfully distinguish between samples containing the pathogen and those not contaminated. Zhao et al. [35] developed a QCM biosensor using 50 nm gold NPs as the amplification probe for DNA detection in the order of 10 fM of target, which was higher than what has been reported using the same method. The high sensitivity was explained by the weight of the larger particles, and the larger area occupied by the larger particles that needed less target DNA for their binding. Another QCM biosensor applied to the detection of *E. coli* in water in combination with PCR amplification (of the *lac* gene) was able to detect a 10 fg of genomic *E. coli* DNA (few viable *E. coli* cells in 100 ml of water) [36]. When used for detection of *Hepatitis B virus*, [37] observed that the QCM could detect frequency shifts of DNA hybridization as a linear relationship, in the range 0.02–0.14 μg/ml with a detection limit of 0.1 μg/ml, similar to the QCM biosensor developed by He and Liu [38] for *Pseudomonas aeruginosa*.

***3.1.2 Surface Acoustic Wave Biosensors.*** Surface Acoustic Wave (SAW) sensors are the second class of acoustic wave sensors that have found applications in biosensor devices. SAW sensors consist of two metal interdigital transducers (IDT) etched from a thin metal film deposited on a piezoelectric substrate. The sensing mechanism is based on the changes in SAW velocity or attenuation when mass is sorbed on the sensor surface. Since the acoustic energy is strongly confined to the surface, SAW devices are very sensitive to surface changes such as mass loading, viscosity, and conductivity changes [39]. It has been suggested that SAW based biosensors have good sensitivities because of their higher mass sensitivities [39].

SAW biosensors have been successfully applied for the detection of bacteria and viruses. *E. coli* detection using SAW biosensors have been reported in the literature by multiple authors [40–43]. The biosensors have used antibodies as the biological sensing element with sensitivities ranging from $10^6$ cells/ml to 0.4 cells/μl. Branch and Brozik have developed a 36° YX-cut $LiTaO_3$ based love-wave device for the detection of the *B. anthracis*, as simulated by *B. thuringiensis* spores in aqueous conditions [44]. The authors have investigated two waveguide materials polyimide and polystyrene for creating the love-wave sensors. Detection of *B. thuringiensis* spores at concentrations below the lethal dose of anthrax spores was possible using both waveguide materials. The sensor had a detection limit of a few hundred cells per ml and a response time of $<100$ s. Jin et al. [45] developed a SAW biosensor for detecting the gene of Staphylococcal Enterotoxin B utilizing ST-cut quartz and $SiO_2$ guiding layer. The biosensor had a sensitivity of 10 ng/ml and a linear range of 35–200 ng/ml [45]. Recently, SAW biosensors were used for detecting viral bioagents by Bisoffi et al. [46]. A lithium-tantalate based SAW transducer with $SiO_2$ waveguide sensor platform was used for Coxsackie virus B4 and Sin Nomber virus detection.

SAW resonators are suitable for use in simple electronic setups because of their low insertion losses and sharp resonance frequencies. As a result, insertion of such devices into oscillator circuits is beneficial as such circuits are commonly used in point-of-care diagnostics. Furthermore, the SAW-based biosensors can be prepared from cheap components thus making them suitable for integration into inexpensive sensor arrays [47].

***3.1.3 Microcantilever-Based Biosensors.*** Microcantilever-based biosensors are derived from microfabricated cantilevers used in atomic force microscopy (AFM). Detection is based on the bending induced in the cantilever when a biomolecular interaction takes

place on one of its surfaces which is translated into nanomechanical motion and is commonly coupled to an optical or piezoelectric readout system [48]. The cantilevers can be operated in the static deflection mode where analyte binding causes cantilever bending or in the dynamic resonant mode where analyte binding causes change in resonant frequency [49]. Microcantilever sensors are promising for biosensor applications since they can perform local, high resolution, and label-free molecular recognition measurements [48].

Davila et al. have demonstrated microcantilever-based biosensors in the detection of *B. anthracis* Sterne spores in air and water [50]. The detection scheme involved measurement of the decrease in resonant frequency driven by thermally induced oscillations as a result of the mass of spores measured by a laser Doppler vibrometer. The authors reported a minimum detection of 2 spores (740 fg) and 50 spores (139 pg) in air and water, respectively, using 20 μm long, 9 μm wide, and 200 nm thick cantilevers. Campbell and coworkers have utilized piezoelectric-excited millimeter-sized cantilever sensors for the detection of *B. anthracis* Sterne spores and *E. coli* O157:H7 cells [51]. The sensors consisted of a piezoelectric and glass layer and were able to detect *B. anthracis* spores at 300 spores/ml and *E. coli* O157:H7 cells in ground beef at 50 to 100 cells/ml. Extremely sensitive microcantilever-based biosensors capable of detecting a single pathogen have also been reported in literature [51]. Illic et al. was able to detect a single *E. coli* O157:H7 cell using low stress silicon nitride cantilever beams in air [52]. The mass of a single *E. coli* O157:H7 cell was found by the authors to be 665 fg. Similarly, Johnson et al. reported the use of microscale silicon cantilever resonators for vaccinia virus detection in air [53]. The authors measured the mass of a single vaccinia virus particle to be $12.4 \pm 1.3$ fg and $7.9 \pm 4.6$ fg using two different-sized cantilever beams [51]. The ability to detect small amounts of bacterial organisms was demonstrated using micro-electromechanical systems (MEMS) for the qualitative detection of specific *Salmonella enterica* strains with a functionalized silicon nitride microcantilever. Detection was achieved due to a change in the surface stress on the cantilever surface *in situ*, upon binding of a small number of bacteria with less than 25 adsorbed bacteria required for detection [54].

## 3.2 Optical Biosensors

***3.2.1 Surface Plasmon Resonance Biosensors.*** Surface Plasmon Resonance (SPR) is an optical technique for monitoring biomolecular interactions that occur in the close vicinity of a transducer surface. SPR-based biosensing can be subdivided into three categories depending on the mode of SPR detection: angular, spectral, and local SPR biosensing. Angular SPR biosensing is the most common form and involves attenuated total reflection approach using Kretschmann geometry [55]. Spectral SPR biosensing is conducted at a fixed incident angle and utilizes the wavelength dependence of the dielectric constant of the metal film to interrogate the surface plasmon coupling conditions. Local SPR (LSPR) biosensing or nanoparticle-based SPR involves coupling of surface-immobilized metallic NPs or nanostructures into a plasmon mode which results in a decrease in the transmitted power at a specific resonant wavelength dependent on environmental dielectric conditions [55].

SPR biosensors provide several advantages over conventional transduction techniques, such as capability of label-free detection, ability to produce continuous real-time responses, regeneration of the active sensor surface, feasibility for miniaturization, multiplexing ability, and sensitive detection of small molecules [56].

SPR-based immunosensors have been developed for the detection of *E. coli* O157:H7 by Irudayaraj and coworkers [57, 58]. The authors have demonstrated a sensitivity of $10^3$ CFU/ml for the pathogen using a SAM-based SPR biosensor and the commercially available Spreeta SPR biosensor [57, 58]. Detection of *Salmonella* Typhimurium in chicken carcasses was achieved using an antibody-based SPR biosensor by Lan et al. [59]. The SPR biosensor had a lowest detection limit of $10^6$ CFU/ml, and highly sensitive detection of *Salmonella* Enteritidis was attained by Waswa et al. using the commercial Biacore™ SPR biosensor [60]. The limit of detection (LOD) of the biosensor as reported by the authors was 23 CFU/ml for *Salmonella*. Chen et al. have demonstrated an immunomagnetic separation based SPR detection method for the foodborne pathogen *Staphylococcus aureus* [61]. The detection system involved an initial immunomagnetic bead-based separation step of 30 min and had a sensitivity of $10^6$ CFU/ml in a total assay time of 2 h. A SAM-based SPR immunosensor was developed by Jyoung et al. for the detection of *V. cholerae* O1 with a detection range of $10^5$ to $10^9$ cells/ml [62]. Detection of viruses using SPR-based biosensors have been reported by Chung et al. [63], Vaisocherova et al. [64]. Vaisocherova and coworkers developed an SPR biosensor for detecting antibodies against the Epstein-Barr virus. The antibody detection was performed using an immunoreaction between the antibody and a synthetic peptide for the virus. The sensor had a sensitivity of 0.2 ng/ml ($\sim$1 pM). Furthermore, multiplex detection of four foodborne bacterial pathogens (*E. coli* O157:H7, *Salmonella* Typhimurium, *Listeria monocytogenes*, and *Campylobacter jejuni*) was demonstrated by Taylor et al. using an eight-channel SPR biosensor [65]. The LOD for each of the four species of bacteria was in the range of $3.4 \times 10^3$ and $1.2 \times 10^5$ CFU/ml. Additional review articles focus on different SPR based detection techniques and their applications [56, 66, 67]. *Listeria* and *Salmonella enterica* were detected at $10^6$ CFU/ml by an SPR biosensor [68]. Additional SPR biosensors for different bacterial targets, such as *P. aeruginosa*, *B. cereus*, and *E. coli* O157:H7, were later developed by various researchers [27, 69–71], and showed similar detection limits.

***3.2.2 Fluorescence-Based Biosensors.*** Fluorescence is the radiative de-excitation of a molecule following the absorption of a photon. Generally, the emitted photon is of lower energy than the absorbed photon, and the fluorescence emission peak of a species is at longer wavelengths than the absorption peak, the wavelength separation being referred to as Stoke's shift. Fluorescence based detection systems have gained popularity in biosensors due to their high sensitivity and are mostly based on the detection of the fluorescent signal generated by fluorophores that are used to label the biomolecules [72].

Fluorescence detection techniques can be performed in high throughput mode in combination with platforms such as microarrays. Microarrays offer the advantage of using a two-dimensional layout of recognition elements for simultaneous detection and quantification. Taitt et al. have demonstrated a fluorescence-based microarray immunosensor for the simultaneous detection of nine targets comprising *B. anthracis* Sterne, *B. globigii*, *Francisella tularensis*, *Y. pestis*, *Salmonella* Typhimurim, Staphylococcal enterotoxin B, ricin, cholera toxin, and MS2 coliphage [73]. More recently, Li et al. have developed a DNA microarray based on fluorescent nanobarcodes, for the simultaneous detection of DNA of four targets (*B. anthracis*, *Francisella tularensis*, Ebola virus, and SARS coronavirus) [74]. The detection procedure involved confocal microscopy, dot blotting and flow cytometry, and resulted in sensitivity in the attomolar range.

Fluorescence resonance energy transfer (FRET-based) detection involves nonradiative energy transfer between a donor fluorophore and an acceptor fluorophore when they are in close proximity [75]. A fiber-optic portable biosensor utilizing the principle of FRET was developed by Ko and Grant for rapid detection of *Salmonella* ser. Typhimurium in ground pork samples [76]. The biosensor had a sensitivity of $10^5$ CFU/ml in a response time of 5 min. Kim et al. reported a molecular beacon (MB) DNA microarray system for fast detection of *E. coli* O157:H7 based on FRET [77]. In this system, unlike conventional fluorophore-quencher beacon design, two fluorescence molecules allowed active visualization of both hybridized and unhybridized states of the beacon. The target gene detection limit for the system was 1 ng/μl.

Fluorescence-based tapered fiber-optic biosensors have also been employed in pathogen detection. A fluorescence-based fiber-optic biosensor for detecting *E. coli* O157:H7 in ground beef samples was developed by Geng et al. [78]. The authors reported sensitivity of $10^3$ CFU/ml in pure cultures and of 1 CFU/ml in artificially contaminated ground beef samples after 4 h enrichment using a sandwich immunoassay. A fiber-optic biosensor was also developed by Geng et al. for detecting *L. monocytogenes* in hot-dog and bologna naturally contaminated or artificially inoculated with 10 to $10^3$ CFU/g, after enrichment in buffered *Listeria* enrichment broth [79]. A cyanine5-labeled antibody was used to generate a specific fluorescent signal. The sensitivity threshold was about $4.3 \times 10^3$ CFU/ml. Nanduri et al. developed an automated fiber-optic based immunosensor called RAPTOR$^{TM}$ for the detection of *Listeria monocytogenes* in food samples. The LOD of the system was $5 \times 10^5$ CFU/ml in food samples and $1 \times 10^3$ CFU/ml in phosphate buffered saline (PBS) solution [80]. In another study, a microcapillary flow injection liposome immunoanalysis system (mFILIA) was developed for the detection of heat-killed *E. coli* O157:H7. Liposomes tagged with anti-*E. coli* O157:H7 and an encapsulating fluorescent dye were used to generate fluorescence signals measured by a fluorometer. The mFILIA system successfully detected as few as 360 cells/ml with a total assay time of 45 min [81].

An automated optical biosensor system based on fluorescence excitation and detection in the evanescent field of a quartz fiber was used to detect 16-mer oligonucleotides in DNA hybridization assays. The detection limit for the hybridization with a complementary fluorescein-labeled oligonucleotide was $2 \times 10^{-13}$ *M* [82]. Another optical fiber evanescent wave DNA biosensor used an MB-DNA probe that became fluorescent upon hybridization with target DNA [83]. The detection limit of the evanescent wave biosensor with synthesized complementary DNA was 1.1 nM. Liu et al. later developed MB-DNA biosensors with micrometer to submicrometer sizes for DNA/RNA analysis. The MB-DNA biosensor was highly selective with single base-pair mismatch identification capability, and could detect 0.3 n*M* and 10 n*M* of rat gamma-actin mRNA with a 105-μm biosensor and a submicrometer (0.1 μm) biosensor, respectively [84].

Optical biosensors targeting RNA as the analyte offer an added advantage over traditional DNA-based detection methods, that is, viable cell detection. Baeumner et al. [85] detected as few as 40 *E. coli* cells/ml in samples using a simple optical dipstick-type biosensor coupled to Nucleic Acid Sequence Based Amplification (NASBA), emphasizing the fact that only viable cells were detected, and no false positive signals were obtained from dead cells present in a sample. The detection of viable cells is important with respect to safety, and also food and environmental sample sterilization assessments. Similarly, a biosensor for the protozoan parasite *Cryptosporidium parvum* was developed [86]. Hartley and Baeumner [87] developed a simple membrane-strip based biosensor for

the detection of viable *B. anthracis* spores. The study combined the optical detection process with a spore germination procedure, as well as a nucleic acid amplification reaction to identify as little as one viable *B. anthracis* spore in 12 h.

### 3.3 Electrochemical Biosensors

Electrochemical biosensors are based on the detection of electrochemical signals generated by consumption or production of electrons from biological interactions occurring at the sensor surface. Advantages such as low cost, high sensitivity, miniaturization ability, low power requirements, and simple instrumentation make electrochemical biosensors well-suited for clinical and environmental analysis. Electrochemical biosensors are generally classified as amperometric, potentiometric, conductometric, and impedimetric.

***3.3.1 Amperometric Biosensors.*** Amperometric biosensors are based on the measurement of current changes resulting from oxidation or reduction of an electroactive species in a biochemical reaction. The current is typically measured at a fixed potential (amperometry) or during controlled variations of the potential (voltammetry).

Theegala et al. reported an oxygen-electrode based amperometric biosensor for the qualitative detection of *E. coli* O157:H7 in water [88]. The biosensor detected changes in oxygen concentration due to decrease in enzymatic activity upon binding of bacterial cells. The biosensor could detect as low as 50 cells/ml in 20 min. A renewable amperometric immunosensor for the detection of *S. typhi* was reported by Singh et al. [89]. The detection technique involved a sandwich ELISA system with an LOD of $10^5$ cells/ml in 90 min. Amperometric detection of antibodies against *B. anthracis* protective antigen was also achieved by Aguilar et al. [90]. The antibodies were captured and detected using microcavities with an LOD of 10 fg in a 200 nl sample. A disposable amperometric immunosensor based on a screen-printed electrode (SPE) coated with agarose or nano-Au membrane and horseradish peroxidase-labeled antibody for specific detection of the foodborne pathogen *Vibrio parahaemolyticus* was developed by Zhao et al. [91]. The immunosensor showed a sensitivity of $7 \times 10^4$ CFU/ml for the pathogen with good consistency (97.5%) as compared to the ELISA results.

Lermo et al. described a genomagnetic assay for the electrochemical detection of *Salmonella* spp. based on *in situ* DNA amplification and magnetic primers [92]. Detection was achieved by double hybridization of the target on magnetic beads which were then separated by a magneto-electrode based on graphite-epoxy composite followed by electrochemical detection using an enzyme marker anti-digoxigenin horseradish peroxidase. The authors achieved a sensitivity of 2.8 fmol with PCR amplicons. Multi-analyte detection using electrochemical genosensors have also been studied by Elsholz et al. [93], Farabullini et al. [94]. Farabullini et al. achieved nanomolar detection limits for the toxin-producing bacteria such as *Salmonella* sp., *E. coli* O157:H7, *L. monocytogenes*, and *S. aureus*, using differential pulse voltammetry to detect $\alpha$-napthol signal in less than 1 h.

Additional biosensors (targeting DNA) that have been developed include MEMS-based amperometric [95] and high throughput PCR biosensors [96], microcantilever-based cyclic voltammetry biosensor [97], pulsed amperometry- [98], and capacitance-based biosensors [99, 100].

***3.3.2 Potentiometric Biosensors.*** Potentiometric devices are based on the measurement of accumulation of charge potential at the working electrode of an electrochemical cell

in comparison to the reference electrode with zero or negligible current flow between the electrodes. The measured potential is related to the concentration of the analyte through the Nernst equation:

$$E = E_0 \pm (\mathrm{R}T/n\mathrm{F}) \ln Q$$

where, $E$ is the cell potential at zero current, $E_0$ is the standard potential, R is the universal gas constant, $T$ is the absolute temperature, F is the Faraday's constant, $n$ is the total number of charges of ion, $Q$ is the ratio of ion concentration at the anode to that at the cathode [101, 102].

Among electrochemical transducing methods, potentiometric methods are the least exploited in pathogen detection due to their high detection limits and poor selectivity, the main advantage of these devices being wide detectable concentration range and continuous measurement capability [103]. Another approach involves ion selective filed effect transistors (ISFETs) that employ semiconductor field-effect to detect biorecognition events. However, the application of these devices in biosensors has been limited by production problems related to immobilization, fabrication and packaging, poor detection limits, and device stability [22]. An advancement that has evolved from the ISFET is the light addressable potentiometric sensor (LAPS) which combines potentiometry with optical detection [22, 104]. Ercole et al. reported an antibody-based LAPS biosensor for the determination of *E. coli* in food [105]. The biosensor detected variations in pH due to ammonia production by urease-*E. coli* antibody conjugates in commercial lettuce, sliced carrot, and rucola samples. The sensor was able to reach a sensitivity of 10 cells per ml in an assay time of 1.5 h.

***3.3.3 Conductometric Biosensors.*** Conductometric biosensors utilize the electrical conductivity of a sample to determine the components and their concentration [106]. Muhammad-Tahir and Alocilja [107–110] have developed a conductometric biosensor for the detection of pathogenic bacteria and viruses. The biosensor was fabricated using conducting polyaniline as an electronic label in a sandwich immunoassay scheme, and the authors demonstrated that polyaniline improved the sensitivity of the biosensor by forming a conductive molecular bridge between silver electrodes. The authors reported a sensitivity of $10^{1.8.3} \times 10^1$ CFU/ml for *Salmonella*, $7.9 \times 10^1$ CFU/ml for *E. coli* O157:H7, $7.5 \times 10^1$ CFU/ml for *E. coli*, and $10^3$ CCID/ml for BVDV virus in a detection time of 10 min. A conductometric immunosensor based on magnetic NPs has been recently developed by Hnaiein et al.,for the detection of *E. coli* [111]. The immunosensor was composed of streptavidin-modified magnetic nanoparticle layer immobilized on a conductometric transducer consisting of interdigitated gold electrodes. Conductivity measurements allowed detection of 0.5 CFU/ml of *E. coli* without the need for amplification.

***3.3.4 Impedimetric Biosensors.*** Impedance spectroscopy involves applying small amplitude, perturbing sinusoidal voltage signals to an electrochemical cell and measuring the resulting current response. The complex impedance, sum of real and imaginary impedance components, can be calculated as a function of the excitation frequency of the applied potential by varying it over a range of frequencies [112]. Impedimetric detection techniques provide the advantages of high sensitivity, linearized current-potential

characteristics, measurement over wide time or frequency ranges, and label-free sensing [22, 106]

Radke and Alocilja had developed a microimpedance biosensor for the detection of *E. coli* O157:H7 [113]. The sensor detected changes in impedance caused by the presence of bacteria immobilized on interdigitated gold electrode arrays fabricated from silicon. The biosensor was able to discriminate between different cellular concentrations of the bacteria ($10^5$ to $10^7$ CFU/ml) in 5 min. Nandakumar et al. have demonstrated the detection of *Salmonella* Typhimurium using electrochemical impedance spectroscopy based on Bayesian decision theory [114]. The technique detected the pathogen in 6 min at a lowest concentration of 500 CFU/ml. An impedance biosensor based on an interdigitated array microelectrode coupled with magnetic nanoparticle-antibody conjugates was developed for rapid and specific detection of *E. coli* O157:H7 in ground beef samples, by Varshney and Li [115]. Magnitude of impedance and phase angle was measured in a frequency range of 10 Hz to 1 MHz in the presence of 0.1 *M* mannitol solution. The lowest detection limit of the biosensor for *E. coli* O157:H7 was $7.4 \times 10^4$ CFU/ml in pure cultures and $8.0 \times 10^5$ CFU/ml in ground beef samples, the total detection time being 35 min.

An impedance biosensor chip for detection of *E. coli* O157:H7 was developed based on the surface immobilization of affinity-purified antibodies onto indium tin oxide (ITO) electrode chips, with a detection limit of $6 \times 10^3$ cells/ml [116]. Shah et al. [117] developed an amperometric immunosensor with a graphite-coated nylon membrane serving as a support for antibody immobilization and as a working electrode. This approach was used for detection of *E. coli*, with a low detection limit of 40 CFU/ml.

### 3.4 Magnetic Biosensors

Devices based on the detection of magnetic labels are emerging as a promising new approach in the field of biosensing [118]. Magnetic labels have gained popularity in biosensing because they are physically and chemically stable, are relatively inexpensive, and can easily be made biocompatible. Several approaches have been developed in the past few years for both direct and indirect detection of magnetic labels. Direct detection includes approaches for measuring magnetic parameters, such as magnetic permeability, magnetic remanence, magnetoresistance, and Hall Effect. The indirect detection methods are based on microcantilever-based force amplified sensors and magnetic relaxation switches [119]. However, the applications of these magnetic devices for detection of actual targets such as pathogenic microorganisms remain limited and require further research.

Edelstein et al. had developed a multi-analyte BARC (Bead Array Counter) biosensor using giant magnetoresistive (GMR) sensors to detect and identify biological warfare agents [120]. The prototype designed by the authors consisted of a microfabricated chip with GMR sensor arrays, an electronic chip-carrier board, a fluidics cell and an electromagnet. DNA probes were patterned onto the GMR sensor chips and hybridized with complementary PCR products. Micron-sized magnetic beads were then bound to the DNA sample by streptavidin biotin interactions and the unbound beads were removed by applying a magnetic field. The bound magnetic beads were then detected by the GMR sensors. The authors were able to demonstrate the detection of *B. anthracis* lethal factor and *C. botulinum* neurotoxin A using the BARC biosensor.

A mass-sensitive magnetoelastic immunosensor for the detection of *E. coli* O157:H7 was reported by Ruan et al. [121]. The detection was based on the immobilization of

alkaline phosphatase-labeled antibodies on the surface of a micrometer-scale magnetoelastic cantilever and amplification of the mass change associated with antigen-antibody binding reaction by biocatalytic precipitation of 5-bromo-4-chloro-3-indolyl phosphate. The minimum detectable level of the immunosensor was $6 \times 10^2$ cells/ml.

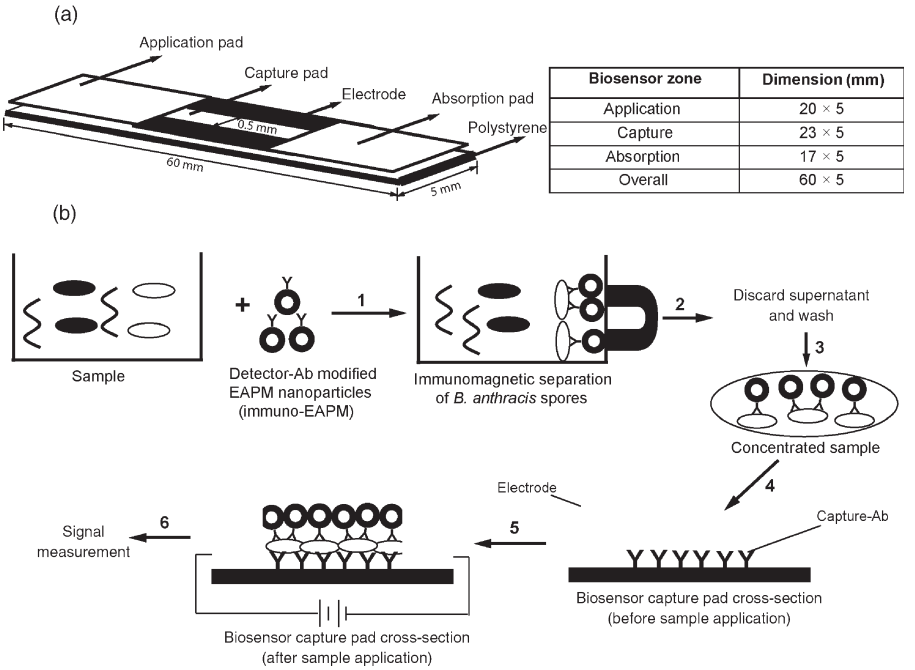
A high efficiency Hall-Effect microbiosensor platform has recently been developed for the detection of magnetically labeled biomolecules by Sandhu et al. [122]. In this system, the integration of Hall-Effect structures with microcurrent lines allowed manipulation of the magnetic beads position via field gradients. The authors studied the hybridization of fully complementary DNA strands of 20–25 bases using Dynabeads as magnetic labels with this platform. Although, the sensitivity of the sensor was not reported, the authors were able to demonstrate a quantitative relationship between the number of magnetic labels and the output signal.

## 4 INTEGRATED EXTRACTION/DETECTION MAGNETIC NANOPARTICLE-BASED BIOSENSOR SYSTEM

In this section, we illustrate an integrated extraction-detection system. Specifically we present how electrically active polyaniline-coated magnetic (EAPM) NPs are used in a direct charge transfer biosensor for the concentration and detection of *B. anthracis* spores from complex food matrices such as romaine lettuce, lean ground beef, and ultra-pasteurized whole milk. For lettuce and beef, 25 g samples were weighed, mixed with 225 ml of 0.1% (w/v) peptone water in a Whirl-Pak plastic bag, and stomached in a stomacher (Microbiology International, MD) for one minute. The milk samples were used as purchased. Nine ml of the liquid samples were thoroughly mixed with 1 ml of appropriate concentrations of *B. anthracis* spores stock solution in a vortex mixer (Fisher Scientific, IA). Finally, a series of 10 ml samples inoculated with *B. anthracis* spores at concentrations ranging from $10^1$ to $10^7$ spores/ml were obtained. For details of this illustration, please refer to Pal and Alocilja [123].

The biosensor design is shown in Figure 3a [123]. A three-component biosensor system is made up of a sample application pad, capture pad, and absorption pad. Silver electrodes are fabricated along both sides of the capture pad leaving an electrode gap of 0.5 mm. For data acquisition, the biosensor unit is connected to a handheld multimeter linked to a computer.

There are three important materials in the detection scheme: detector antibodies conjugated to EAPM-NPs ($Ab_d$-EAPM), capture antibodies immobilized on the nitrocellulose membrane ($Ab_c$), and target *B. anthracis* spores. Figure 3b is a schematic representation of the immunomagnetic separation and biosensor detection procedure. The biosensor detection involves a sandwich immunoassay to form the biological structure $Ab_c$-spore-$Ab_d$-EAPM. To start, EAPM-NPs are conjugated with mouse monoclonal anti-*B. anthracis* IgG molecules through direct physical adsorption (Step 1), forming $Ab_d$-EAPM. Then $Ab_d$-EAPM are used to immunomagnetically concentrate the spores from the complex food matrices (Step 2). The concentrated targets (spore-$Ab_d$-EAPM) are then washed to remove unbound materials (Step 3) and applied to the sample application pad of the biosensor (Step 4). The spore-$Ab_d$-EAPM complex flows to the capture pad by capillary action, where the antigen is anchored by the capture antibodies ($Ab_c$) and the sandwich structure $Ab_c$-spore-$Ab_d$-EAPM is formed (Step 5). The conductive EAPM-NPs bound to the spores in the sandwich act as a voltage-controlled "ON" switch




| Biosensor zone | Dimension (mm) |
|---|---|
| Application | 20 × 5 |
| Capture | 23 × 5 |
| Absorption | 17 × 5 |
| Overall | 60 × 5 |

**FIGURE 3** (a) Biosensor architecture and dimensions; (b) Schematic representation of the biosensor detection system [123].

resulting in a decreased resistance across the silver electrodes that is recorded electrically (step 6) [123].

Figure 4a shows the magnetization versus magnetic field i.e. the *M-H* loop measurements of both unmodified $Fe_2O_3$ and synthesized EAPM NPs, using a DC SQUID magnetometer at 300 K. Both systems start to saturate at 5 kOe. The saturation magnetization ($M_S$) for the $Fe_2O_3$ NPs is 64.4 emu/g, whereas the saturation magnetization of the EAPM-NPs is 44.1 emu/g. The decrease in $M_S$ value for the EAPM-NPs is expected due to surface interactions between the polymer (polyaniline) which is diamagnetic in nature, and iron oxide NPs [124]. The remanent magnetization $M_r$ for the $Fe_2O_3$ and the EAPM-NPs are 14.2 and 10.4 emu/g, respectively, and the coercive force $H_c$ for both NPs is 200 Oe. The low values of $M_r$ and $H_c$ suggest that the NPs are still in the ferromagnetic phase but approaching superparamagnetic behavior [125]. Figure 4b (inset) shows electrical conductivity measurements of both synthesized EAPM and unmodified $Fe_2O_3$ NPs compressed into pellets of 2000 microns thickness at room temperature. The $Fe_2O_3$ NPs have an electrical conductivity as low as $3.4/10^5$ S/cm whereas the conductivity of the EAPM-NPs is 5 orders of magnitude higher: 3.3 S/cm. This increase in electrical conductivity is expected and confirms the presence of electrically active polyaniline in the NPs.

Figure 5a and 5b reveal Transmission Electron Microscope (TEM) images of the unmodified $Fe_2O_3$ NPs and the polyaniline-coated EAPM-NPs. The iron oxide NPs have an average diameter of 20 nm according to manufacturer's specifications, which is consistent with the TEM image in Figure 5a, whereas the polyaniline-coated EAPM-NPs show a diameter ranging from 50 to 100 nm (Figure 5b).

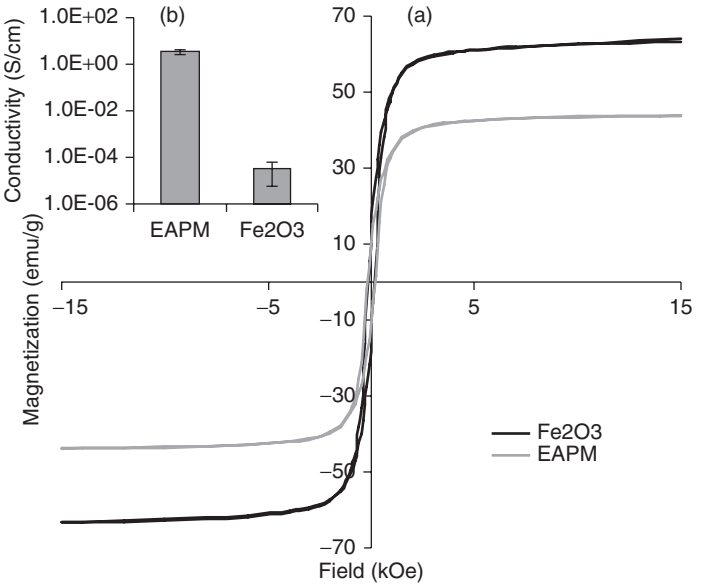



**FIGURE 4** (a) Experimental *M-H* curves of the synthesized EAPM and unmodified $Fe_2O_3$ nanoparticles at 300 K; and (b, inset) Electrical conductivity measurements for the EAPM and $Fe_2O_3$ nanoparticles at room temperature [printed with permission from Pal and Alocilja [123]].

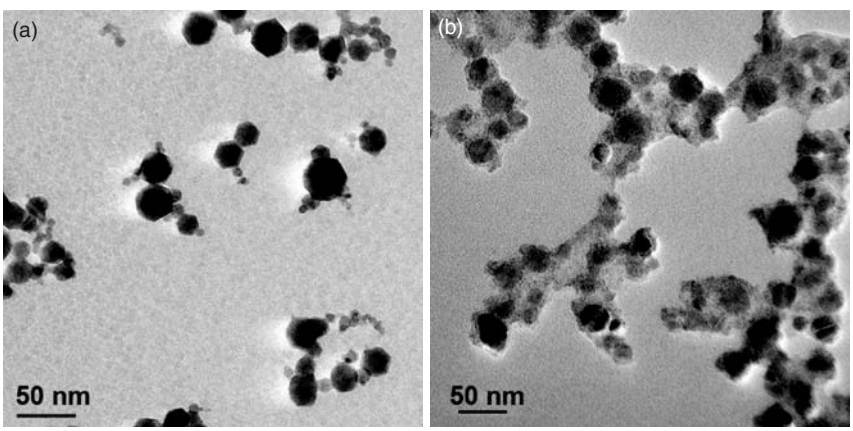



**FIGURE 5** TEM images of (a) unmodified $Fe_2O_3$ nanoparticles; and (b) Synthesized EAPM nanoparticles [printed with permission from Pal and Alocilja [123]].

The immunomagnetic capture of *B. anthracis* spores using EAPM-NPs from the three different food matrices was confirmed by microbial plating in TSA II blood agar plates and the capture efficacy of the NPs was evaluated. The capture ratio (CR) of the EAPM-NPs was evaluated using the formula $CR = C_{captured}/C_{actual}$, where, $C_{actual}$ is the actual concentration of viable spores in the sample, and $C_{captured}$ is the concentration of viable spores extracted from the food samples. The capture effects of the EAPM-NPs on *B. anthracis* spores from the lettuce and ground beef samples are quite similar. In

both samples, the capture effect is highest at a viable spore concentration of $1.52 \times 10^2$ CFU/ml with a CR value of 0.97 for lettuce and that of 0.72 for ground beef. Also, the EAPM-NPs could achieve an immunomagnetic capture at viable spore concentration as low as $1.52 \times 10^1$ CFU/ml from both lettuce and ground beef samples. However, for whole milk samples, the immunomagnetic capture of the viable *B. anthracis* spores could only go as low as $1.52 \times 10^2$ CFU/ml and the capture effects are observed to be similar for all viable spore concentrations with CR values in the range of 0.06 and 0.11. This could be explained by the high fat content of the whole milk samples which might have interfered in the immunomagnetic capture process.

Figure 6a, b, and c show the average resistance readings measured with the EAPM nanoparticle-based direct charge transfer biosensor in lettuce, whole milk, and ground beef samples inoculated with *B. anthracis* spores. The average resistance signals obtained from three replicates were plotted for the control and the food samples, contaminated with spore concentrations ranging from $4.2 \times 10^1$ to $4.2 \times 10^7$ spores/ml. As observed, the resistance values recorded for the different spore concentrations are much lower than the values for the control solution that has no spores in it. The average resistances for the control solutions for all three food samples are in the range of $288 \pm 50$ and $353 \pm 51$ kΩ, whereas the average resistances for the different spore concentrations in the three food samples vary from $75.1 \pm 14$ to $132.6 \pm 19$ kΩ. The reduced resistance values support the formation of a sandwich complex on the capture pad, where the conductive EAPM-NPs act as a charge transfer agent causing a drop in the resistance signal across the silver electrodes [126–129]. Single factor analysis of variance (ANOVA) to a significance of 95% ($P < 0.05$) was used to compare the differences in the resistance values between

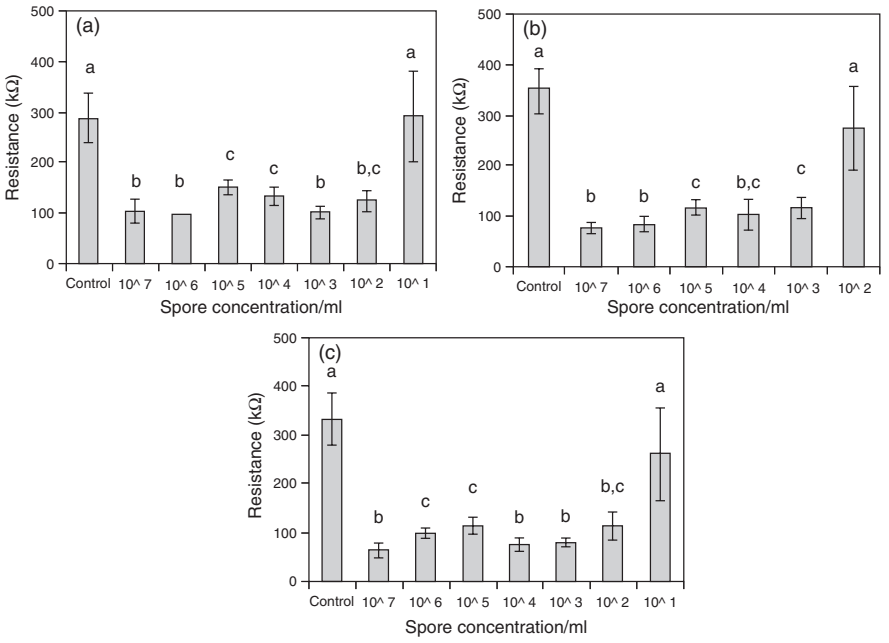



**FIGURE 6** The EAPM nanoparticle-based direct charge transfer biosensor resistance responses in (a) Romaine lettuce, (b) Whole milk, and (c) Ground beef samples contaminated with *B. anthracis* spores. Average resistances with the same letters are not significantly different ($P > 0.05$).

the control and the different spore concentrations. The lowest spore concentration that produced a resistance signal significantly different ($P < 0.05$) from the control was considered to be the sensitivity or detection limit of the biosensor. For the lettuce and ground beef samples, the biosensor sensitivity was $4.2 \times 10^2$ spores/ml with statistically significant differences from the control ($P$-value for lettuce at $10^2$ spores/ml was 1.79 E-05; $P$-value for ground beef at $10^2$ spores/ml was 2.63E-06). For whole milk samples, the biosensor could reach a sensitivity of $4.2 \times 10^3$ spores/ml where statistically significant differences could be observed from the control ($P$-value at $10^3$ spores/ml was 8.47E-08). The reduced biosensor sensitivity in the whole milk samples could be attributed to the high fat content in these samples. As observed in Figure 6, although the biosensor resistance readings recorded for the different spore concentrations were different from the control, statistical analysis did not reveal any significant differences between the concentrations. Artifacts in biosensor fabrication, probabilistic antigen-antibody interactions, antibody orientations, and stability of the sandwich complex on the capture pad might be some of the factors behind such biosensor performance. At this stage the biosensor is only considered to be a qualitative device for a yes/no diagnosis of *B. anthracis* spores. However, the biosensor shows excellent sensitivity and fast detection time in comparison to the very few rapid detection systems for *B. anthracis* in the food matrices that have been reported in the literature [130, 131].

Specificity evaluation of the biosensor is also presented here. A comparison of the biosensor resistance responses was made in pure cultures of *E. coli* with cell concentrations ranging from $1.7 \times 10^1$ to $1.7 \times 10^5$ CFU/ml, in pure cultures of *Salmonella* Enteritidis with cell concentrations ranging from $1.6 \times 10^1$ to $1.6 \times 10^5$ CFU/ml, and pure spore suspensions of *B. anthracis* with spore concentrations ranging from $4.2 \times 10^1$ to $4.2 \times 10^5$ spores/ml. The biosensor average resistance values for different concentrations of the nontarget bacteria (i.e. *E. coli* and *Salmonella* Enteritidis) are similar to the values observed for the control. Single factor ANOVA tests to a significance of 95% ($P < 0.05$) showed no statistically significant differences between the control and different cell concentrations of *E. coli* and *Salmonella* Enteritidis with $P$-values ranging from 0.278 to 0.887 for *E. coli*, and from 0.348 to 0.981 for *Salmonella* Enteritidis. The results indicate that the effects of nonspecific interactions are not significant for the range of cell concentrations tested on the biosensor. In comparison, for pure *B. anthracis* spore suspensions, the biosensor average resistance responses show significant differences between the control and spore concentrations ranging from $10^2$ to $10^5$ spore/ml ($P$-value range: 0.009−0.0009) which is expected since the antibodies used in the biosensor are specific for *B. anthracis*.

## 5 CONCLUDING COMMENTS

In this chapter, we attempted to present biosensors using various transduction mechanisms that have been developed for rapid detection of microbial pathogens of concern to food defense and food safety. These biosensors are designed for rapid, highly sensitive, specific, and user-friendly operation. While they are not exhaustive, the chapter provides a wide range and scope of the detection mechanisms that are novel and potentially market-ready. The illustrated biosensor on the EAPM-based system is an excellent demonstration on the potential speed, sensitivity, and specificity that can be achieved by biosensors in general.

## REFERENCES


1. Inglesby, T. V., Dennis, D. T., Henderson, D. A., Bartlett, J. G., Ascher, M. S., Eitzen, E., et al. (2000). Plague as a biological weapon-medical and public health management. *JAMA* **283**(17), 2281–2290.
2. Jernigan, J. A., Stephens, D. S., Ashford, D. A., Omenaca, C., Topiel, M. S., Galbraith, M., et al. (2001). Bioterrorism-related inhalational anthrax: the first 10 cases reported in the United States. *Emerging Infect. Dis.* **7**(6), 933–944.
3. Spencer, R. C. (2003). Bacillus anthracis. *J. Clin. Pathol.* **56**(3), 182–187.
4. Mock, M., and Fouet, A. (2001). Anthrax. *Annu. Rev. Microbiol.* **55**, 647–671.
5. Okinaka, R. T., Cloud, K., Hampton, O., Hoffmaster, A. R., Hill, K. K., Keim, P., et al. (1999). Sequence and organization of pXO1, the large *Bacillus anthracis* plasmid harboring the anthrax toxin genes. *J. Bacteriol.* **181**(20), 6509–6515.
6. Collier, R. J., and Young, J. A. T. (2003). Anthrax toxin. *Annu. Rev. Cell Dev. Biol.* **19**, 45–70.
7. Sirisanthana, T., and Brown, A. E. (2002). Anthrax of the gastrointestinal tract. *Emerging Infect. Dis.* **8**(7), 649–651.
8. Mock, M., and Mignot, T. (2003). Anthrax toxins and the host: a story of intimacy. *Cell. Microbiol.* **5**(1), 15–23.
9. Mead, P. S., Slutsker, L., Dietz, V., McGaig, L., Bresee, J., Shapiro, C., Griffin, P., and Tauxe, R. (1999). Food-related illnesses and death in the United States. *Emerging Infect. Dis.* **5**, 607–625.
10. CDC. (2001a). *Outbreaks Caused by Shiga Toxin-producing Escherichia Coli-Summary of 2000 Surveillance Data*. Centers for Disease Control and Prevention. Available at http://www.cdc.gov/foodborneoutbreaks/ecoli/2000_summaryLetter.pdf.
11. Doyle, M. P., Zhao, T., Meng, J., and Zhao, S. (1997). Escherichia coli O157:H7. *Food Microbiology Fundamentals and Frontiers*. American Society for Microbiology, Washington, DC.
12. FDA. (2006). *Foodborne Pathogenic Microorganisms and Natural Toxins Handbook: The "Bad Bug Book". FDA-CFSAN*. Available at http://www.cfsan.fda.gov/~mow/intro.html
13. WHO. (2002). *Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems*. World Health Organization Food Safety Dept, Geneva, Switzerland.
14. CDC. (2009). *Multistate Outbreak of E. coli O157:H7 Infections Linked to Eating Raw Refrigerated, Prepackaged Cookie Dough. Updated June 25, 2009*. Available at http://www.cdc.gov/ecoli/2009/0619.html
15. FDA. (2005). *Bacteriological Analytical Manual*. Food and Drug Administration, Rockville, MD. Available at http://www.cfsan.fda.gov/~ebam/bam-toc.html
16. CDC. (2002b). *Preliminary FoodNet Data on the Incidence of Foodborne Illnesses-Selected Sites, United States, 2001. MMWR 51: 325-9*.
17. CDC. (2002a). *Notice to Readers: Final 2001 Reports of Notifiable Diseases. MMWR 51: 710*.
18. CDC. (2001b). *Salmonellosis*. Available at http://www.cdc.gov/ncidod/dbmd/diseaseinfo/salmonellosis_g.htm
19. FDA. (1992). *Foodborne Pathogenic Microorganisms and Natural Toxins Handbook: Salmonella spp*. Available at http://www.cfsan.fda.gov/~mow/chap1.html
20. Inglesby, T. V. (2000). Anthrax as a biological weapon: medical and public health management (vol 281, pg 1735, 1999). *JAMA* **283**(15), 1963.

21. Erickson, M. C., and Kornacki, J. L. (2003). Bacillus anthracis: current knowledge in relation to contamination of food. *J. Food Prot.* **66**(4), 691–699.
22. Lazcka, O., Del Campo, F. J., and Munoz, F. X. (2007). Pathogen detection: a perspective of traditional methods and biosensors. *Biosens. Bioelectron.* **22**(7), 1205–1217.
23. Cooper, M. A., and Singleton, V. T. (2007). A survey of the 2001 to 2005 quartz crystal microbalance biosensor literature: applications of acoustic physics to the analysis of biomolecular interactions. *J. Mol. Recognit.* **20**(3), 154–184.
24. O'Sullivan, C. K., and Guilbault, G. G. (1999). Commercial quartz crystal microbalances-theory and applications. *Biosens. Bioelectron.* **14**(8–9), 663–670.
25. Shen, Z. H., Huang, M. C., Xiao, C. D., Zhang, Y., Zeng, X. Q., and Wang, P. G. (2007). Nonlabeled quartz crystal microbalance biosensor for bacterial detection using carbohydrate and lectin recognitions. *Anal. Chem.* **79**(6), 2312–2319.
26. Safina, G., van Lier, M., and Danielsson, B. (2008). Flow-injection assay of the pathogenic bacteria using lectin-based quartz crystal microbalance biosensor. *Talanta* **77**(2), 468–472.
27. Su, X. L., and Li, Y. B. (2004). A self-assembled monolayer-based piezoelectric immunosensor for rapid detection of Escherichia coli O157: H7. *Biosens. Bioelectron.* **19**(6), 563–574.
28. Lee, S. H., Stubbs, D. D., Cairney, J., and Hunt, W. D. (2005). Rapid detection of bacterial spores using a quartz crystal microbalance (QCM) immunoassay. *IEEE Sens. J.* **5**(4), 737–743.
29. Wu, T. Z., Su, C. C., Chen, L. K., Yang, H. H., Tai, D. F., and Peng, K. C. (2005). Piezoelectric immunochip for the detection of dengue fever in viremia phase. *Biosens. Bioelectron.* **21**(5), 689–695.
30. Yao, C. Y., Zhu, T. Y., Tang, J., Wu, R., Chen, Q. H., Chen, M., et al. (2008). Hybridization assay of hepatitis B virus by QCM peptide nucleic acid biosensor. *Biosens. Bioelectron.* **23**(6), 879–885.
31. Mao, X. L., Yang, L. J., Su, X. L., and Li, Y. B. (2006). A nanoparticle amplification based quartz crystal microbalance DNA sensor for detection of *Escherichia coli* O157: H7. *Biosens. Bioelectron.* **21**(7), 1178–1185.
32. Wang, L. J., Wei, Q. S., Wu, C. S., Hu, Z. Y., Ji, J., and Wang, P. (2008). The *Escherichia coli* O157:H7 DNA detection on a gold nanoparticle-enhanced piezoelectric biosensor. *Chin. Sci. Bull.* **53**(8), 1175–1184.
33. Park, I. S., Kim, W. Y., and Kim, N. (2000). Operational characteristics of an antibody-immobilized QCM system detecting *Salmonella* spp. *Biosens. Bioelectron.* **15**, 167–172.
34. Tombelli, S., Mascini, M., Sacco, C., and Turner, A. P. F. (2000). A DNA piezoelectric biosensor assay coupled with a polymerase chain reaction for bacterial toxicity determination in environmental samples. *Anal. Chim. Acta* **418**, 1–9.
35. Zhao, H. Q., Lin, L., Li, J. R., Tang, J. A., Duan, M. X., and Jiang, L. (2001). DNA biosensor with high sensitivity amplified by gold nanoparticles. *J. Nanopart. Res.* **3**, 321–323.
36. Mo, X. T., Zhou, Y. P., Lei, H., and Deng, L. (2002). Microbalance-DNA probe method for the detection of specific bacteria in water. *Enzyme Microb. Technol.* **30**, 583–589.
37. Zhou, X. D., Liu, L. J., Hu, M., Wang, L. L., and Hu, J. M. (2002). Detection of *Hepatitis B* virus by piezoelectric biosensor. *J. Pharm. Biomed. Anal.* **27**, 341–345.
38. He, F. J., and Liu, S. Q. (2004). Detection of P. *aeruginosa* using nano-structured electrode-separated piezoelectric DNA biosensor. *Talanta* **62**, 271–277.
39. Galipeau, D. W., Story, P. R., Vetelino, K. A., and Mileham, R. D. (1997). Surface acoustic wave microsensors and applications. *Smart Mater. Struct.* **6**(6), 658–667.

40. Berkenpas, E., Millard, P., and da Cunha, M. P. (2006). Detection of *Escherichia coli* O157:H7 with langasite pure shear horizontal surface acoustic wave sensors. *Biosens. Bioelectron.* **21**(12), 2255–2262.

41. Deobagkar, D. D., Limaye, V., Sinha, S., and Yadava, R. D. S. (2005). Acoustic wave immunosensing of Escherichia coli in water. *Sens. Actuators, B Chem.* **104**(1), 85–89.

42. Moll, N., Pascal, E., Dinh, D. H., Pillot, J. P., Bennetau, B., Rebiere, D., et al. (2007). A Love wave immunosensor for whole *E-coli* bacteria detection using an innovative two-step immobilisation approach. *Biosens. Bioelectron.* **22**(9–10), 2145–2150.

43. Moll, N., Pascal, E., Dinh, D. H., Lachaud, J. L., Vellutini, L., Pillot, J. P., et al. (2008). Multipurpose Love acoustic wave immunosensor for bacteria, virus or proteins detection. *Irbm* **29**(2–3), 155–161.

44. Branch, D. W., and Brozik, S. M. (2004). Low-level detection of a *Bacillus anthracis* simulant using Love-wave biosensors on 36 degrees YX LiTaO3. *Biosens. Bioelectron.* **19**(8), 849–859.

45. Jin, X., Gao, Z., Pan, H., Zhu, H., Zhou, M., and Chen, H. (2003). The surface acoustic wave biosensor for detecting the gene of Staphylococal Enterotoxin B. *Proceedings of the International Symposium on Test and Measurement 1*, 261–264.

46. Bisoffi, M., Hjelle, B., Brown, D. C., Branch, D. W., Edwards, T. L., Brozik, S. M., et al. (2008). Detection of viral bioagents using a shear horizontal surface acoustic wave biosensor. *Biosens. Bioelectron.* **23**(9), 1397–1403.

47. Lange, K., Rapp, B. E., and Rapp, M. (2008). Surface acoustic wave biosensors: a review. *Anal. Bioanal. Chem.* **391**(5), 1509–1519.

48. Carrascosa, L. G., Moreno, M., Alvarez, M., and Lechuga, L. M. (2006). Nanomechanical biosensors: a new sensing tool. *Trends Analyt. Chem.* **25**(3), 196–206.

49. Waggoner, P. S., and Craighead, H. G. (2007). Micro- and nanomechanical sensors for environmental, chemical, and biological detection. *Lab Chip* **7**(10), 1238–1255.

50. Davila, A. P., Jang, J., Gupta, A. K., Walter, T., Aronson, A., and Bashir, R. (2007). Microresonator mass sensors for detection of *Bacillus anthracis* Sterne spores in air and water. *Biosens. Bioelectron.* **22**(12), 3028–3035.

51. Campbell, G. A., and Mutharasan, R. (2006). Piezoelectric-excited millimeter-sized cantilever (PEMC) sensors detect *Bacillus anthracis* at 300 spores/mL. *Biosens. Bioelectron.* **21**(9), 1684–1692.

52. Ilic, B., Czaplewski, D., Zalalutdinov, M., Craighead, H. G., Neuzil, P., Campagnolo, C., and Batt, C. (2001). Single cell detection with micromechanical oscillators. *J. Vac. Sci. Technol. B* **19**(6), 2825–2828.

53. Johnson, L., Gupta, A. T. K., Ghafoor, A., Akin, D., and Bashir, R. (2006). Characterization of vaccinia virus particles using microscale silicon cantilever resonators and atomic force microscopy. *Sens. Actuators, B Chem.* **115**(1), 189–197.

54. Weeks, B. L., Camarero, J., Noy, A., Miller, A. E., Stanker, L., and De Yoreo, J. J. (2003). A microcantilever-based pathogen detector. *Scanning* **25**, 297–299.

55. Erickson, D., Mandal, S., Yang, A. H. J., and Cordovez, B. (2008). Nanobiosensors: optofluidic, electrical and mechanical approaches to biomolecular detection at the nanoscale. *Microfluid. Nanofluidics* **4**(1–2), 33–52.

56. Shankaran, D. R., Gobi, K. V. A., and Miura, N. (2007). Recent advancements in surface plasmon resonance immunosensors for detection of small molecules of biomedical, food and environmental interest. *Sens. Actuators, B Chem.* **121**(1), 158–177.

57. Waswa, J., Irudayaraj, J., and DebRoy, C. (2007). Direct detection of *E-coli* O157:H7 in selected food systems by a surface plasmon resonance biosensor. *LWT-Food Sci. Technol.* **40**(2), 187–192.

58. Subramanian, A., Irudayaraj, J., and Ryan, T. (2006). A mixed self-assembled monolayer-based surface plasmon immunosensor for detection of *E-coli* O157: H7. *Biosens. Bioelectron.* **21**(7), 998–1006.

59. Lan, Y. B., Wang, S. Z., Yin, Y. G., Hoffmann, W. C., and Zheng, X. Z. (2008). Using a surface plasmon resonance biosensor for rapid detection of *Salmonella* typhimurium in chicken carcass. *J. Bionic Eng.* **5**(3), 239–246.

60. Waswa, J. W., DebRoy, C., and Irudayaraj, J. (2006). Rapid detection of *Salmonella enteritidis* and *Escherichia coli* using surface plasmon resonance biosensor. *J. Food Process Eng.* **29**(4), 373–385.

61. Chen, L. L., Deng, L., Liu, L. L., and Peng, Z. H. (2007). Immunomagnetic separation and MS/SPR end-detection combined procedure for rapid detection of *Staphylococcus aureus* and protein A. *Biosens. Bioelectron.* **22**(7), 1487–1492.

62. Jyoung, J. Y., Hong, S. H., Lee, W., and Choi, J. W. (2006). Immunosensor for the detection of *Vibrio cholerae* O1 using surface plasmon resonance. *Biosens. Bioelectron.* **21**(12), 2315–2319.

63. Chung, J. W., Kim, S. D., Bernhardt, R., and Pyun, J. C. (2005). Application of SPR biosensor for medical diagnostics of human hepatitis B virus (hHBV). *Sens. Actuators, B Chem.* **111**, 416–422.

64. Vaisocherova, H., Mrkvova, K., Piliarik, M., Jinoch, P., Steinbachova, M., and Homola, J. (2007). Surface plasmon resonance biosensor for direct detection of antibody against Epstein-Barr virus. *Biosens. Bioelectron.* **22**(6), 1020–1026.

65. Taylor, A. D., Ladd, J., Yu, Q., Chen, S., Homola, J., and Jiang, S. (2006). Quantitative and simultaneous detection of four foodborne bacterial pathogens with a multi-channel SPR sensor. *Biosens. Bioelectron.* **22**(5), 752–758.

66. Homola, J. (2008). Surface plasmon resonance sensors for detection of chemical and biological species. *Chem. Rev.* **108**(2), 462–493.

67. Hoa, X. D., Kirk, A. G., and Tabrizian, M. (2007). Towards integrated and sensitive surface plasmon resonance biosensors: a review of recent progress. *Biosens. Bioelectron.* **23**, 151–160.

68. Koubova, V., Brynda, E., Karasova, L., Skvor, J., Homola, J., Dostalek, J., Tobiska, P., and Rosicky, J. (2001). Detection of foodborne pathogens using surface plasmon resonance biosensors. *Sens. Actuators, B Chem.* **74**, 100–105.

69. Vaughan, R. D., Carter, R. M., O'Sullivan, C. K., and Guilbault, G. G. (2003). A quartz crystal microbalance (QCM) sensor for the detection of *Bacillus cereus*. *Anal. Lett.* **36**, 731–747.

70. Kim, N., Park, I. S., and Kim, D. K. (2004). Characteristics of a label-free piezoelectric immunosensor detecting *Pseudomonas aeruginosa*. *Sens. Actuators, B Chem.* **100**, 432–438.

71. Su, X. L., and Li, Y. (2005). Surface plasmon resonance and quartz crystal microbalance immunosensors for detection of *Escherichia coli* O157: H7. *Trans. ASAE* **48**, 405–413.

72. Zhang, D., Carr, D. J., and Alocilja, E. C. (2009). Fluorescent bio-barcode DNA assay for the detection of *Salmonella enterica* serovar Enteritidis. *Biosens. Bioelectron.* **24**(5), 1377–1381.

73. Taitt, C. R., Anderson, G. P., Lingerfelt, B. M., Feldstein, M. J., and Ligler, F. S. (2002). Nine-analyte detection using an array-based biosensor. *Anal. Chem.* **74**(23), 6114–6120.

74. Li, Y. G., Cu, Y. T. H., and Luo, D. (2005). Multiplexed detection of pathogen DNA with DNA-based fluorescence nanobarcodes. *Nat. Biotechnol.* **23**(7), 885–889.

75. Epstein, J. R., Biran, I., and Walt, D. R. (2002). Fluorescence-based nucleic acid detection and microarrays. *Anal. Chim. Acta* **469**(1), 3–36.

76. Ko, S. H., and Grant, S. A. (2006). A novel FRET-based optical fiber biosensor for rapid detection of Salmonella Typhimurium. *Biosens. Bioelectron.* **21**(7), 1283–1290.

77. Kim, H., Kane, M. D., Kim, S., Dominguez, W., Applegate, B. M., and Savikhin, S. (2007). A molecular beacon DNA microarray system for rapid detection of *E-coli* O157:H7 that eliminates the risk of a false negative signal. *Biosens. Bioelectron.* **22**(6), 1041–1047.

78. Geng, T., Uknalis, J., Tu, S. I., and Bhunia, A. K. (2006). Fiber-optic biosensor employing Alexa-Fluor conjugated antibody for detection of *Escherichia coli* O157: H7 from ground beef in four hours. *Sensors* **6**(8), 796–807.

79. Geng, T., Morgan, M. T., and Bhunia, A. K. (2004). Detection of low levels of *Listeria monocytogenes* cells by using a fiber-optic immunosensor. *Appl. Environ. Microbiol.* **70**, 6138–6146.

80. Nanduri, V., Kim, G., Morgam, M. T., Ess, D., Hahm, B., Kothapalli, A., et al. (2006). Antibody immobilization on waveguides using a flow-through system shows improved *Listeria monocytogenes* detection in an automated fiber optic biosensor: RAPTOR™. *Sensors* **6**, 808–822.

81. Ho, J.-A. A., Hsu, H.-W., and Huang, M.-R. (2004). Liposome-based microcapillary immunosensor for detection of *Escherichia coli* O157:H7. *Anal. Biochem.* **330**, 342–349.

82. Abel, A. P., Weller, M. G., Duveneck, G. L., Ehrat, M., and Widmer, H. M. (1996). Fiber-optic evanescent wave biosensor for the detection of oligonucleotides. *Anal. Chem.* **68**, 2905–2912.

83. Liu, X., and Tan, W. (1999). A fiber-optic evanescent wave DNA biosensor based on novel molecular beacons. *Anal. Chem.* **71**, 5054–5059.

84. Liu, C. H., Liao, K. T., and Huang, H. J. (2000). Amperometric immunosensors based on protein A coupled polyaniline-perfluorosulfonated ionomer composite electrodes. *Anal. Chem.* **72**, 2925–2929.

85. Baeumner, A. J., Cohen, R. N., Miksic, V., and Min, J. (2003). RNA biosensor for the rapid detection of viable *Escherichia coli* in drinking water. *Biosens. Bioelectron.* **18**, 405–413.

86. Esch, M. B., Locascio, L. E., Tarlov, M. J., and Durst, R. A. (2001). Detection of viable *Cryptosporidium parvum* using DNA-modified liposomes in a microfluidic chip. *Anal. Chem.* **73**, 2952–2958.

87. Hartley, H. A., and Baeumner, A. J. (2003). Biosensor for the specific detection of a single viable *B. anthracis* spore. *Anal. Bioanal. Chem.* **376**, 319–327.

88. Theegala, C. S., Small, D. D., and Monroe, W. T. (2008). Oxygen electrode-based single antibody amperometric biosensor for qualitative detection of *E-coli* and bacteria in water. *J. Environ. Sci. Health A Tox. Hazard Subst. Environ. Eng.* **43**(5), 478–487.

89. Singh, C., Agarwal, G. S., Rai, G. P., Singh, L., and Rao, V. K. (2005). Specific detection of *Salmonella typhi* using renewable amperometric immunosensor. *Electroanalysis* **17**(22), 2062–2067.

90. Aguilar, Z. P., and Sirisena, M. (2007). Development of automated amperometric detection of antibodies against *Bacillus anthracis* protective antigen. *Anal. Bioanal. Chem.* **389**(2), 507–515.

91. Zhao, G., Xing, F., and Deng, S. (2007). A disposable amperometric enzyme immunosensor for rapid detection of *Vibrio parahaemolyticus* in food based on agarose/Nano-Au membrane and screen-printed electrode. *Electrochem. Commun.* **9**(6), 1263–1268.

92. Lermo, A., Campoy, S., Barbe, J., Hernandez, S., Alegret, S., and Pividori, M. (2007). In situ DNA amplification with magnetic primers for the electrochemical detection of food pathogens. *Biosens. Bioelectron.* **22**(9–10), 2010–2017.

93. Elsholz, B., Worl, R., Blohm, L., Albers, J., Feucht, H., Grunwald, T., et al. (2006). Automated detection and quantitation of bacterial RNA by using electrical microarrays. *Anal. Chem.* **78**(14), 4794–4802.

94. Farabullini, F., Lucarelli, F., Palchetti, I., Marrazza, G., and Mascini, M. (2007). Disposable electrochemical genosensor for the simultaneous analysis of different bacterial food contaminants. *Biosens. Bioelectron.* **22**(7), 1544–1549.
95. Gau, J.-J., Lan, E. H., Dunn, B., Ho, C.-M., and Woo, J. C. S. (2001). A MEMS based amperometric detector for *E. coli* bacteria using self-assembled monolayers. *Biosens. Bioelectron.* **16**, 745–755.
96. Nagai, H., Murakami, Y., Yokoyama, K., and Tamiya, E. (2001). High-throughput PCR in silicon based microchamber array. *Biosens. Bioelectron.* **16**, 1015–1019.
97. Zhang, Z. X., and Li, M. Q. (2005). Electrostatic microcantilever array biosensor and its application in DNA detection. *Prog. Biochem. Biophys.* **32**, 314–317.
98. Ramanaviciene, A., and Ramanavicius, A. (2004). Pulsed amperometric detection of DNA with an ssDNA/polypyrrole-modified electrode. *Anal. Bioanal. Chem.* **379**, 287–293.
99. Berney, H., West, J., Haefele, E., Alderman, J., Lane, W., and Collins, J. K. (2000). A DNA diagnostic biosensor: development, characterisation and performance. *Sens. Actuators, B Chem.* **68**, 100–108.
100. Lee, J. S., Choi, Y.-K., Pio, M., Seo, J., and Lee, L. P. (2002). Nanogap capacitors for label free DNA analysis. *BioMEMS Bionanotechnol.* **729**, 185–190.
101. Diamond, D. (1998). *Principles of Chemical and Biological Sensors*. John Wiley & Sons, New York.
102. Eggins, B. R. (2002). *Chemical Sensors and Biosensors*. John Wiley & Sons, Chichester.
103. Palchetti, I., and Mascini, M. (2008). Electroanalytical biosensors and their potential for food pathogen and toxin detection. *Anal. Bioanal. Chem.* **391**(2), 455–471.
104. Hafeman, D. G., Parce, J. W., and Mcconell, H. M. (1988). Light-addressable potentiometric sensor for biochemical systems. *Science* **240**(4856), 1182–1185.
105. Ercole, C., Del Gallo, M., Mosiello, L., Baccella, S., and Lepidi, A. (2003). *Escherichia coli* detection in vegetable food by a potentiometric biosensor. *Sens. Actuators, B Chem.* **91**(1–3), 163–168.
106. Rahman, M. A., Kumar, P., Park, D. S., and Shim, Y. B. (2008). Electrochemical sensors based on organic conjugated polymers. *Sensors* **8**(1), 118–141.
107. Muhammad-Tahir, Z., and Alocilja, E. C. (2003a). A conductometric biosensor for biosecurity. *Biosens. Bioelectron.* **18**(5–6), 813–819.
108. Muhammad-Tahir, Z., and Alocilja, E. C. (2003b). Fabrication of a disposable biosensor for *Escherichia coli* O157:H7 detection. *IEEE Sens. J.* **3**, 345–351.
109. Muhammad-Tahir, Z., Alocilja, E. C., and Grooms, D. L. (2005a). Polyaniline synthesis and its biosensor application. *Biosens. Bioelectron.* **20**, 1690–1695.
110. Muhammad-Tahir, Z., Alocilja, E. C., and Grooms, D. L. (2005b). Rapid detection of Bovine viral diarrhea virus as surrogate of bioterrorism agents. *IEEE Sens. J.* **5**(4), 757–762.
111. Hnaiein, M., Hassen, W. M., Abdelghani, A., Fournier-Wirth, C., Coste, J., Bessueille, F., et al. (2008). A conductometric immunosensor based on functionalized magnetite nanoparticles for *E. coli* detection. *Electrochem. Commun.* **10**(8), 1152–1154.
112. Katz, E., and Willner, I. (2003). Probing biomolecular interactions at conductive and semiconductive surfaces by impedance spectroscopy: routes to impedimetric immunosensors, DNA-Sensors, and enzyme biosensors. *Electroanalysis* **15**(11), 913–947.
113. Radke, S. M., and Alocilja, E. C. (2005). A high density microelectrode array biosensor for detection of *E. coli* O157:H7. *Biosens. Bioelectron.* **20**(8), 1662–1667.

114. Nandakumar, V., La Belle, J. T., Reed, J., Shah, M., Cochran, D., Joshi, L., and Alford, T. L. (2008). A methodology for rapid detection of *Salmonella* Typhimurium using label-free electrochemical impedance spectroscopy. *Biosens. Bioelectron.* **24**(4), 1039–1042.

115. Varshney, M., and Li, Y. (2007). Interdigitated array microelectrode based impedance biosensor coupled with magnetic nanoparticle-antibody conjugates for detection of *Escherichia coli* O157:H7 in food samples. *Biosens. Bioelectron.* **22**(11), 2408–2414.

116. Ruan, C. M., Yang, L. J., and Li, Y. B. (2002). Immunobiosensor chips for detection of *Escherichia coli* O157: H7 using electrochemical impedance spectroscopy. *Anal. Chem.* **74**, 4814–4820.

117. Shah, J., Chemburu, S., Wilkins, E., and Abdel-Hamid, I. (2003). Rapid amperometric immunoassay for *Escherichia coli* based on graphite coated nylon membranes. *Electroanalysis* **15**, 1809–1814.

118. Wang, S. X., and Li, G. (2008). Advances in giant magnetoresistance biosensors with magnetic nanoparticle tags: review and outlook. *IEEE Trans. Magn.* **44**(7), 1687–1702.

119. Tamanaha, C. R., Mulvaney, S. P., Rife, J. C., and Whitman, L. J. (2008). Magnetic labeling, detection, and system integration. *Biosens. Bioelectron.* **24**(1), 1–13.

120. Edelstein, R. L., Tamanaha, C. R., Sheehan, P. E., Miller, M. M., Baselt, D. R., Whitman, L. J., and Colton, R. J. (2000). The BARC biosensor applied to the detection of biological warfare agents. *Biosens. Bioelectron.* **14**(10–11), 805–813.

121. Ruan, C. M., Zeng, K. F., Varghese, O. K., and Grimes, C. A. (2003). Magnetoelastic immunosensors: amplified mass immunosorbent assay for detection of *Escherichia coli* O157:H7. *Anal. Chem.* **75**(23), 6494–6498.

122. Sandhu, A., Kumagai, Y., Lapicki, A., Sakamoto, S., Abe, M., and Handa, H. (2007). High efficiency Hall effect micro-biosensor platform for detection of magnetically labeled biomolecules. *Biosens. Bioelectron.* **22**(9–10), 2115–2120.

123. Pal, S., and Alocilja, E. C. (2009). Electrically-active polyaniline coated magnetic (EAPM) nanoparticle as novel transducer in biosensor for detection of *Bacillus anthracis* spores in food samples. *Biosens. Bioelectron. J.* **24**(5), 1437–1444.

124. Alam, J., Riaz, U., and Ahmad, S. (2007). Effect of ferrofluid concentration on electrical and magnetic properties of the $Fe_3O_4$/PANI nanocomposites. *J. Magn. Magn. Mater.* **314**(2), 93–99.

125. Kryszewski, M., and Jeszka, J. K. (1998). Nanostructured conducting polymer composites - superparamagnetic particles in conducting polymers. *Synth. Met.* **94**(1), 99–104.

126. Kim, J. H., Cho, J. H., Cha, G. S., Lee, C. W., Kim, H. B., and Paek, S. H. (2000) *Biosens. Bioelectron.* **14**(12), 907–915.

127. Pal, S., Alocilja, E. C., and Downes, F. P. (2007). Nanowire labeled direct-charge transfer biosensor for detecting *Bacillus* species. *Biosens. Bioelectron. J.* **22**, 2329–2336.

128. Pal, S., Setterington, E., and Alocilja, E. C. (2008a). Electrically-active magnetic nanoparticles for concentrating and detecting *Bacillus anthracis* spores in a direct-charge transfer biosensor. *IEEE Sens. J.* **8**(6), 647–654.

129. Pal, S., Ying, W., Alocilja, E. C., and Downes, F. P. (2008b). Sensitivity and specificity performance of a direct-charge transfer biosensor for detecting *Bacillus cereus* in selected food matrices. *Biosyst. Eng.* **99**(4), 461–468.

130. Tims, T. B., and Lim, D. V. (2004) *J. Microbiol. Methods* **59**(1), 127–130.

131. Cheun, H. I., Makino, S. I., Watarai, M., Shirahata, T., Uchida, I., Takeshi, K. (2001). *J. Appl. Microbiol.* **91**(3), 421–426.

# GENERAL DETECTOR CAPABILITIES FOR FOOD SAFETY APPLICATIONS

S. HUANG, R. S. LAKSHMANAN, S. HORIKAWA, AND B. A. CHIN
*Materials Engineering, Auburn University, Auburn, Alabama*
J. M. BARBAREE
*Department of Biological Sciences, Auburn University, Auburn, Alabama*

## 1 INTRODUCTION

### 1.1 Threats to Food Safety

Every year, more than 76 million Americans suffer from foodborne illnesses that result in an estimated 325,000 hospitalizations and 5000 deaths [1]. Costs of these illnesses are between $9.3 and 12.9 billion in direct medical expenses [2]. Foodborne illnesses are primarily caused by four types of microorganisms (bacteria, fungi, eukaryotic parasites, and viruses) that are pathogenic, but commonly found in the natural environment.

The US Food and Drug Administration (FDA) and Centers for Disease Control and Prevention (CDC) have concluded that foodborne illness is one of the most serious, yet unavoidable, health problems facing the nation. The majority of foodborne illnesses can be attributed to changing human demographics, lifestyle choices, food consumption trends, mass transportation of food items, and microbial adaptation [3, 4]. In addition, the nation's aging population contributes to a rise in such illnesses; as one grows older, his/her immune system weakens, and, consequently, a further increase in the number of foodborne illnesses is anticipated. Another factor stems from new interests in international cuisines that increase the importation of exotic foods from many countries. These foods are grown, harvested, and often processed in foreign countries. Therefore, they must be shipped longer distances to reach the final consumers. As the health standards of foreign countries are often significantly different from those in the United States, food importation becomes an additional source of possible contamination. The greater transportation distances and longer-term storage of food may allow small amounts of bacteria and other pathogens to multiply and potentially reach their infectious doses.

### 1.2 Outbreaks of Foodborne Illnesses

Bacteria are responsible for more than 90% of the confirmed foodborne illnesses and deaths in humans reported to the CDC. Of the foodborne bacterial pathogens, *Salmonella* causes most of the foodborne illnesses worldwide [5]. For the nation's entire population, the CDC estimates that there are 173 cases of *Salmonella* illnesses per million people

each year [6]. In the United States, human gastrointestinal illnesses are most commonly due to *Salmonella* and *Escherichia coli* infections. *Salmonella* infection is usually caused by the *S. typhimurium*, *S. enteritidis*, or *S. heidelberg* serotypes [7].

In 1985, a large US outbreak of salmonellosis that occurred in Chicago was attributed to *S. typhimurium* in pasteurized milk from a single dairy plant [8]. In September 2006, the outbreak due to the *E. coli* O157:H7-contaminated fresh spinach resulted in 187 reported cases of illness in 27 states, including 97 hospitalizations, at least 29 cases of kidney failure, and 1 death. In December of the same year, another outbreak linked to Taco Bell restaurants in the northeastern United States was also caused by *E. coli* O157:H7. There were 71 people with illness reported from five states: New Jersey (33), New York (22), Pennsylvania (13), Delaware (2), and South Carolina (1) [9]. In 2008, several *Salmonella* outbreaks occurred in the United States. The most serious case of these occurred in the mid-April, when the *Salmonella* St. Paul outbreak involving contaminated tomatoes became one of the largest *Salmonella* outbreaks in the recent history, sickening at least 869 people and resulting in the hospitalization of 257 individuals. On the basis of the CDC's estimated ratio of nonreported salmonellosis cases to reported cases (38.6:1), around 52,826 illnesses resulted from the *Salmonella St. Paul* outbreak.

*Salmonella* and other foodborne pathogens (e.g. *E. coli* O157:H7) can be spread easily throughout the food chain. Daily consumed food items, such as oat cereal [3, 10], tomatoes [11], eggs [12], milk [13], vegetables and fruits (e.g. raw tomatoes), water [12], green onions, jalapeño peppers, red plum, peanut butter [14], and cilantro [15], have recently been found to be contaminated with *Salmonella*. Although it appears that more outbreaks are being linked to vegetable and fruit products, this has not been proven, because of the difficulty that scientists and inspectors often experience in locating the source of the pathogen contamination. Foodborne contamination is difficult to monitor because products may be cleaned at the harvesting site, transported to a warehouse, and then repackaged several times before reaching retail outlets. This leaves a lengthy trail that covers many states and often more than one country. In order to reduce the incidence of foodborne illnesses, there is an urgent need to develop a device capable of rapid, on-site detection of bacterial pathogens. The device needs to be inexpensive as well as easy to use so that it can readily be adopted by every link in the food chain, up to and including the final individual consumers.

### 1.3 Major Pathogenic Bacteria Studied for Food Safety

Pathogenic bacterial detection is of the utmost importance for the prevention and identification of problems related to health and safety [16]. Figure 1 summarizes the distribution of scientific literature covering bacterial detection, where *Salmonella is ranked as* the most commonly studied bacterium. Other than *Salmonella*, *E. coli*, *Listeria*, *Campylobacter*, and *Legionella* are also popularly studied.

### 1.4 Capability of Detectors for Foodborne Pathogen Detection

The prevention of foodborne illnesses depends on the availability of rapid, simple, and effective detection devices capable of identifying and distinguishing various pathogenic microorganisms in food, food production facilities, clinical medicine, and the natural environment. High sensitivity and selectivity are two important criteria for effective biological detection methods. Some pathogenic organisms, such as *E. coli* O157:H7, are

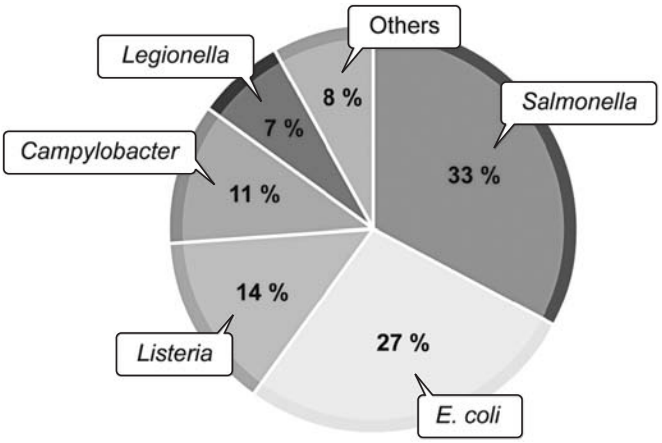



**FIGURE 1** The distribution of scientific literature covering the detection of pathogenic bacteria [16].

able to infect people at doses as small as a few cells. Hence, extremely sensitive methods are required to detect them [17–19]. At the same time, microbiological detection methods should be cheap and robust from a commercial applications point of view. For a pathogen detection method to be industrially successful, detection test equipment must be portable so that they can be taken outside of laboratory confines and used with a minimal need of skilled personnel [20, 21].

Today, intensive research is being conducted to develop new techniques for the early detection of the causes of foodborne illnesses. Traditional methods of identifying the pathogens responsible for foodborne illnesses are very time consuming (i.e. several days to yield results) and typically require highly trained personnel in laboratories with expensive equipment [22]. There is, therefore, a real need for the development of portable, rapid, specific, and sensitive biosensors to enable real-time, on-site detection of foodborne pathogens. To achieve the objective, various biosensing techniques have been developed and used in the food safety field. However, real-time biological monitoring remains a challenge. The ever-growing need for rapid detection of pathogenic microorganisms has resulted in an increased interest in the research and development of biosensor systems.

### 1.5 The Objective

In this review paper, we will provide an overview of general detectors that may be used to insure food safety and their capabilities. First, various bacterial detection methods will be classified and described. Next, the capability of each of the methods will be summarized, covering the working principle, detection limit, advantages, and weaknesses. Finally, phage-based detectors, especially one type of potential biosensor, phage-based magnetoelastic (ME) biosensors, will be discussed in detail.

## 2 DETECTORS FOR FOOD SAFETY APPLICATIONS

Figure 2 compares the number of articles using different bacterial detection methods. To date, polymerase chain reaction (PCR) [23] and culture-based methods (colony counting)

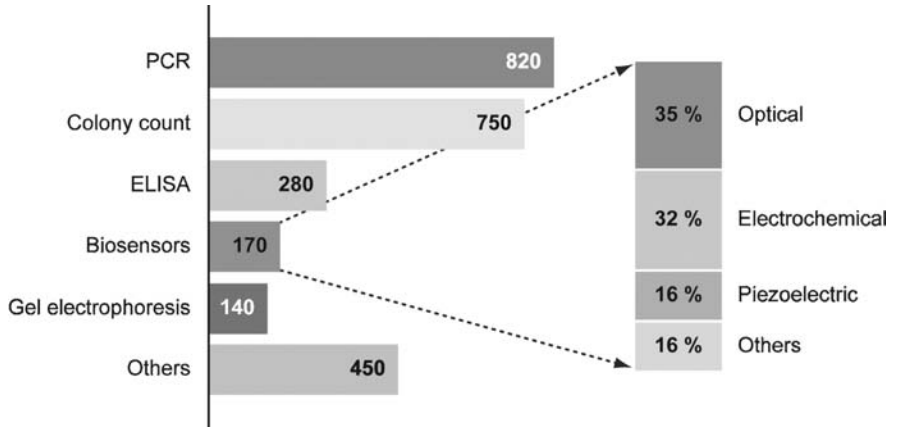



**FIGURE 2** Approximate number of articles using different techniques to detect and/or identify pathogenic bacteria [16].

[24] have been the most commonly used methods and are able to provide unambiguous results. Other than these methods, newly developed biosensor technologies and traditional enzyme-linked immunosorbent assay (ELISA)-based [25] methods are also promising and drawing a lot of attention.

### 2.1 Culture-Based Methods

Culture-based morphological evaluation has been one of the most commonly used bacterial identification methods for food safety. It relies on the use of microbiological media to selectively cultivate bacteria and colony count, followed by biochemical characterization. Although culture-based methods can be used to identify a very small number of bacterial pathogens (down to single pathogens) there are two major drawbacks: They are time-consuming and labor-intensive processes, which make them unsuitable for rapid, on-site bacterial detection methods that ideal future instruments must be able to perform. In culture-based methods, cumbersome and lengthy experimental steps such as pre-enrichment, selective enrichment, biochemical screening, and sometimes serological confirmation are required [26]. This may take 14–16 days to complete [27], depending on the target organisms. The second drawback is that no single culture-based test leads to the universal identification of unknown bacterial pathogens [26]. Some examples of culture-based methods used for detection of pathogenic bacteria in food are shown in Table 1.

### 2.2 Surveillance System

The surveillance system traditionally used to collect foodborne disease outbreak data has been overwhelmed by the emergence of megafarms, distribution centers, and transporters. To address these issues, an automated bioterrorism surveillance system, Real-time Outbreak Disease Surveillance (RODS), was implemented by the University of Pittsburgh in 1999. RODS collects data from multiple sources (e.g. clinics, laboratories, and drug sales) and uses this data to identify a bioterrorism event. Within a year, this system had been modified by RODS lab member Michael Wagner and his coworkers to collect data

**TABLE 1 Culture-Based Detectors**

| Year | Detection Method | Foodborne Pathogen | Source | Detection Limit | Reference |
|---|---|---|---|---|---|
| 1998 | Selective special media | *Legionella pneumophila* | Drinking water | <10 cfu/ml | 28 |
| 2001 | EN ISO-11290-1 | *Listeria monocytogenes* | Cheese, meat, eggs | <100 cfu/25 g | 29 |
| 2006 | NGFIS | *Listeria monocytogenes* | Minced meat, fermented sausage, and others | <10 cfu/g | 30 |
| | FDA | Listeria monocytogenes | Milk (goat) | <0.7 cfu/ml | |
| | USDA-FSIS Cold enrichment | | | | |

from 20,000 national retail locations and was being supported by a $300 million grant to equip all 50 states with biosurveillance systems [31].

### 2.3 Enzyme-Linked Immunosorbent Assay (ELISA)

ELISA, which may also be referred to as *EIA* (*enzyme immunoassay*), is a biochemical technique that is primarily used to quantify the presence of an antibody, hormone, or antigen in a sample [32]. In the food industry, ELISA is used as a rapid quality control test to identify the presence of allergens in foods such as milk, peanuts, walnuts, almonds, and eggs [33].

ELISA is based on the reaction between a substrate-specific enzyme and an appropriate antibody (specific to that antigen) to produce a visible signal. Older ELISA tests utilized a chromogenic or color-generation substrate to produce a visible signal, but newer ELISA assays employ a fluorogenic substrate, where the amount of fluorescence can be accurately quantified by a spectrophotometer, hence providing much higher sensitivity.

There are three types of ELISA: (i) "direct" or sandwich ELISA, which uses an immobilized antibody to detect the presence of a particular antigen in a sample; (ii) indirect ELISA, which uses an antigen to look for a specific antibody in a sample; and (iii) competitive ELISA, where the competitive binding abilities of two antibodies are determined by comparing the binding signals to their immobilized antigens.

Generally, indirect ELISA is used for determining serum antibody concentrations. This method, shown in Figure 3, involves five steps: (1) *Antigen immobilization*, (2) *Blocking*, (3) *Primary antibody immobilization*, (4) *Secondary antibody immobilization*, and (5) *Substrate reaction*. The specific substrate reacts with the antibody–enzyme complex and incubates for color development. This final signal can be viewed/quantified using a spectrophotometer or spectrofluorometer.

In most cases, this final signal is quantified by measuring the optical density (OD) with a microplate reader. A standard curve is plotted as the concentration of a standard antigen versus the corresponding mean OD value, and the sample concentration can then be interpolated from the standard curve. However, indirect ELISA suffers from two major

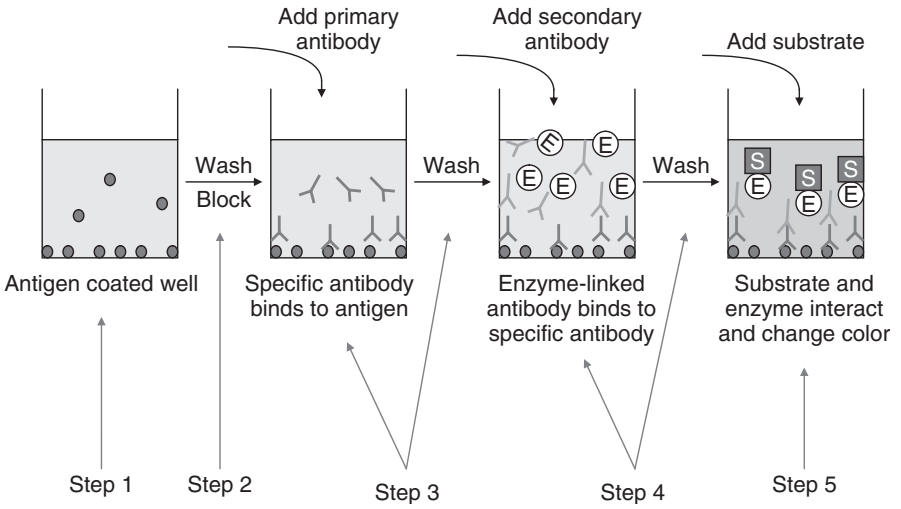



**FIGURE 3** Schematic of ELISA procedure for indirect ELISA.

disadvantages: (i) as the antigen immobilization on the well is nonspecific, any protein in the sample will bind to the plate and produce a noisy signal; and (ii) during the antigen immobilization, the analyte in the serum must compete with other serum proteins, thus decreasing the antigen–protein binding levels.

In order to overcome these problems, the sandwich or direct ELISA was developed and is used to detect sample antigens of biological warfare agents [34]. The procedure is shown in Figure 4 and is generally similar to the one used for the indirect ELISA. Compared to other ELISA methods, the sandwich ELISA has a higher binding affinity because, even for impure samples, the antibodies still bind selectively with any antigens that may be present. Moreover, by using the primary antibody, the chance that other proteins in the sample will adsorb nonspecifically to the plate well decreases when the quantity of immobilized antigens increases. Generally, using a polyclonal antibody for ELISA will increase the number of possible detection objects, while a monoclonal antibody will improve the specificity and lower the background noise.

The third type of ELISA uses competitive binding and is therefore referred to as *competitive ELISA*. This method is somewhat different from the previous ones. First, the unlabeled antibody is incubated with the antigen to form an antibody–antigen complex that is added to an antigen-coated well, and the unbound antibody is washed away. The secondary antibody (specific to the primary antibody) that has been conjugated with the enzyme is then applied to the well, and a substrate is added to react with the remaining enzymes to convert the bound antibody to a detectable signal (i.e. a chromogenic or fluorescent signal). This approach was dubbed "competitive" because when the complexes are formed, the more antigens exist in the sample, the fewer antibodies will be able to bind to the antigen in the well. As a result, the higher the original antigen concentration, the weaker the final signal.

Besides the stand-alone methods described above, ELISA can be combined with immunoseparation techniques. Mansfield et al. [35] have used immunomagnetic beads to separate *Salmonella* serovar cells, followed by ELISA to detect the cells in raw chicken.

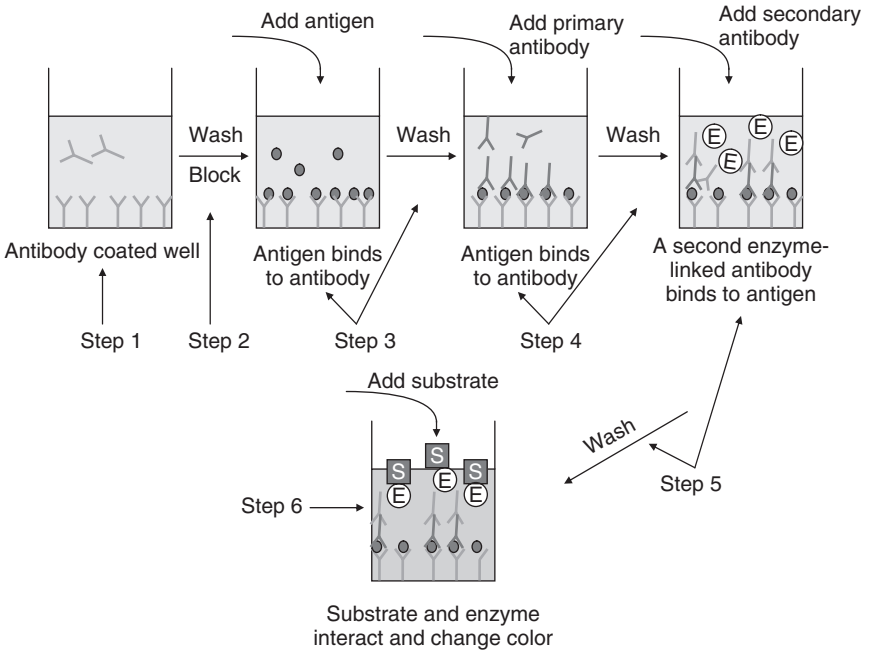



**FIGURE 4** Schematic of ELISA procedure for sandwich ELISA.

**TABLE 2 Bacterial Pathogen Detection Using ELISA**

| Year | Detection Method | Foodborne Pathogen | Source | Detection Limit | Reference |
|---|---|---|---|---|---|
| 1999 | Sandwich ELISA | *Listeria monocytogenes* | Milk (1:10 diluted) | $1 \times 10^3$ cells/ml | 36 |
| 2001 | IMS–ELISA | *Salmonella* serovars | Raw chicken | $10^6$ cells/ml | 35 |
| | Sandwich ELISA | *Salmonella* | Pork, chicken, beef | 1–10 cells/25 g | 37 |
| 2004 | ELISA | *Escherichia coli O157* | Ground beef | $1.2 \times 10^3$ cfu/ml | 38 |
| | | *Campylobacter fetus* | Bovine preputial washing and vaginal mucus samples | $10^5$ cells/ml | 27 |

Some examples of pathogenic bacterial detection using ELISA techniques are shown in Table 2.

### 2.4 Polymerase Chain Reaction (PCR)

PCR is a vital tool that is used to amplify specific regions of a DNA strand (i.e. a single gene, a part of a gene, or a noncoding sequence). The name was derived from DNA

polymerase, which is used to amplify a fragment of DNA by enzymatic replication. Generally, PCR methods require 20–40 thermal cycles of replication. As the number of cycles goes up, the target DNA fragments replicate. This replication is exponentially amplified and is therefore called a *chain reaction*.

In order to set up a PCR process, several components and reagents are required [39]. These include (i) a DNA template, (ii) thermoresistive DNA polymerase, (iii) a buffer solution, (iv) forward and reverse primers, (v) deoxynucleoside triphosphates (dNTPs), and (vi) divalent cations (i.e. $Mg^{2+}$ or $Mn^{2+}$) and a monovalent cation (i.e. $K^{+}$).

In PCR, a small amount of the DNA target is added to the six components listed above in a test tube. Each replication cycle of this mixture is composed of three steps (shown in Fig. 5) that are mainly controlled by the temperature: (i) *Denaturation*: separating dsDNA (double-stranded deoxyribonucleic acid) into ssDNA (single-stranded deoxyribonucleic acid) at a temperature of 94–96°C. (ii) *Annealing*: allowing the two primers to anneal their complementary DNA sequences, and (iii) *Extension*: extending the primers with the activity of DNA polymerase to synthesize complementary strands. The amount of DNA target will double after each cycle, resulting in exponential amplification of the DNA target. As each cycle requires several minutes, more than a billion molecules of DNA can be produced in hours. Following amplification, the final PCR products are analyzed to confirm that the DNA fragment has the original defined length. Agarose gel electrophoresis is used to determine the length of the DNA fragments through comparison with the migration of a DNA ladder, which is made up of molecular weight markers containing DNA fragments of a known size.

PCR has become a common technique and is widely used in fields such as molecular biology, clinical microbiology, forensic science, food safety, and many other applications [40]. In food safety, PCR is used to detect bacterial pathogens in water [21], milk, chicken

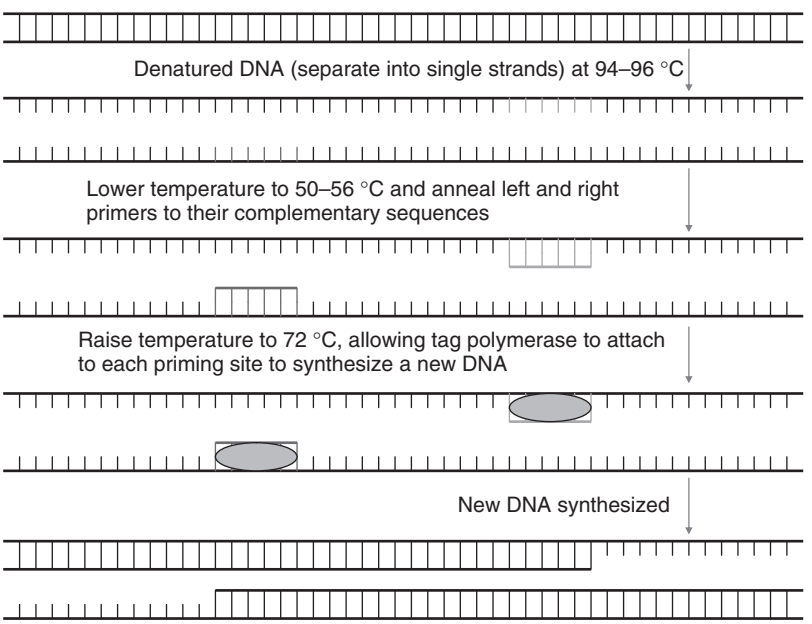



**FIGURE 5** Schematic diagram of PCR first replication cycle.

fecal samples [41], and ground beef [42] and has been used to detect *Bacillus anthracis* [43–45] in a variety of media.

Overall, PCR offers advantages such as low detection limits and rapid replication. It is also very robust and is capable of amplifying specific sequences from a few DNA molecules. However, several disadvantages do limit its use: (i) a number of techniques and procedures are required to optimize the PCR conditions, and even a minor contamination of sample DNA can yield spurious results; (ii) the selection of a suitable primer is also a challenge due to the need for some prior knowledge of the target DNA sequence; and (iii) trained personnel, along with extremely clean and controlled environments, are required.

On the basis of the "standard" PCR technique described above, small modifications in PCR protocol or components lead to a large number of variants of PCR, such as real-time PCR and multiplexed PCR. In general, real-time PCR employs a double fluorescent-labeled probe (labeled with a reporter dye and a quencher dye) complementary to a partial region of the target gene located between two primers. During the extension step of thermal cycling, the reporter dye departs from the quenching dye due to the cleavage of the probe by the activity of DNA polymerase. This results in fluorescence emission. DNA amplification can be monitored in a real-time manner by measuring the fluorescence signals. Multiplex PCR is another derivative that uses multiple pairs of primers designed to perform simultaneous amplification of different genes. Table 3 lists some applications of PCR techniques used for foodborne pathogen detection. PCR has been successfully combined with other techniques such as ELISA and immunomagnetic separation (IMS).

## 3 BIOSENSOR TECHNIQUES

The use of biosensors has increased dramatically in recent years. As defined in the Oxford English Dictionary, *a sensor is a device that detects or measures a physical property and records, indicates or otherwise responds to it*, and a biosensor does this by applying biological agents in the detection process. There are two main parts to a biosensor: a transducer and a bioreceptor. Figure 6 shows a schematic representation of a biosensor that uses a biosensing element as its bioreceptor, along with a transducer system and the associated electronics or signal processors that display the results in a user-friendly way [62].

When a specific biological reaction occurs between the biosensing element and the target antigens, a physical and/or chemical change takes place on the biointerface. The transducer is responsible for converting this change into a measurable signal. This signal will then be sent to the output system to be amplified, processed, and displayed [63].

Sensors can be divided into three types, namely, physical, chemical, and biological. As their name suggests, physical sensors measure physical quantities such as length, weight, temperature, and pressure, while chemical sensors respond quantitatively to a particular analyte in a selective way through a chemical reaction. Biosensors incorporate a biological sensing element, which is connected to the transducer.

Biosensors are now being used in many fields, for example, in industrial process monitoring, environmental monitoring, foodborne pathogen detection, and healthcare. The most popular medical application of biosensors is to monitor glucose levels in diabetic patients. One particularly desirable goal for medical biosensors is to create a type of implantable biosensor capable of continuously monitoring a metabolite; an implantable

**TABLE 3 Pathogenic Bacterial Detection Using PCR Methods**

| Year | Detection Method | Foodborne Pathogen | Source | Detection Limit | Reference |
|---|---|---|---|---|---|
| 1997 | Real-timePCR | *Listeria monocytogenes* | Ground beef | 3 cfu/g | 46 |
| 1998 | PCR | *Legionella pneumophila* | Water | <10 cfu/ml | 28 |
| 2002 | PCR | *E. coli* | Pasteurized milk | $10^3$ cfu/ml | 47 |
| | PCR–ELISA | *E. coli* | Pasteurized milk | $10^2$ cfu/ml | 47 |
| 2003 | Real-time PCR | *E. coli* | Stream water | $10^2$ bacteria/ml | 48 |
| | PCR | *Listeria monocytogenes* | Salmon | 2 cfu/25 g | 49 |
| | | *Listeria monocytogenes* | Frankfurter | 10 cfu/25 g | 49 |
| 2004 | Real-time PCR | *Yersinia enterocolitica* | Pork (juice) | $4.2 \times 10^3$ cfu/ml | 50 |
| | | *Salmonella* spp. | Artificially contaminated meat and milk | <5 cells/25 g | 51 |
| | PCR–ELISA | *Salmonella* | Artificially contaminated meat and milk | <5 cells/25 g | 51 |
| | IMS-real-time PCR | *Campylobacter* spp. | Chicken fecal samples | 100–150 cfu/ml | 52 |
| | Quantitative PCR | *S. enterica* | Drinking and fishpond water | 2 genomes (*invA* gene) | 53 |
| 2005 | Multiplex PCR | *E. coli* | Stools (considered for drinking water contamination) | $10^3$ cfu/ml | 54 |
| | | *E. coli* O157:H7 | Fecal and chicken samples | Detection rate of >99% | 55 |
| | Real-time PCR | *E. coli* O157:H7 | Ground beef | $1.3 \times 10^4$ cells/g | 56 |
| 2006 | Multiplex PCR | *S. enterica* ssp. *enterica* | Culture | Identification rate of 97% | 57 |
| 2007 | Quantitative PCR | *Helicobacter pylori* | Sewage and waste water | 2 cells/ml | 58 |
| | Multiplex real-time PCR | *Arcobacter* spp. | Culture | <10 cfu per PCR reaction | 59 |
| 2008 | Triplex real-time PCR | *Mycobacterium avium* complex | Culture | 10 cfu/g feces | 60 |
| | Multiplex single-tube nested PCR | *Vibrio cholerae* O1 | Environmental water samples | 1 pg? | 61 |

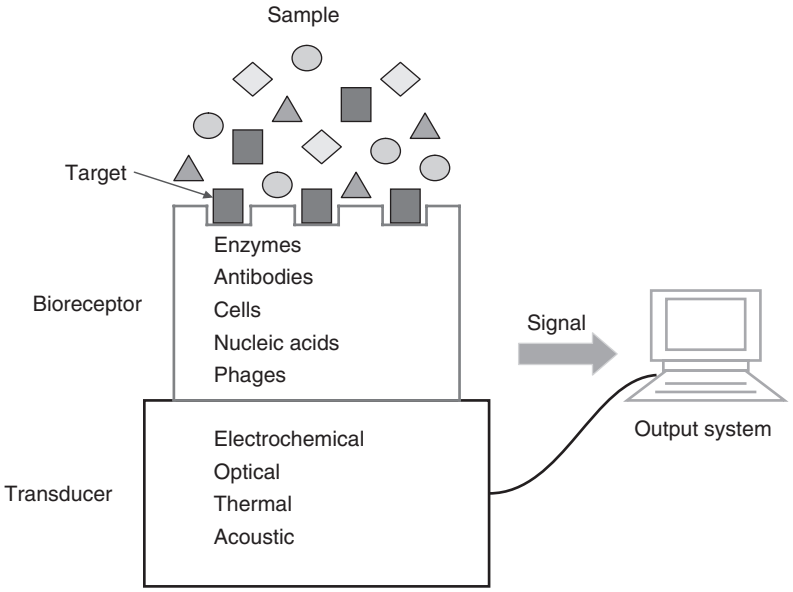



**FIGURE 6** Schematic configuration of a biosensor.

glucose biosensor would allow patients to continuously measure their glucose level in real time and adjust their medication accordingly. Biosensors also offer many advantages in detecting chemicals and foodborne pathogens. They are not only highly target specific and sensitive, but also respond rapidly, making them ideal for real-time detection. Some are even reusable and portable for on-the-spot analysis.

### 3.1 Biorecognition Elements

Biorecognition elements, generally referred to as *bioreceptors*, include enzymes, tissues, antibodies, and phages. Among these, antibodies and bacteriophages are the most commonly used biological components.

***3.1.1 Enzymes.*** Enzymes have been used as biorecognition probes for various biosensors. Enzymes usually aid in catalytic reactions to produce measurable signals. The catalytic power of enzymes, coupled with their high specificity of action, make them ideal biorecognition elements. Enzyme-based biosensors are used in electrochemical assays, for the detection of glucose, aromatic hydrocarbons, and monitoring of pH changes [64]. However, there is limited use of enzyme-based biosensors for the detection of bacterial pathogens [64].

***3.1.2 Nucleic Acid.*** Nucleic acid bioprobes have been widely used with different sensor platforms to detect pathogens in water supplies, food, and animals [65–67]. *Nucleic acid recognition element* refers to a segment of a nucleic acid (DNA/RNA) strand with specific sequences. Different nucleotides on the nucleic acid duplex make bonds only with counterparts with specific sequences. This property enables nucleic acid bioprobes to recognize the target nucleic acids of interested pathogens.

Aptamers, which are another group of nucleic acid bioprobes [64, 68], refer to nucleic acid ligands such as RNA, single-stranded ribonucleic acid (ssRNA), DNA, or peptides. They are selected from libraries of oligonucleotides with random sequences and synthesized against a broad range of molecules, proteins, and whole cells. Aptamers display high affinity and specificity toward the interested targets by shape instead of recognizing target species by DNA sequences [64]. Biosensors that combine aptamers as biorecognition elements with acoustic wave (AW) devices have been used to detect IgE antibodies [69] and HIV-1 Tat protein [70], and monitor blood-coagulation cascades [71].

***3.1.3 Antibodies.*** Antibodies, or immunoglobulins (Ig) [72], are produced by B cells, a type of white blood cell. These immune system-related proteins are present in the blood and other bodily fluids of vertebrates [72]. As antibodies are capable of identifying and neutralizing foreign objects, they have become widely used as diagnostic tools to detect bacteria and viruses.

Polyclonal and monoclonal antibodies are two kinds of antibodies, widely generated. Polyclonal antibodies are produced by injecting the target bacteria into an efficient antibody producing animal. The animal's immune system then builds a family of polyclonal antibodies with mildly varying specificities and affinities to the injected bacteria, after which the antibodies are extracted from the blood/serum. This process of immunization and extraction is time consuming and requires specialized facilities. To produce monoclonal antibodies, antibody-secreting lymphocytes are fused with a cancer cell line after isolation from animals, and then grown in a culture. Both polyclonal and monoclonal antibodies need to be purified by protein A/G or antigen-affinity chromatography [73]. In addition to the complexity of extracting and purifying, antibodies require controlled laboratory environments that are extremely sensitive to temperature and pH changes. Hence, there is a need for a more robust biorecognition elements that can withstand conditions in the field.

Currently, antibodies are being applied as a biorecognition layer on sensors for the specific capture of analytes [74]. Antibody-based sensors offer several advantages: there is no need for extensive sample clean-up and they require only limited hands-on time, while at the same time they offer high-throughput screening, real-time analysis, label-free detection, and the possibility of quantification [74]. There are several different types of antibody-based biosensors in use, namely, surface plasmon resonance (SPR) sensors, quartz crystal microbalances (QCMs), and cantilevers. They have become well-established techniques for the detection of the pathogens *E. coli* [75], *Salmonella* [76, 77], *Bacillus cereus*, and *Listeria monocytogenes* [78, 79]. Overall, antibody-based sensors are quite effective, adaptable for many applications, and hold great promise in the field of research. However, antibodies are sensitive to environmental conditions such as heat and pH.

***3.1.4 Bacteriophages.*** Bacteriophages, or phages, are viruses that infect only bacteria, but are much smaller in size (20–200 nm). Phages are absolute parasites, found ubiquitously wherever their bacterial hosts live (soil, sewage, animals [80], deep sea vents, water, food, and other environments [81]). Consequently, phages are estimated to be the most widely distributed and diverse entities (ranging from $10^{30}$ to $10^{32}$ in total population) on the earth [82].

Each bacteriophage contains an outer protein hull (or lipoprotein coat or capsid) and an enclosed nucleic acid genome. The enclosed genome can be ssRNA, dsRNA

(double-stranded ribonucleic acid), ssDNA, or dsDNA. These RNA/DNA strands have a circular or linear arrangement that is 5–500 kb long. On the basis of their life cycle, phages can be classified as either lytic or lysogenic. Lytic phages multiply only by a cycle, where the phage first attaches to the host cell and injects its own genome to take over much of the host metabolism, after which new phages are liberated after the host cell lyses. Lysogenic phages, in contrast, have modes of replication that do not destroy the host bacteria and bind with part of the bacterial genome. Lysogenic phages are sometimes referred to as *temperate*, but they can revert to a lytic cycle.

Classification of bacteriophages is difficult but practical for phage research. The International Committee on Taxonomy of Viruses classifies bacteriophages based on their morphology and the type of nucleic acid they enclose. Recently, Ackermann studied 5000 bacteriophages by electron microscopy, making this the largest category of viruses examined by microscopy methods so far [81]. Table 4 provides an overview of bacteriophage classification. These phages take one of four different shapes: tailed, polyhedral (with cubic symmetry), filamentous (with helical symmetry), and pleomorphic (without obvious symmetry). Most of these classified phages contain dsDNA, while only a small group contains ssDNA, ssRNA, or dsRNA. The dsDNA tailed phages are the major phages (95% of all those reported) on the planet [82] and also the oldest viruses [83]. Tail-less phages only include about 190 known viruses and account for less than 4% of the currently recognized bacterial viruses. They are classified into 10 families [84].

Bacteriophages have many applications. They have been successfully used for treating bacterial infections in the medical field due to their antibacterial activity. Environmentally, bacteriophages have been used in hydrological tracing in river systems and as dye markers due to their low adsorption when passing through ground water and ease of detection at low concentrations [85]. Phages also have many uses in food production. In 2006, the FDA approved the use of bacteriophages to kill *L. monocytogenes* bacteria on cheese [86]. Fluorescently labeled phages can serve as a recognition element for the detection of *S. typhimurium* and *E. coli* [71, 87].

**TABLE 4 Classification of Bacteriophages**

| Shape | Family | Morphology | Nucleic Acid |
|---|---|---|---|
| Tailed | *Myoviridae* | Nonenveloped, contractile tail | Linear dsDNA |
| | *Siphoviridae* | Nonenveloped, long noncontractile tail | |
| | *Podoviridae* | Nonenveloped, short noncontractile tail | |
| Polyhedral | *Microviridae* | Nonenveloped, isometric | Circular ssDNA |
| | *Tectiviridae* | Nonenveloped, isometric | Linear dsDNA |
| | *Corticoviridae* | Nonenveloped, isometric | Circular dsDNA |
| | *Leviviridae* | Nonenveloped, isometric | Linear ssRNA |
| | *Cystoviridae* | Enveloped, spherical | Segmented dsRNA |
| Filamentous | *Lipothrixviridae* | Enveloped, rod-shaped | Linear dsDNA |
| | *Inoviridae* | Nonenveloped, filamentous | Circular ssDNA |
| | *Rudiviridae* | Nonenveloped, rod-shaped | Linear dsDNA |
| Pleomorphic | *Fuselloviridae* | Nonenveloped, lemon-shaped | Circular dsDNA |
| | *Plasmaviridae* | Enveloped, pleomorphic | Circular dsDNA |
| | *Guttaviridae* | Droplet-shaped | Circular dsDNA |

Antibodies were the first proteins to be displayed on the surface of a phage [88]. This was achieved by fusing the coding sequence of the antibody variable regions to the amino terminus of the phage minor protein coat pIII. This type of phage–antibody combination is particularly useful for biological detection and has been demonstrated to have higher performance than monoclonal antibodies when used in several different assay formats, including SPR, flow cytometry, ELISA, and handheld immunochromatographic assays [89, 90].

### 3.2 Transducers

The transducer is the most important part of a sensor because it is responsible for detecting the analyte. There are four main classifications of transducers, namely, electrochemical transducers, optical transducers, thermal sensors, and acoustic devices. Figure 7 lists these, along with some sensor examples of each type. Among these, ME material as the transducer is considered to be a novel type of AW device.

***3.2.1 Electrochemical Biosensors.*** Electrochemical biosensors are the most commonly used class of biosensors [91]. Their working principle depends on a biointeraction occurring where electrochemical species (e.g. electrons) are generated or consumed to produce an electrochemical signal that can be measured by an electrochemical detector. On the basis of the type of electrical signal, electrochemical sensors can be classified [91, 92] as either *potentiometric*, where the potential difference between an indicator and a reference electrode is measured; *amperometric*, where the current produced by an electrochemical oxidation or an electroactive species reduction under a constant potential is measured; or *conductometric/impedimetric*, where the alternating conductance between a pair of metal electrodes is measured [93, 94].

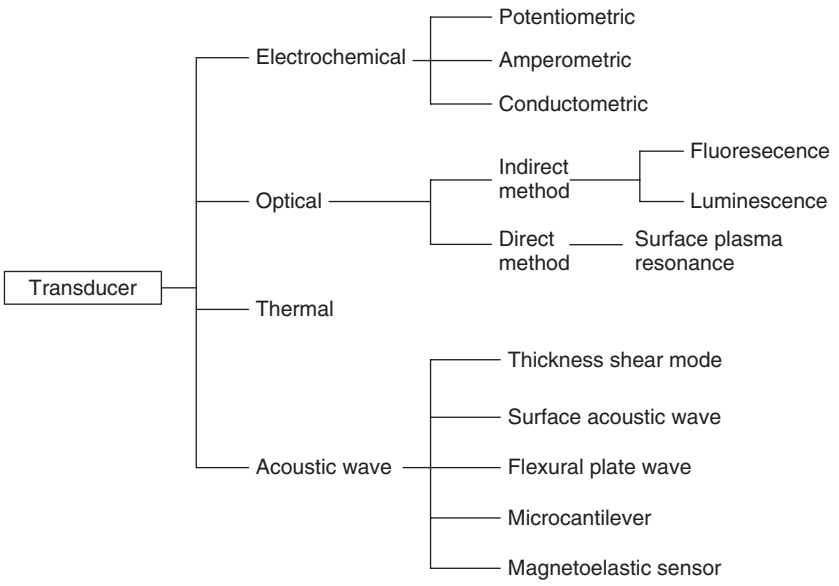



**FIGURE 7** Classification of sensor transducer types.

When the biological components interact, the conductance or capacitance of the medium will increase with decreasing impedance. Therefore, by measuring this change, a conductometric biosensor is able to detect the concentration and physiological state of foodborne pathogens [95].

In potentiometric biosensors, the transducer can be either an ion-selective electrode (ISE) or an immunoelectrode. For ISE, when the target ions bind to the selective membrane at the indicator electrode, a detectable difference in the potential between the indicator and reference electrode that is proportional to the logarithm of ion activity is realized [91]. For the immunoelectrode, enzymes or antibodies are usually immobilized on the electrode surface, and when target antigens in the sample interact with enzymes or antibodies, there is a detected potential shift. This method is useful in biosensing [92, 96].

An amperometric biosensor measures the current generated by a chemical/biological reaction rather than measuring the potential change. By using an enzyme to catalyze electrooxidation or electroreduction, almost all microorganisms can be sensed by amperometric biosensors. An amperometric system has a linear relationship with the analyte concentration, which makes it particularly convenient and suitable for bacterial detection [96] with species such as *Staphylococcus aureus* [97, 98], *Salmonella* [99], and *E. coli* O157:H7 [100, 101].

Some advantages of electrochemical sensors include their high sensitivity, small size, low cost, versatility, rapid measurement time, and capability of stand-alone operation [102]. However, amperometric sensors suffer from poor selectivity, which is controlled using the redox potential of the electroactive species in the sample solution. Table 5 lists the capability of different electrochemical sensors for pathogenic bacteria detection.

***3.2.2 Optical Biosensors.*** The working principle of optical biosensors is based on the modulation of optical properties that occurs when the biorecognition element interacts with the target analytes on the interface. These optical properties include UV absorption, bio- and chemiluminescence, reflectance, and fluorescence [119–123]. Applications of optical sensors include the measurement of pH, oxygen, carbon dioxide, and ions. Moreover, they are very attractive for label-free and quick detection of bacteria [63].

Depending on the type of interaction that produces the output signal, optical devices are classified as either *indirect* or *direct*. Methods that utilize the fluorescence or bioluminescence that results from antigen–probe interactions are defined as indirect methods, while those based on a direct change in the light properties due to the analyte–probe interactions are defined as direct methods. The total internal reflection of light incident at the interface, which depends on the refractive index, is an example of a direct optical method.

Some biospecies emit light with a lower wavelength when exposed to ultraviolet light, which is known as *fluorescence* [96]. Fluorescence biosensing is a type of optical biosensing method by frequency change, which includes direct sensing, indirect sensing, and fluorescence energy transfer. Fluorescence spectroscopy is widely used for analytical chemistry and offers a sensitive technique for low concentration analyte detection.

Some living microorganisms emit light when a biochemical reaction takes place, which is known as *bioluminescence*, and this is important for real-time monitoring. Luminescence biosensors have very high specificity, but suffer from poor sensitivity when the concentration of the target analyte becomes low [124]. Biosensors that monitor the color

**TABLE 5 Electrochemical Sensors for Pathogenic Bacteria Detection**

| Year | Detection Method | Foodborne Pathogen | Source | Detection Limit | Reference |
|---|---|---|---|---|---|
| 1996 | Amperometric biosensor | *Salmonella* | Culture | $5 \times 10^4$ cfu/ml | 103 |
| 1998 | Conductometry | *Escherichia coli* | Broiler chicken carcasses | 40 cfu/ml | 104 |
| 1999 | Amperometric measurement | *Listeria monocytogenes* | Buffer and milk | $9 \times 10^2$ cells/ml (for milk, signal decreased by 15%) | 36 |
| | Silicon chip-based LAPS | *Salmonella typhimurium* | Poultry | 119 cfu | 105 |
| 2000 | Amperometric biosensor | *Salmonella typhimurium* | Chicken carcass wash water | $5 \times 10^3$ cfu/ml | 106 |
| 2002 | Electrochemcial impedance spectroscopy | *E. coli* O157:H7 | Culture | $6 \times 10^3$ cells/ml | 107 |
| 2004 | Impedance immunosensor | *E. coli* O157:H7 | Culture | $10^6$ cfu/ml | 108 |
| 2005 | Dielectrophoretic impedance measurement | *E. coli* | Culture | $10^2$ cfu/ml | 109 |
| | Impedance microbiology-on-a-chip | *Listeria monocytogenes* | Culture | $10^4$ cfu/ml | 110 |
| | Impedance biosensor | *E. coli* O157:H7 | Culture | $10^4$ cfu/ml | 111 |
| | Amperometric immunoassay | *E. coli*, *L. monocytogenes*, *Cambylobacter jejuni* | Milk and chicken extract samples | 50, 10, 50 cells/ml | 112 |
| 2006 | Multifrequency reactance measurement | *E. coli* O157:H7 | Culture | $10^2$ cfu/ml | 113 |
| | Capacitometry | *Salmonella* | Culture | 10 cfu/ml | 108 |
| | Multichannel electrochemical immunosensor | *Salmonella enterica* | Meat samples | $2 \times 10^6$ cfu/ml | 114 |
| 2007 | Impedance biosensor | *E. coli* O157:H7 | Ground beef | $1.2 \times 10^3$ cells/ml | 115 |
| 2008 | Impedance biosensor | *E. coli* O157:H7 | Culture | 8 cfu/ml | 116 |
| | Amperometric biosensor | *E. coli* O157:H7 | Culture | 50 cells/ml | 117 |
| | Electrochemcial impedance spectroscopy | *Listeria monocytogenes* cell surface protein (Internalin B) | Culture | 4.1 pg/ml | 118 |

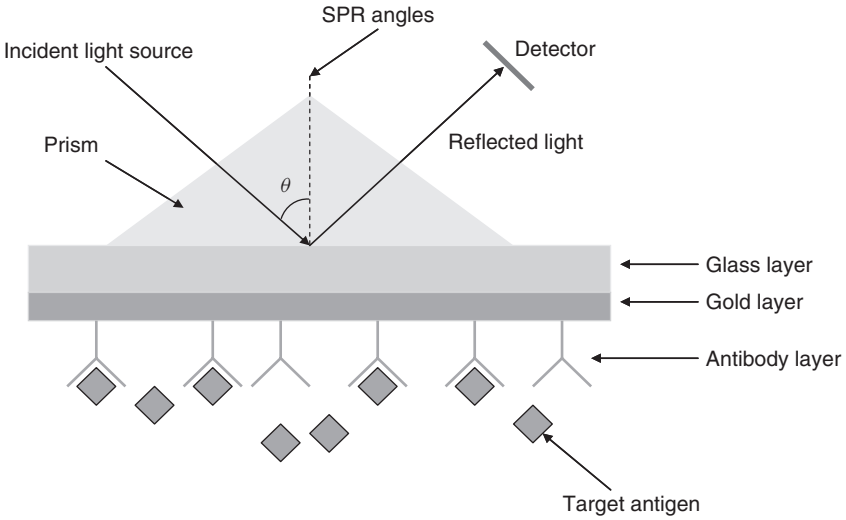



**FIGURE 8** Operational principles of an SPR biosensor.

change in response to toxins produced by microbial pathogens in the presence of test analytes are known as *colorimetric biosensors*. For example, a colorimetric whole cell bioassay [125] can be used for the detection of environmental pollutants.

Optical transducers incorporate optic fibers, which allow for greater flexibility and miniaturization. SPR, where the surface plasmons are excited by light, is an attractive optical biosensor transducer for many applications. The operational principles of an SPR biosensor are shown in Figure 8. It consists of two types of material with two different refractive indices: metal (gold) and glass. On the metal (gold) surface, incident light energy excites electrons to oscillate resonantly forming surface plasmons. SPR is excited along the metal surface at a specific incident angle ($\theta$), at which the intensity of the reflected light reduces to minimum. As this surface wave is on the boundary of the surface, the oscillation becomes sensitive to the environment of the metal surface. Any change on the metal surface such as an antibody–antigen interaction results in a change in the SPR angle ($\theta$). Therefore, SPR biosensors can be used to detect foodborne pathogens by measuring this shift [126]. The advantages of SPR biosensors are that they are simple, can be used in real time, and are label-free. However, they are relatively expensive, and it is hard to measure the target species when the concentration is very low. Also, the signal of SPR biosensors is vulnerable to interference from the environment [96, 127]. Table 6 lists the capabilities of optical biosensors used for pathogenic bacteria detection.

***3.2.3 Thermal Biosensors.*** Thermal transducers involve the production or absorption of heat. They measure the concentration of analytes based on the amount of heat adsorbed by a thermistor. Thermal sensors can be used either to measure the change in temperature of a substance directly during the course of a reaction or to measure the enthalpy of change in an enzymatic reaction.

***3.2.4 Acoustic Wave Sensors.*** Recently, a great deal of attention has been devoted to efforts to develop simple and inexpensive microsensors. Among these, the AW sensor is a common device that has been used for many chemical and biological applications.

**TABLE 6 Capabilities of Optical Biosensors Used for Pathogenic Bacteria Detection**

| Year | Detection Method | Foodborne Pathogen | Source | Detection Limit | Reference |
|---|---|---|---|---|---|
| 1997 | Interferometry | *S. typhimurium* | Culture | $5 \times 10^5$ cfu/ml | 128 |
| | Fiber-optic biosensor | *Salmonella* | Nutrient broth | $10^4$ cfu/ml | 129 |
| 1998 | SPR | *E. coli* O157:H7 | Culture | $5 \times 10^7$ cells/ml | 130 |
| 2000 | Micromachined resonant cantilever | *E. coli* O157:H7 | Culture | 16 cells | 131 |
| 2001 | Micromachined resonant cantilever | *E. coli* O157:H7 | Culture | Single cell | 132 |
| 2003 | SPR | *Legionella pneumophila* | Culture | $10^5$ cells/ml | 133 |
| | | *Salmonella* spp. | Culture | $1.7 \times 10^5$ cfu/ml | 134 |
| | Resonant mirror | *Listeria monocytogenes* | Culture | 208 μg/ml | 135 |
| 2004 | SPR | *S. typhimurium* | Culture | $10^2$ cfu/ml | 136 |
| | | *Listeria monocytogenes* | Culture | $1 \times 10^5$ cells/ml | 77 |
| 2004 | Fiber-optic biosensor | *Listeria monocytogenes* | Enriched hot dogs and bologna | 10–1000 cfu/g | 137 |
| 2005 | SPR | *E. coli* O157:H7 | Culture | $10^4 - 10^6$ cfu/ml | 138 |
| 2005 | Ellipsometry | *S. typhimurium* | Culture | $10^3$ cfu/ml | 139 |
| 2006 | SPR | *S. typhimurium* | Milk | $1.25 \times 10^5$ cells/ml | 140 |
| | | *S. enterica* serovar enteritidis | Skim milk | 23 cfu/ml<br>25 cfu/ml | 141 |

(*continued overleaf*)

**TABLE 6 (*Continued*)**

| Year | Detection Method | Foodborne Pathogen | Source | Detection Limit | Reference |
|---|---|---|---|---|---|
| | | *E. coli* | | | |
| | | *Listeria monocytogenes* | Culture | $10^7$ cells/ml | 142 |
| 2006 | Multichannel SPR sensor (simultaneous detection) | *E. coli* O157:H7 *S. enterica* ssp. *choleraesuis* serotype typhimurium *Listeria monocytogenes* *Campylobacter jejuni* | Culture | $3.4 \times 10^3 - 1.2 \times 10^5$ cfu/ml | 143 |
| 2006 | Fiber-optic biosensor | *E. coli* O157:H7 | Ground beef | 1 cfu/ml | 144 |
| | | *Listeria monocytogenes* | Frankfurter samples | $5 \times 10^5$ cfu/ml | 145 |
| 2006 | FRET-based optical fiber biosensor | *S. typhimurium* | Ground pork | $10^5$ cfu/g | 146 |
| 2007 | SPR | *E. coli* O157:H7 | Milk, apple juice, and ground beef | $10^2 - 10^3$ cfu/ml | 147 |
| | | *Campylobacter jejuni* | Processed broiler carcass | $10^3$ cfu/ml | 148 |
| 2007 | The NRL array biosensor | *S. typhimurium* | Culture | $8 \times 10^4$ cfu/ml | 149 |
| | | *E. coli* O157:H7 | | $5 \times 10^3$ cfu/ml | |
| | | *Listeria monocytogenes* | | $10^4$ cfu/ml | |
| | | *Campylobacter jejuni* | | $10^3$ cfu/ml | |
| 2008 | Microring resonator | *Escherichia coli* O157:H7 | Culture | $10^5$ cfu/ml | 150 |

Examples include sensors to monitor pressure, vapor, humidity, temperature, and film characterization. AW devices are sensitive to small changes in many different physical parameters [151]. They have been commercially available for more than 60 years because they offer real-time and fast detection, and are sensitive, simple to use, intrinsically reliable, and cost-effective [151]. Some can also be used wirelessly.

*3.2.4.1 Operating principles and performance criteria.* AW devices typically generate a mechanical or AW that propagates either through the bulk material or on its surface. The velocity and/or amplitude of this wave will change if the propagation path or its characteristics change in any way. Consequently, any variation that is observed in the properties of the AW, that is, its velocity and/or amplitude, can be linked to corresponding changes in the material's physical characteristics, thus allowing them to be monitored in real time by the AW sensor.

AW sensors usually use a piezoelectric material as the platform. When an oscillating electrical field is applied to the piezoelectric platform, a mechanical wave is generated. This phenomenon is known as the *converse piezoelectric effect*. The "direct piezoelectric effect" is the reciprocal of this and refers to the application of strain to the material, which results in the creation of an electrical change. The direct piezoelectric effect was discovered by brothers Pierre and Paul-Jacques Curie in 1880 and is defined as piezoelectricity [152]. Most AW piezoelectric sensors utilize the principle of converse piezoelectricity. When the AW produced propagates through or on the surface of the substrate, the velocity or amplitude of the wave will change if the characteristics of the propagation path change. The frequency or phase characteristic of the sensor is measured to monitor such changes, which can then be correlated to the corresponding physical quantity.

An AW sensor can also be used as a mass sensor; when an AW device is used as a resonator, the resonance frequency of the AW device will change when there is a mass load on the device surface. On the basis of this principle, different biosensors can be developed by immobilizing a biomolecular recognition layer (i.e. antibody, bacteriophage) on the AW sensor surface. When the target pathogen and the biomolecular recognition layer undergo a chemical reaction or sorptive interaction (i.e. adsorption/absorption) on the sensor's surface, the surface mass changes. This mass change can be detected by measuring the resulting shift in the characteristic resonance frequency of the sensor. Therefore, the majority of analytical applications of AW sensors are based on changes in mass loading.

*3.2.4.2 Different types of AW devices.* An AW can propagate in an elastic medium, causing the device to vibrate. The direction of vibration can be either parallel or perpendicular to the direction of propagation. The types of elastic waves that may propagate in a solid are shown in Figure 9 [151], and these depend on the properties and the boundary conditions of the solid [153]. There are four AW devices that are most commonly utilized and investigated for sensing applications, namely, the thickness shear mode (TSM) resonator, the surface acoustic wave (SAW) device, the flexural plate wave (FPW) device [151], and the microcantilever (MC) [154, 155]. As depicted in Figure 9a and b, bulk waves exist in a medium without any boundaries, such as a TSM resonator. When a single plane boundary exists, the wave will propagate along that boundary, for example, in a SAW device (Figure 9c). If two boundaries exist, the wave will propagate within the thin plate, as in an FPW device (Figure 9d).

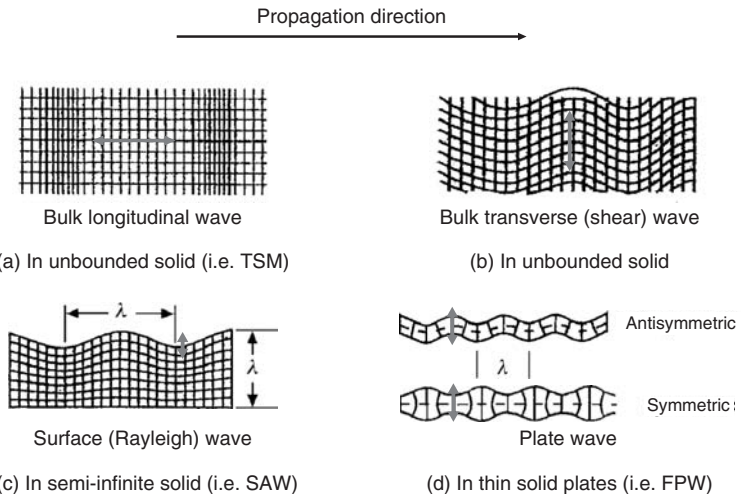



**FIGURE 9** Types of elastic wave propagation: (a) and (b) in an unbounded solid, (c) in a semi-infinite solid with a single boundary, and (d) in a thin solid plate with two boundaries. Vertical and horizontal displacements are exaggerated for clarity. The red (nondimensional) arrow represents the direction of vibration. (See online version for color.)

**Quartz Crystal Microbalances (QCM).** The familiar QCM, also commonly referred to as a *TSM resonator*, is one of the most widely used AW sensor platform in both research studies and commercial applications for biological threat detection. It typically consists of a thin AT-cut quartz disk with circular electrodes patterned on both sides [151]. When applying a voltage between these two electrodes, the crystal will undergo shear deformation due to the piezoelectric effect and will be electrically excited in a number of resonant TSMs, allowing the mechanical resonance frequencies to be detected. When there is a uniformly distributed thin film deposited on the crystal surface, the added mass of the thin film results in a change in TSM resonant frequency, which can be expressed by the Sauerbrey Equation [156]:

$$\Delta f = -\frac{2 f_0^2 \Delta m}{A\sqrt{\mu_{\mathrm{q}}\rho_{\mathrm{q}}}} \tag{1}$$

where $\Delta f$ is the frequency shift, $f_0$ is the fundamental mode of the crystal, $\Delta m$ is the mass change per unit area (grams per square centimeter), $A$ is the active area on the surface, $\rho_q$ is the density of quartz, and $\mu_q$ is the shear modulus of quartz. Mass sensitivity can be derived from the equation:

$$S_{\mathrm{m}} = -\frac{f_0}{(t\rho)_{\mathrm{quartz}}} \tag{2}$$

where $t$ and $\rho$ is the thickness and density of the thin film layer on the crystal. A TSM resonator can be operated in a liquid in order to determine its properties (i.e. viscosity, density [157, 158]) by measuring the mass loading on the crystal surface from the liquid environment. TSM resonators have also been used for microbial contamination detection (i.e. *S. typhimurium*, *B. anthracis* spores) by immobilizing biological active elements on the surface (i.e. antibody, phage) [159–162].

**SAW Devices.** SAW devices are usually composed of ST-cut piezoelectric crystals with two patterned gold/titanium-interdigitated transducers (IDTs) (emitter and receiver) deposited on the same side of crystal surface. This SAW, also known as a *Rayleigh wave* [163], is utilized for sensor applications because the propagation of waves is confined to the surface, making the AWs extremely sensitive to surface perturbations and allowing them to be detected by lithographically patterned interdigital surface electrodes [164]. SAW sensors exhibit the highest sensitivity of the acoustic sensors reviewed [162], because the AW confines all the acoustic energy to the zone within one wavelength of the surface. When applying an alternating voltage on one of the electrodes, an AW will be produced that propagates along the surface until it reaches the other electrode [151]. However, when the SAW sensor is placed in a liquid medium, the waves will be strongly damped, because they are surface-normal waves, making SAW sensors unsuitable for liquid sensing. One of the most common applications for SAW sensors is to detect the interaction, in terms of the fundamental resonance frequency change, that results from changes in the areal/mass density on the sensor surface.

**FPW Devices.** In an FPW device, the AW is excited in a membrane that is relatively thin compared to the acoustic wavelength. An FPW sensor is usually fabricated by a micromachining process and uses silicon nitride, silicon dioxide, oxynitride, aluminum nitride, or diamond as the membrane layer. This membrane is deposited onto a silicon substrate for ease of handling, and then the substrate is etched away. After depositing a conducting layer, a layer of piezoelectric zinc oxide will be sputtered on, followed by sputtering of a second conducting layer. Two interdigitated conducting electrodes are formed in the conducting layer, one of which is used as a wave generator (output) and the other as the wave receiver (input). The piezoelectric film is deformed and excited by the interdigitated conducting electrodes in order to generate and detect AWs. When a wave propagates, the membrane moves both perpendicularly and parallel to its surface such that the shape of the entire membrane is like a flag waving in the wind [151, 165]. FPW has high sensitivity compared to other AW devices. As the operating frequencies are of the order of few megahertz or even lower, this makes it relatively easy to design the electronics for the operation. Also, the wave propagates at low speeds in the plate; therefore, it is possible to use FPW sensors in liquids. However, the fabrication of FPW devices is difficult as it is hard to make a low stress membrane layer with a thickness of few microns, and the resulting membrane is fragile. Because of this, FPW sensors have not made much progress in terms of miniaturization.

**Microcantilevers.** Micromachined cantilevers were first used as force probes in atomic force microscopy. Owing to their extremely high sensitivity to a variety of environmental factors, including acoustic noise, temperature, ambient pressure, and humidity [166], researchers at Oak Ridge National Laboratory and IBM Zurich investigated converting them into a new sensor platform [167, 168] and found that this standard cantilever provided a substantial improvement (i.e. sensitivity) over more traditional approaches (i.e. QCM, SAW). A MC also acts as a mass sensitive device, producing a frequency shift when there is a mass loading on the device [169–171]. In the last decade, with the development of microelectromechanical systems (MEMSs) that integrate electronics and micromechanical structure on chips, MCs have become one of the simplest MEMS-based devices. A large number of papers have reported on the potential of MCs for physical, chemical, and biological sensing [172–176]. Moreover, nanocantilevers have been

successfully fabricated in the last few years, significantly increasing the sensitivity for sensing applications and allowing the detection of even smaller masses, ranging from several molecules to a single bacteria cell (i.e. *E. coli* [177]) or spore [178, 179]. Recently, it was reported that a mass sensitivity of as low as a few femtograms can be achieved using nanocantilevers [180]. Sensors using cantilevers as a platform have a high sensitivity and a good safety record, as well as being cheap, simple, fast, low power, and having a low analyte requirement for testing. These advantages make them very promising for the next generation of miniaturized and highly sensitive sensors [181].

A fundamental cantilever is constructed from a long and thin microbeam with one end fixed by a support. The readout schemes for a cantilever can be broadly classified into two types: optical and electrical. Depending upon the parameters measured (i.e. cantilever tip position, spatial orientation, intrinsic stress, or radius of curvature) [154], cantilever operation can also be divided into static and dynamic modes. The static bending mode is used to detect cantilever deflection, which can be caused either by external forces added to the cantilever (i.e. adsorption of molecules) or intrinsic stresses produced in the cantilever (i.e. thermal expansion, physicochemical changes). In the dynamic mode, the MC operates as a mechanical oscillator whose resonance frequency changes due to three main mechanisms: (i) the mass loaded on the beam; (ii) the viscosity of the medium; and (iii) the environmentally induced elasticity changes in the MC material [154, 182]. When the target binds to the cantilever beam, the frequency shifts from $f_0$ to $f_1$ due to the additional suspended mass ($\Delta m$), and the relationship can be expressed as [154]

$$\frac{1}{f_1^2} - \frac{1}{f_0^2} = \frac{\Delta m}{\left(4\pi^2 K\right)} \tag{3}$$

Here, $K$ is the spring constant of the cantilever. In order to obtain an appreciable mass sensitivity, high frequencies are required.

Dynamic MCs can also be divided into three types: single beam MCs (i.e. silicon-based MCs), composite-beam MCs (i.e. piezoelectric/piezoresistance MCs), and ME MCs.

Silicon-based MCs are driven by mechanical force and the deflection is detected by optical methods, which includes optical beam deflection [183] and optical interferometry [184, 185]. A typical optical method applies a position-sensitive photodetector (PSD) and a laser beam of very low power. The laser beam falls on the cantilever beam surface and the reflected beam is then captured by the PSD. If an additional mass loaded on the beam has caused the deflection of the cantilever, the reflected beam falls on a different part of the PSD and the magnitude of this deflection can be calculated by appropriate electronics. Optical methods offer significant advantages of miniaturization, batch fabrication, and integration of signal-processing circuitry with a relatively high mechanical quality factor (Q), which greatly increases the sensitivity of the device. However, a high Q value is likely to adversely affect the stability of device by acting to promote mechanical coupling, resulting in a change in the vibration mode. The system is also complex, expensive, and bulky, and requires a sophisticated data acquisition system and extra driving equipment to make it vibrate. Optical methods are of particular importance for many applications, because of the dispersion of the laser beam in a liquid, although they are limited for in-liquid applications [183].

Compared with silicon-based cantilevers, piezoelectric cantilevers are optimized by using electrical means, which overcomes the need for complex optical detection equipment. It can be used electrically for both actuation and sensing and is able to integrate

the driving and characterizing circuits in the chip with MCs. By applying an AC voltage to the driving electrode, the cantilever vibrates due to the converse piezoelectric effect. At resonance, these vibrations produce piezoelectric voltages that can be detected by the direct piezoelectric effect at the sensing electrode. An impedance analyzer can also be used to measure the resonance frequencies and characterize the sensor using the impedance spectrum (impedance vs. frequency). As only one electrode is needed, the measurements can all be obtained conveniently using an impedance analyzer.

The two types of platforms employed by piezoelectric-based MCs are unimorph and bimorph. Unimorph MCs are composed of one piezoelectric layer bound to a substrate layer (stiff metal). There are two types of bimorph connections, parallel and series, and these consist of two piezoelectric layers with different pole directions bonded together. When mass is added to the cantilever, the oscillation of the cantilever is damped. Thus, a piezoelectric actuator can be used as a viscosity-meter or as a microbalance to detect mass change. No external detection devices or tedious alignment are required, and they are also capable of enclosing an integrated electromechanical system. Piezoelectric cantilevers not only act as mass detectors, but also function well in liquids by monitoring peak broadening and the resonance frequency shift. As MCs are highly mass sensitive, their length, width, and resonance mode all have an effect on an individual cantilever. Mutharasan and coworkers at Drexel University successfully utilized piezoelectric-excited millimeter-sized cantilever (PEMC) sensors that consisted of a piezoelectric and a borosilicate glass layer immobilized with different biorecognition elements to develop a sensitive, reliable, and near real-time method for the detection of *Cryptosporidium parvum* oocyst [186], airborne *B. anthracis* spores in conjunction with a commercial air sampler (at 5 spores/l) [187], *Staphylococcus aureus* enterotoxin B (SEB, at 12.5–50 pg/ml) [188], and *E. coli* O157:H7 in ground beef samples (50–100 cells/ml) [189].

**Magnetoelastic (ME) Sensors.** ME materials are generally amorphous, soft ferromagnetic materials. Nickel, laminated metallic glass alloys, and rare-earth iron compounds are common ME materials. This class of materials is a subset of magnetostrictive materials, which undergo a change in dimensions when exposed to a magnetic field. ME materials can be made to resonate in a time-varying ("AC") magnetic field at a specific frequency that is dependent on their geometry and mass. For rectangular sheet sensor platforms, varying the magnetic field can be used to cause oscillations mainly along the length direction. Table 7 summarizes the AW sensors used for foodborne pathogen detection.

## 4 POTENTIAL BIOSENSORS FOR FOOD SAFETY APPLICATIONS

### 4.1 Modified Filamentous Phage fd as a Biorecognition Element

***4.1.1 Landscape Phages.*** Phages play an important role in molecular biology. For example, they are commonly used as a vector to infect the standard recombinant DNA host (*E. coli*) in recombinant DNA research. The method of using a phage as a vector to connect proteins to display genetic information is called *phage display*. Tens of billions of heterogeneous phage clones can be collected together to create a "phage display library." Each clone displays multiple copies of a specified peptide on the virion surface [200–202], and a phage display library can be used to select high specificity phages to an immobilized molecule and then multiply these phage clones for further study.

**TABLE 7 Acoustic Wave Sensors for Foodborne Pathogen Detection**

| Year | Detection Method | Foodborne Pathogen | Source | Detection Limit | Reference |
|---|---|---|---|---|---|
| 1998 | FPW sensor | *E. coli* | Culture | $3.0 \times 10^5 - 6.2 \times 10^7$ cells/ml | 190 |
| 2000 | QCM | *S. typhimurium* | Culture | $3.2 \times 10^6$ cfu/ml | 191 |
| | Love wave immunosensor | *Legionella* and *Escherichia coli* | Culture | $10^5 - 10^6$ cells/ml | 192 |
| 2001 | QCM | *Listeria monocytogenes* | Culture | $1 \times 10^7$ cells/ml | 193 |
| 2002 | QCM | *E. coli* | Drinking water, milk, rice, dumplings, and others | $1.7 \times 10^5 - 8.7 \times 10^7$ cfu/ml | 194 |
| | | | Culture | $10^4$ cells/ml | 195 |
| 2004 | QCM | *E. coli* O157:H7 | Culture | $10^3$ cfu/ml | 196 |
| 2005 | QCM combined with resistance measurement | *S. typhimurium* | Chicken meat samples | $10^5 - 10^8$ cells/ml for frequency measurement<br>$10^2$ cells/ml for resistance measurement | 197 |
| 2007 | Piezoelectric cantilever | *E. coli* O157:H7 | Ground beef | 50–100 cells/ml | 189 |
| | Love wave imuunosensor | *E. coli* | Culture | $10^6$ bacteria/ml | 198 |
| 2006 | SH SAW LGS biosensor | *E. coli* O157:H7 | Culture | $10^6$ cells/ml | 199 |

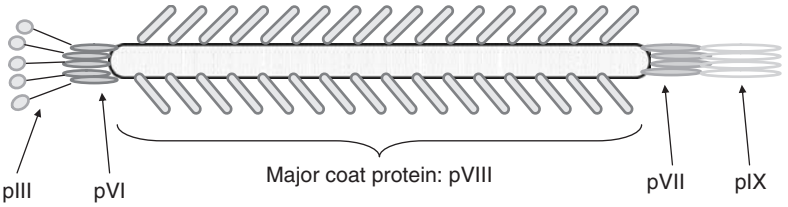



**FIGURE 10** Schematic showing filamentous phage structure. pIII, pVI, pVIII, pVII, pIX represent phage proteins. Exogenous peptides are usually displayed on protein pIII and pVIII.

The filamentous phage Ff class, which includes M13, f1, and fd phages, has been subjected to extensive research for phage display applications [202, 203]. Filamentous phage fd is a phage shaped like a rod filament, as shown in Figure 10. Each phage filament is generally about 7 nm wide and 800–900 nm long. The outer coat is a tubelike structure composed of a major protein coat pVIII, which has an ssDNA buried inside. At the tip ends of the phage particle, there are several copies of four minor proteins, pIII, pVI, pVII, and pIX [204, 205]. The major protein coat occupies 98% of the phage's mass and is present in 2700 or more copies per phage.

Studies have shown that the common filamentous phages can be modified by using phage filaments as the framework and then fusing eight foreign random amino acids to the N-terminus of every copy of the major protein coat pVIII [200, 202, 206]. The replacement of three or four amino acids at the N-terminus of the protein pVIII with 12–19 foreign amino acids in a filamentous phage will not disturb the general architecture of the virions [207]. As the array of thousands of copies of these guest peptides appear in a repeating pattern, a dramatic change in the phage surface architecture occurs, resulting in the number of major protein coat subunits increasing to 4000. The major protein coat now comprises up to 50% of the phage surface [200, 206]. This modified phage is called a *landscape phage* and a mixture of a large number of such landscape phages is named a *landscape phage library*, encompassing billions of phage clones with different surface structures and biophysical properties [208].

Landscape phages are now being investigated as a possible alternative to antibodies for detection probes, as they are more stable, reproducible, and inexpensive to produce [159, 200]. These phage bioprobes have begun to be used as a biological recognition molecule for AW devices such as SPR [209], TSM quartz sensors [159] and ME sensors [210–212] for the real-time detection of a range of pathogens or the adsorption of biochemical macromolecules [213]. Landscape phages are extraordinarily robust in harsh environments and can be heated up to 80°C [202]. They are also resistant to organic solvents (e.g. acetonitrile), acid, alkali, and other chemicals [214]. Purified phages can be stored indefinitely at moderate temperatures without loss of infectivity and probe-binding activity. More importantly, phages have a high affinity to target antigens. This is because phages have an extremely high surface density (300–400 $m^2/g$) and up to 50% of the surface can be subtended by peptides to form the "active receptors" sites. This high density of binding sites exceeds that of the best-known absorbents and catalysts. The thousands of phage filaments also provide far more opportunities for binding.

***4.1.2 Phage Immobilization.*** To form phage-based biosensors for the detection of foodborne pathogens, a specific phage needs to be selected and immobilized onto the sensor platform surface to capture/react with the target pathogens. The immobilization of phage

should meet several requirements: (i) desorption of phage from the sensor surface should not occur in the analyte solution (such as aqueous buffers or food products containing target pathogens) during the detection process; (ii) the immobilized phage should not lose its binding affinity and specificity toward the target pathogen in the daily environment; and (iii) ideally, the immobilized phage should be strongly attached to the sensor platform surface with high coverage and uniform distribution.

Several phage immobilization techniques have been explored by Petrenko, Weiss, Wan, Huang, Lakshmanan et al. [159, 210–212, 215–219]. These techniques can be classified into two distinct methodologies: (i) phage was indirectly immobilized on the sensor surface by attaching on an anchor layer, which had been coated on the sensor platform surface; and (ii) phage was directly immobilized on the sensor surface by physical adsorption.

Langmuir–Blodgett (LB)-coated monolayers have been used to immobilize phages on sensor platforms. To attach phages, Petrenko et al. [215] deposited biotin-modified phospholipid monolayers on the gold surface of the sensor using the LB method and then treated the monolayer with streptavidin. The biotinlyated phage was then immobilized on the sensor through biotin/atreptavidin coupling. By using this LB-coated monolayer, phages selected for affinity to $\beta$-galactosidase were immobilized on QCM sensors. Experiments showed that phages immobilized on QCM sensors using this method exhibit a better affinity to $\beta$-galactosidase than the same phage used in ELISA [215].

Vodyanoy and Petrenko [159, 220] showed phages can be simply immobilized on the gold surface of the sensor platform by physical adsorption. In this method, a phage was immobilized on the clean gold surface of the sensor by incubating the sensor in the phage suspensions in TBS solution (25 m*M* Tris, 3 m*M* KCl, and 140 m*M* NaCl at a pH of 7.4) for about 1 h at room temperature. On the basis of physical adsorption, this immobilization technique avoids complex surface modification procedures, which considerably simplify the immobilization process and reduce the immobilization time. Using physical adsorption, the phage was successfully immobilized on different sensor platforms, such as SPR [209], QCM [159, 220], and ME sensor platforms [210–212, 217, 221, 222] to detect different pathogens. For example, Olsen et al. used QCM coated with phages by physisorption to detect *S. typhimurium*, and a detection limit of 100 cell/ml was achieved [159]. Using this method, Chin's group immobilized the JRB7 phage and the E2 phage on ME biosensors and successfully used them to detect *B. anthracis* spores [210, 217, 222] and *S. typhimurium* [211, 212, 217].

### 4.2 Magnetoelastic (ME) Material as the Sensor Platform

Recently, the use of ME materials as transducer platforms for the remote monitoring of foodborne pathogens [210–212, 217, 222] and other applications in chemical detection and environmental monitoring [223–228] have attracted considerable interest.

ME materials have an interesting and potentially useful property in that the material's physical dimensions change in response to variations in its magnetic environment: this is the direct ME effect, known as *magnetostriction*. Unlike piezoelectric materials, which need external electrical connections, ME materials can be monitored wirelessly as they are activated remotely by a magnetic field. When a time-varying AC external magnetic field is used to resonate the ME platform, the resulting magnetostriction causes the ME platform to exhibit a pronounced ME resonance, and hence change the magnetic flux that can be remotely detected using a pickup coil. As no physical connection is needed

between the ME platform and the device, a biosensor based on this ME platform can be conveniently used in difficult environments such as sealed containers and packages.

The precise mechanical resonance frequency of an ME sensor is based on its physical characteristics, and it can be made to vibrate at this frequency by applying an oscillating magnetic field to cause an elastic length change. For a thin, planar, ribbon shaped sensor of length $L$, vibrating in its basal plane, the fundamental resonant frequency of longitudinal oscillations is given by [229, 230]:

$$f = \sqrt{\frac{E}{\rho(1-\sigma^2)}}\frac{1}{2L} \tag{4}$$

where $E$ is Young's modulus of elasticity, $\rho$ is the density of the sensor material, $\sigma$ is the Poisson's ratio, and $L$ is the length of the sensor.

Any non-ME mass added to the sensor surface reduces the mechanical oscillations causing the resonance frequencies to shift to a lower value. If the mass increase ($\Delta m$) is small compared to the mass of the sensor ($M$) and it is uniformly applied on the sensor surface, the shift in resonant frequency ($\Delta f$) is given by:

$$\Delta f = -\frac{f_0 \Delta m}{2M} \quad (\Delta m << M) \tag{5}$$

where $f_0$ is the initial resonance frequency, $M$ is the initial mass, and $\Delta m$ is the added mass. The negative sign means the resonance frequency of the ME resonator decreases with an increase of the mass load. Thus, the mass load on the ME resonator can be very easily obtained by simply measuring the shift in the resonance frequency.

The mass sensitivity of the ME sensor can be expressed as

$$S_{\mathrm{m}} = \frac{\Delta f}{\Delta m} = -\frac{f_0}{2M} = -\frac{1}{2M}\frac{1}{2L}\sqrt{\frac{E}{\rho\left(1-\sigma^2\right)}} = -\frac{1}{4l^2 wt\rho}\sqrt{\frac{E}{\rho\left(1-\sigma^2\right)}} \tag{6}$$

where $S_m$ is the mass sensitivity of ME sensor, and $w$ and $t$ are the width and thickness of sensor respectively. From this equation, it is clear that when a small mass is loaded on the sensor, the mass sensitivity depends primarily on the length of the sensor and is inversely proportional to $l^2$.

### 4.3 Phage-Based Magnetoelastic Biosensors

In order to detect the presence of selective and specific pathogens (which may be spores, bacteria, or viruses), biomolecular recognition elements (phages, antibodies, or enzymes) will be coated onto the surface of the ME platform to form an ME biosensor. A time-varying (AC) magnetic field, supplied by a network analyzer, is used to resonate the ME biosensors. Before loading the pathogens, the frequency of the ME biosensor is recorded as $f_0$. Upon coming into contact with the biosensor, the target pathogens are captured by the specific recognition elements immobilized onto the biosensor's surface, resulting in an increase in the mass on the ME biosensor. This added mass will cause a corresponding decrease in the biosensor's resonance frequency ($f_{\mathrm{mass}}$). These measurements are performed remotely and wirelessly.

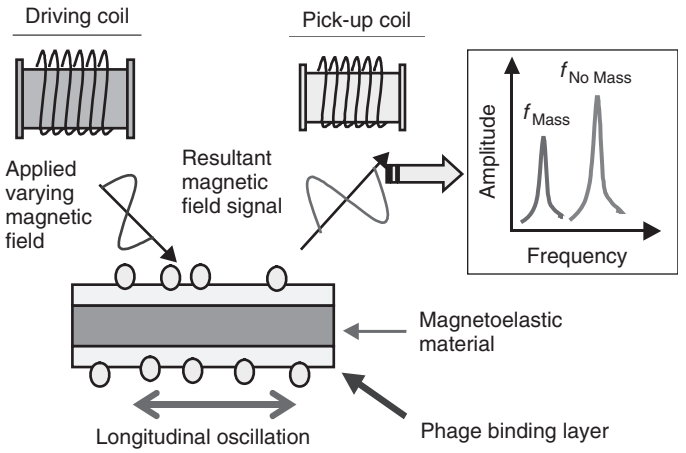



**FIGURE 11** Wireless ME biosensor operation and the basic principle for detecting bacterial cells and spores. The fundamental resonant frequency of the biosensor $f_{\text{No Mass}}$ without target binding decreases to $f_{\text{Mass}}$ due to target binding.

Figure 11 illustrates the wireless nature of the individual ME biosensor and the basic principle for detecting bound mass (target pathogens).

The frequency spectrum of the biosensor can be obtained by sweeping an AC magnetic interrogation field over a predetermined frequency range while monitoring the response of the biosensor using a pickup coil. At the resonance frequency of the biosensor, the conversion of the magnetic energy into elastic energy is maximal and the biosensor undergoes a maximal oscillation.

***4.3.1 ME Sensor Platform.*** Compared to other AW sensor platforms, the simple strip-shaped configuration makes the ME platform easier to be fabricated. The fabrication methods can be divided into three types depending on the desired size of the sensor platform.

Generally, sensor platforms with lengths longer than 500 μm can be fabricated by simply mechanically polishing and dicing commercially available amorphous alloy ribbons. Figure 12 shows the procedure of fabricating ME sensor platforms using the polishing/dicing technique [210–212, 216, 217]. In order to fabricate the ME sensor platform, it was cut off the roll and hand polished to 15 μm using grit paper of 1000–2000 μm. This polishing provided a smoother surface for biorecognition element immobilization and also a thinner platform, decreasing the initial mass of the sensor in order to increase its sensitivity. After polishing, the ME alloy was sandwiched between two sheets of polymer film and cut by a microdicing saw to obtain sensor platforms with the desired sizes. All the platforms were fabricated with a length ($L$) to width ($w$) ratio of 5:1. In order to remove any residual film after dicing, the ME sensor platforms were ultrasonically cleaned in acetone with micro-90 solution for 1 h, in ethanol for 0.5 h, and then dried in air. After dicing, the cleaned ME sensor platforms were annealed to relieve residual internal stress and correct defects due to the mechanical polishing and dicing operations. Annealing was carried out at 220°C for 2 h in a vacuum oven (Fisher Isotemp Model 281A, Vacuum Oven) under a vacuum of at least $10^{-3}$ Torr [231]. Afterwards, the sensor platforms were cooled to room temperature in the oven while still under vacuum. Then,

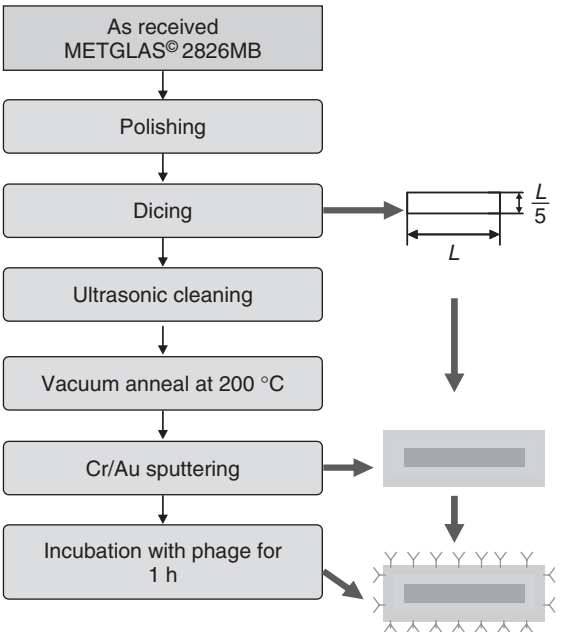



**FIGURE 12** Steps in the fabrication of a magnetoelastic resonator using the polishing/dicing technique. This method is limited to fabrication of resonators greater than 500 μm in size.

thin films of chromium followed by gold were deposited onto both sides of the ME platforms using a Denton™ Vacuum Discovery-18 sputtering system (Moorestown, New Jersey) with two cathodes (RF and DC). All deposition of metals was conducted in a vacuum chamber evacuated to a background pressure of no more than $5 \times 10^{-6}$ Torr. Argon was used as the sputtering gas to bring the deposition pressure up to between 5 and 6 mTorr. On each side of the ME platforms, Cr was deposited first after which the Au layer was deposited without breaking the vacuum. The fabricated platforms were then stored in a desiccator until use. Prior to immobilization of the biorecognition element, the sensor platforms were washed with hexane and air dried.

When the length of the sensor platform is smaller than 500 μm, it is very difficult to fabricate using this mechanical polishing and dicing technique. Therefore, a method employing microelectronic fabrication techniques was developed by Johnson et al. [232, 233] and successfully fabricated the platform with a size down to $50 \times 6 \times 3$μm. Figure 13 shows the microfabrication process. A wafer was patterned with rectangular shapes of the desired size using a photolithography process. Photoresist SPR-220 and developer 453 from Rohm & Haas Electronic Materials LLC (Philadelphia, Pennsylvania) were used to form the pattern. Amorphous iron–boron thick films were magnetron sputtered onto silicon wafers using a Discovery-18 sputter system from Denton Vacuum USA (Moorestown, New Jersey) at a base pressure $7 \times 10^{-7}$ Torr. Thin gold films that serve as a corrosion protection layer for the resonator and form a biological compatible surface were deposited onto the wafer before and after the Fe–B film deposition. A lift-off process employing a wash with solvent was used to remove the resonators from the wafer. The sensor platforms were then cleaned with acetone. More details of the fabrication process are described in Ref. 232.

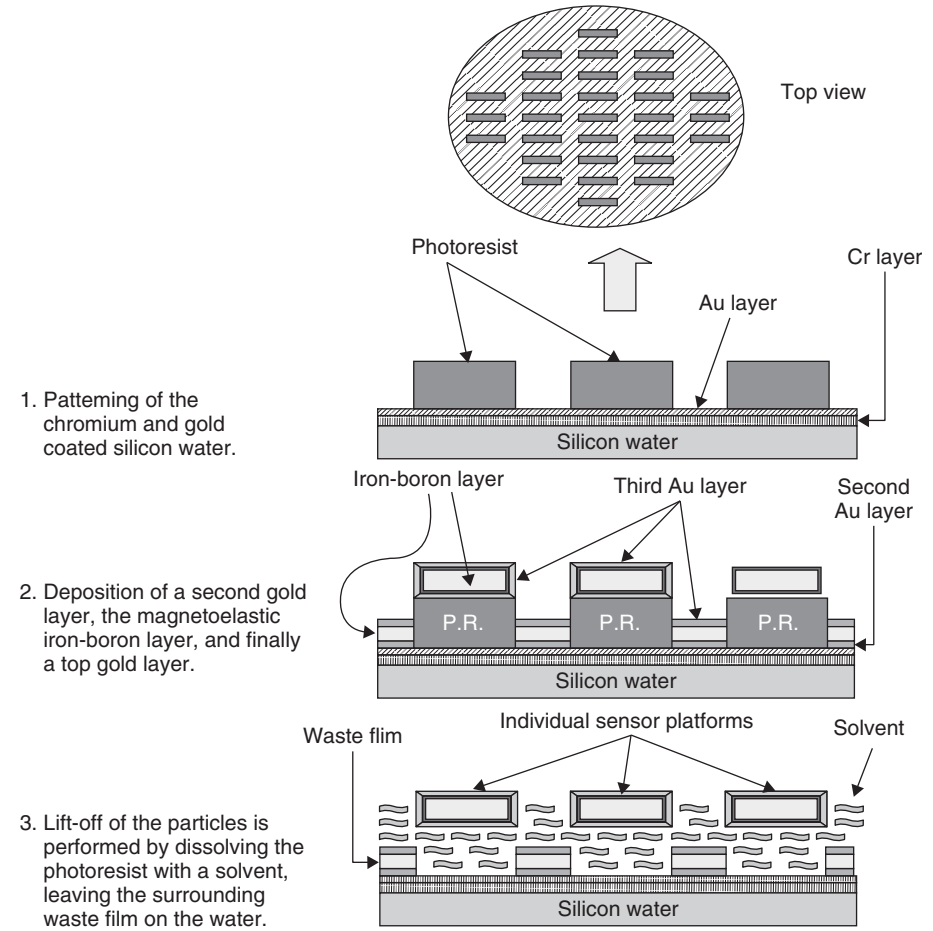



**FIGURE 13** Diagram of the microelectronics fabrication process used to make micron-scale magnetoelastic resonators.

To obtain a sensor platform with nanoscale dimensions, Li et al. fabricated ME nanobars using template-based electrochemical deposition [234, 235]. As seen previously in Section 4.2 the sensitivity of the sensor will increase as its size and characteristic mass is decreased. In order to directly detect the presence of a small amount of pathogenic bacteria (e.g. of the order of 100 or less), the sensor must theoretically be limited to a maximum dimension (length) in the range of 100 μm.

***4.3.2 Fabrication of Phage-Based ME Biosensors.*** So far in the investigation of phage-based ME biosensors, two kinds of affinity-selected phages have been used as bioprobes: the JRB7 phage against *B. anthracis* spores and the E2 phage against *S. typhimurium*. Both the JRB7 phage and the E2 phage were selected from the f8/8 landscape phage library by Dr. Valery Petrenko of Auburn University. The selection procedures have been described in detail in a previous article [236, 237]. To form phage-based ME biosensors, the phage was immobilized on the gold coated surface

of the resonators (sensor platforms) by physical adsorption. In order to prevent nonspecific binding of target pathogens on the gold surface, the phage-immobilized biosensors were coated with 1 mg/ml BSA. Detailed phage immobilization procedures for these biosensors are available in several articles [210–212, 216, 217, 221, 231].

### 4.4 Phage-Based ME Biosensors for Foodborne Pathogen Detection

Wan, Lakshmanan et al. immobilized the JRB7 phage [210, 216] and the E2 phage [211, 212] onto ME platforms to form biosensors to detect *B. anthracis* spores and *S. typhimurium* cells, respectively. The performance of the biosensors, including sensitivity, detection limit, specificity, and longevity (thermal stability), was systemically characterized. Also, a phage-based ME biosensor has been demonstrated to detect *S. typhimurium* cells in fat-free milk or apple juice [212]. Huang et al. developed a multisensor detection system that allows detecting two different pathogens simultaneously [217]. This system is composed of two phage-based ME biosensors and one reference sensor.

In the studies mentioned above, the biosensors were tested in both static and dynamic modes. Static testing involved exposure of the biosensors to static suspensions containing the target pathogen in known concentrations. Dynamic testing involved exposure of the biosensors to flowing suspensions containing known concentrations of target pathogens in a single flow-through mode. The details of the measurement system and experimental procedures have been described in several papers [210–212, 216, 217]. Both JRB7 and E2 ME biosensors exhibit good sensitivity, specificity, and selectivity toward the target pathogen, as well as excellent longevity.

#### *4.4.1 Dose–response of ME Biosensor to Target Pathogen.*

*4.4.1.1 JRB7 phage–based ME biosensor for B. Anthracis spores detection in a static mode.* Wan et al. [210, 216] have successfully employed a JRB7 phage–based ME biosensor to detect *B. anthracis* spores within a static mode. In their research, microelectronically fabricated ME particles ($500 \times 100 \times 4$ μm and $200 \times 40 \times 4$ μm) were immobilized with the JRB7 phage. These formed ME biosensors were sequentially exposed to static *B. anthracis* spore suspensions of increasing concentrations ($5 \times 10^1 - 5 \times 10^8$cfu/ml). The biosensors were exposed to each concentration for 30 min. Figure 14a and b shows the frequency responses of the JRB7 phage–based biosensor with the size of $500 \times 100 \times 4$ μm and $200 \times 40 \times 4$ μm, respectively. The response of reference sensors (no phage coating, with BSA blocking) were also measured under the same experimental conditions. In both cases, as the concentration of the spore suspension was increased, the resonance frequency of the JRB7 phage–based ME biosensors experienced the expected decrease. During the entire test, the frequency of the reference sensor exhibited no appreciable change regardless of the composition of analyte introduced. This showed that nonspecific binding had been blocked during testing by BSA pretreatment.

After the spore exposure tests, the sensor surfaces were observed by scanning electron microscopy (SEM). The SEM studies (Fig. 14) clearly demonstrate that JRB7 phage–based biosensors have good ability to capture *B. anthracis* spores. Only a few spores were observed to have bound to the reference sensor surface, which demonstrates that the nonspecific binding was effectively blocked by precoating the control sensors with 1 mg/ml BSA.

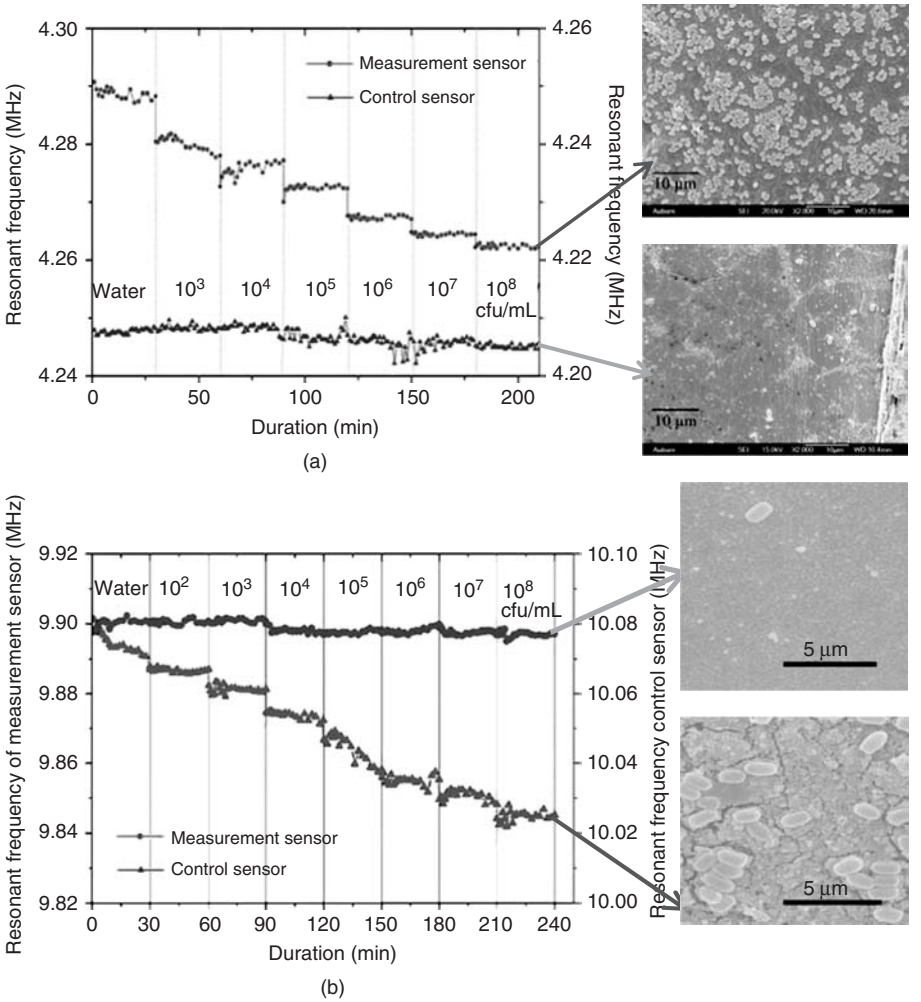



**FIGURE 14** The biosensor response curve (frequency shift as a function of time and concentration) of both measurement and control sensors for (a) $500 \times 100 \times 4$ μm size sensors and (b) for $200 \times 40 \times 4$ μm size sensors [210, 216].

Table 8 summarizes the sensitivity and detection limits of different sized JRB7 phage–based ME biosensors. The results show that the sensitivity, detection limit, and dose–response of the biosensor improved as the size of the biosensor decreased. This result is consistent with predictions of Eq. (6).

Wan et al. [216] also tested biosensors made using mechanically polished/diced ME platforms ($5 \times 1 \times 0.02$ mm) that were immobilized with the JRB7 phage. The dose–responses of these biosensors after exposure to static *B. anthracis* spore suspensions of increasing concentrations ($5 \times 10^1 - 5 \times 10^8$ cfu/ml) are shown in Figure 15. The smooth lines are the sigmoid fits of the experimental data, and each data point is a mean value of the steady-state frequency readings from 50 sensors. The sensitivity of the biosensor, measured as the slope of the linear portion of dose response, was calculated to be 130 Hz per decade or 0.14 cfu/$\mu m^2$ per decade of spore concentration.

**TABLE 8 Table Summarizing the Sensitivity and Detection Limits Achieved for JRB7 Phage-Based Biosensors with Different Dimensions**

| Sensor Dimensions | Sensitivity (Hz/decade) | Detection Limit (cfu/ml) |
|---|---|---|
| $5.0 \times 1.0 \times 0.02$ mm | 130 | $10^3$ |
| $500 \times 100 \times 4$ μm | 6,500 | 850 |
| $200 \times 40 \times 4$ μm | 13,100 | 105 |

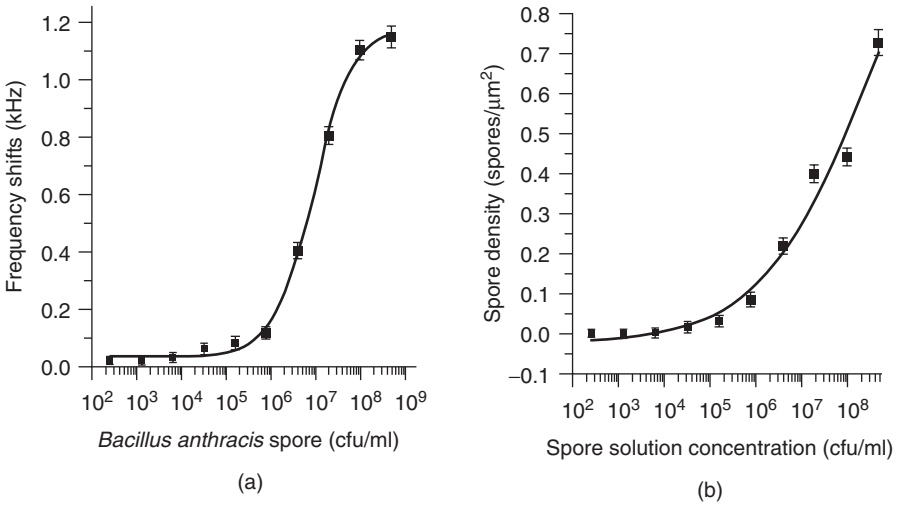



**FIGURE 15** The dose–response of JRB7 phage–based biosensors for detection of *Bacillus anthracis* spores with dimensions of $5 \times 1 \times 0.02$ mm. (a) The mean values of the resonant frequency shifts as a function of spore solution concentration from $10^2$ to $10^8$ cfu/ml. The smooth line is the sigmoidal fit to experimental data points ($\chi = 6.06$, $R^2 = 0.97$). (b) The mean values of bound surface spore density as a function of spore solution concentration from $10^2$ to $10^8$ cfu/ml. The smooth line is the sigmoidal fit to experimental data points ($\chi = 0.043$, $R^2 = 0.98$) [216].

The detection limit of the biosensor was estimated to be $10^3$ cfu/ml, which corresponds to a minimal observable frequency shift of 25 Hz. The dose-dependence curve shows a trend toward saturation at $10^8$ cfu/ml and above.

SEM analysis was used to quantify the number of spores bound to the phage-immobilized ME biosensors, as well as to obtain a visual verification of phage distribution on the sensor surface. In order to count the numbers of spores bound to the biosensor's surface, SEM photographs were taken at 10 randomly chosen regions on the sensor surface, and spores were counted individually. The average number of bound cells per unit area was calculated. The resulting number was multiplied by the entire surface area of the sensor to obtain the total number of bound spores. Figure 15b is the measured density of spores attached to the sensor surface. The results indicate that the measured frequency shifts are due to the additional mass of the bound *B. anthracis* spores.

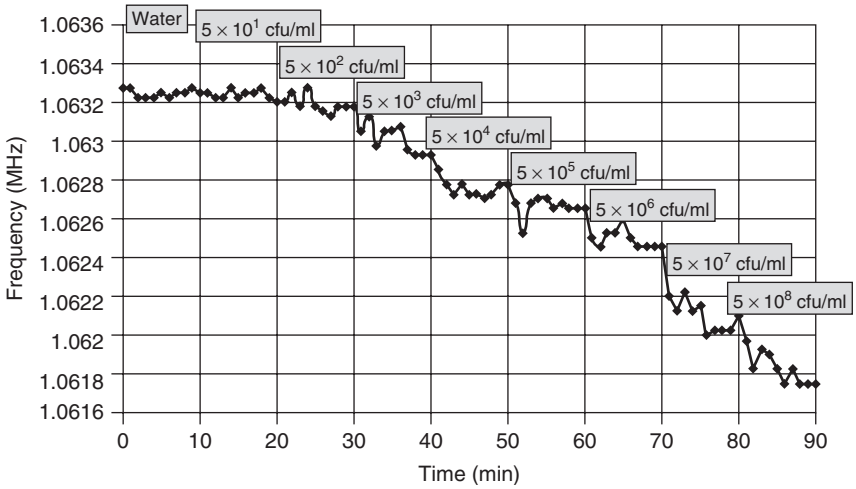



**FIGURE 16** Response of a ME biosensor exposed to different concentrations of *B. anthracis* spores ($5 \times 10^1 - 5 \times 10^8$ cfu/ml) [221].

*4.4.1.2 JRB7 phage–based ME biosensor for B. anthracis spores detection in a dynamic mode.* Huang et al. [221] have demonstrated that *B. anthracis* spores can also be detected by JRB7 phage–based ME biosensors within a dynamic mode. In their research, a mechanically polished/diced ME sensor platform with the size of $2 \times 0.4 \times 0.015$ mm was immobilized with JRB7 phage to form the ME biosensor. Figure 16 shows the dynamic response of a biosensor to increasing concentrations of *B. anthracis* spores ($5 \times 10^1 - 5 \times 10^8$ cfu/ml). As the concentration of the spore suspension was increased, the resonance frequency experienced the expected decrease. The initial frequency remained stable until the solution with a spore concentration of $5 \times 10^3$ cfu/ml was introduced, where the first detectable drop of frequency can be seen. At the end of the test, after introduction of the highest spore concentration, the total resonance frequency shift for this biosensor was 1420 Hz. SEM images (Fig. 17) show the interaction of spores with JRB7 phage on the biosensor surface where the spores were uniformly distributed on the surface. Figure 18 shows the dose–response curve of the ME biosensor dynamic response and represents the sigmoidal fit of the data.

*4.4.1.3 E2 phage-based ME biosensor for S. typhimurium detection.* Lakshmanan, et al. [211, 212] have characterized E2 phage–based ME biosensors for the detection of *S. typhimurium*. Figure 19 shows a typical resonance frequency response as a function of time for an E2 phage–based biosensor ($2 \times 0.4 \times 0.015$ mm) exposed to different solutions containing known concentrations of *S. typhimurium* bacteria. The biosensor's resonance frequency was recorded every 2 min. Exactly 1 ml of each concentration was allowed to flow over the sensor at a flow rate of 50 l/min before the next highest concentration was started. At the flow rate used, it takes 20 min for 1 ml of the analyte to flow over the biosensor. The resonance frequency at the end of every 20 min was used to calculate the resultant frequency shift for that particular concentration. The resonance frequency decreased with the introduction of each successive concentration ($5 \times 10^4$ cfu/mlthrough $5 \times 10^8$ cfu/ml) of *S. typhimurium*. The reference sensor

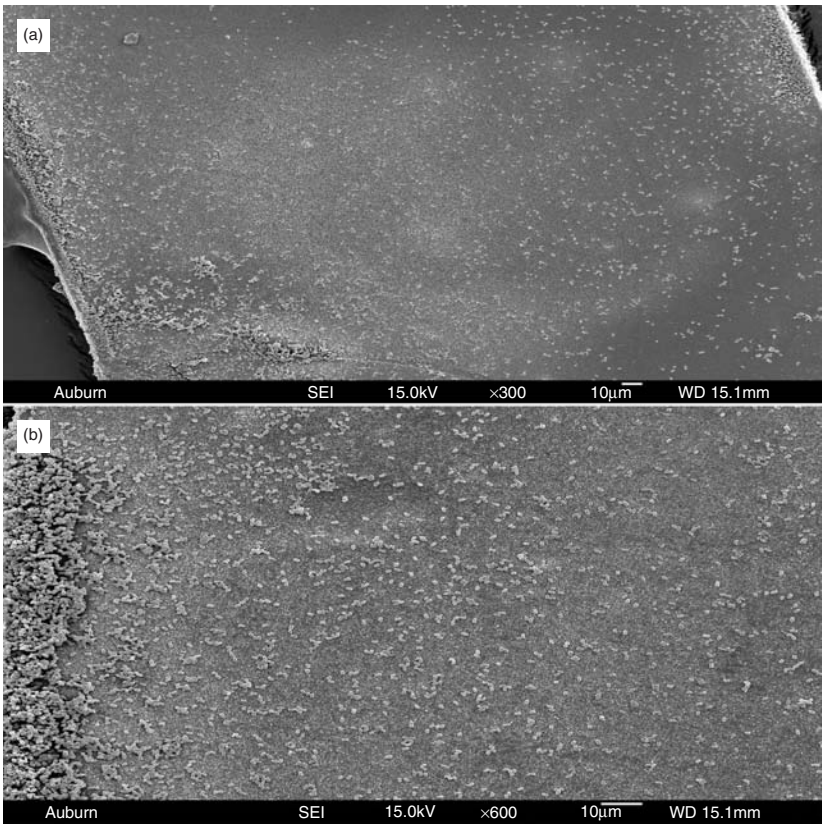



**FIGURE 17** SEM photographs of ME sensor surface after exposure to different concentrations of *B. anthracis* spores ($5 \times 10^1 - 5 \times 10^8$ cfu/ml) dynamically.

(no coating of phage but blocking agent) showed a negligible change in resonance frequency, even upon exposure to very high concentrations ($5 \times 10^8$ cfu/ml) of bacteria. SEM photomicrographs were taken after the exposure experiments to confirm the measured frequency shifts were due to binding of *S. typhimurium*.

Lakshmanan's results showed results similar to the JRB7 phage–based ME biosensor results obtained by Wan and Huang. The smaller the dimensions of the biosensor, the higher the sensitivity and lower the detection limits that were obtained [211, 212]. The dose–response tests were conducted for E2 phage–based ME biosensors with four different lengths (5, 2, 1, and 0.5 mm). Table 9 summarizes the measured sensitivity and detection limits for these E2 phage–based ME biosensors dependent on different sizes. The results showed that as the length of the biosensor decreased from 5 to 0.5 mm, the E2 phage biosensor became more sensitive (sensitivity of 1150 Hz/decade) and was able to detect *S. typhimurium* at a concentration of 60 cfu/ml. Lakshmanan counted [211, 212] the number of bacteria bound to the biosensor surface using SEM micrographs. The results showed that the number of attached *S. typhimurium* cells on the biosensors agrees with the measured frequency shifts of the E2 biosensors. This is consistent with Wan's investigation [216].

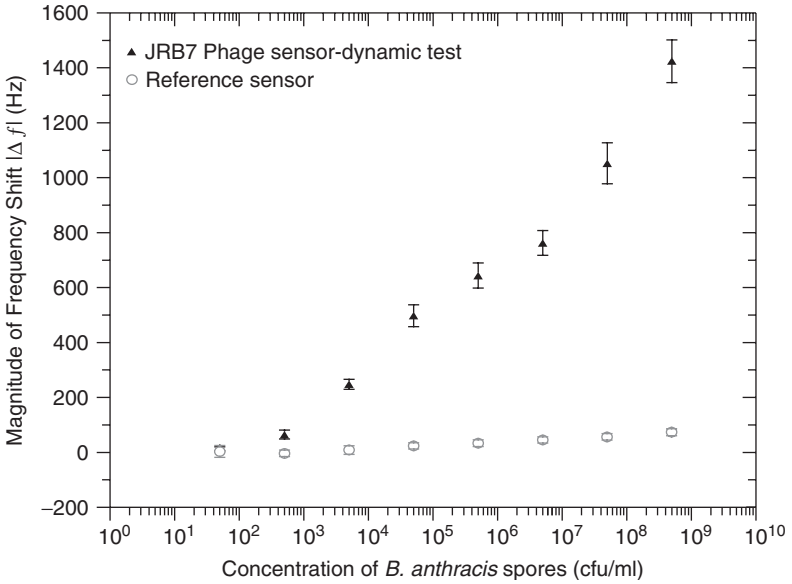



**FIGURE 18** Dose–response curve of ME biosensor ($2 \times 0.4 \times 0.015$ mm) coated with $5 \times 10^{11}$ cfu/ml phage suspension (contain 420 m*M* NaCl) and then exposed to increasing concentrations ($5 \times 10^1 - 5 \times 10^8$ cfu/ml) of *B. anthracis* spores suspensions in water [(▲) ($R^2 = 0.984$)]. Reference sensor (○) represents the uncoated (devoid of phage) sensor's response. The curve represents the sigmoidal fit of signals obtained [221].

***4.4.2 Specificity of Phage-Based ME Biosensors.*** The specificity of phage-based ME biosensors can be evaluated by exposing them to similar pathogenic species, to examine the cross-reaction between a specific phage with nonspecific pathogens. Further investigation can be established by measuring the phage-based ME biosensor's response to specific target pathogens masked with one similar species.

*4.4.2.1 JRB7 phage-based ME biosensor. B. anthracis* spores belong to the *Bacillus* species and have physical characteristics similar to *B. subtilis*, *B. cereus*, *B. licheniformis*, and *B. megaterium* spores. In order to study the specificity of JRB7 phage–based ME biosensors toward *B. anthracis* spores, Wan et al. [210, 216] studied the specificity of JRB7 phage–based ME biosensors by exposing them to concentrated solutions ($10^8$ spores/ml) of various *Bacillus* spores mentioned above (see Figure 20). SEM was used to determine the surface density of bound spores with JRB7 phage. The JRB7 phage–based ME biosensors showed about 40-fold better binding to *B. anthracis* than *B. licheniformis* and *B. megaterium*, and about 15-fold better than *B. subtilis* and *B. cereus* spores. This demonstrated that the JRB7 phage preferentially bound to *B. anthracis* spores better than other *Bacillus* spores. Although the JRB7 phage clone does have some cross-reaction with spores of other *Bacillus* species, compared to the specific binding with *B. anthracis* spores, this cross-reaction is weak enough to be negligible.

In order to further demonstrate the specificity of the JRB7 phage-coated ME biosensors, the biosensor was exposed to increasing concentrations of *B. anthracis* spores suspension ($5 \times 10^3 - 5 \times 10^8$ cfu/ml) in a mixture of a fixed concentration of *B. cereus* spores ($5 \times 10^8$ cfu/ml). Each test suspension was pipetted off followed by adding a new

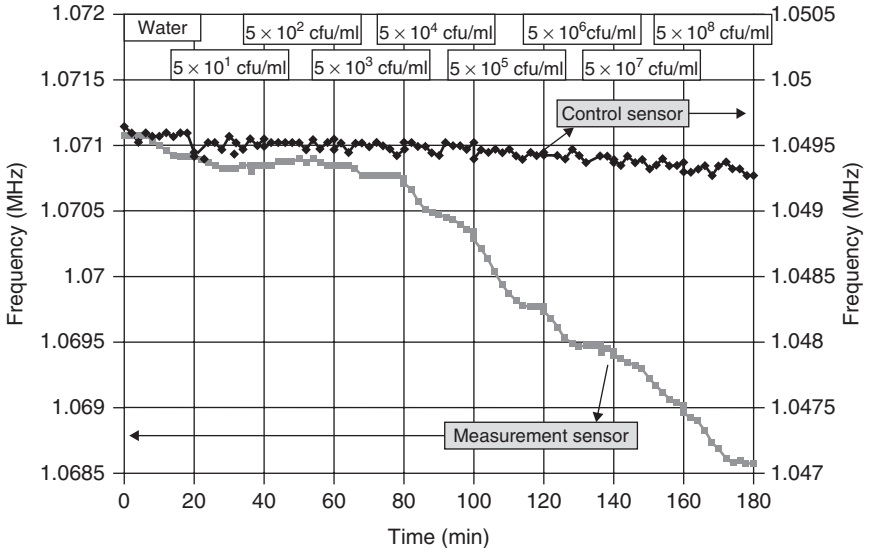



**FIGURE 19** Typical frequency—response curve for an E2 phage–based biosensor for *S. typhimurium* with dimensions $0.015 \times 0.4 \times 2$ mm. 1 ml of each concentration of bacteria containing solution was passed over the sensor at a flow rate of 50 l/min. The control sensor is not coated with the phage [238].

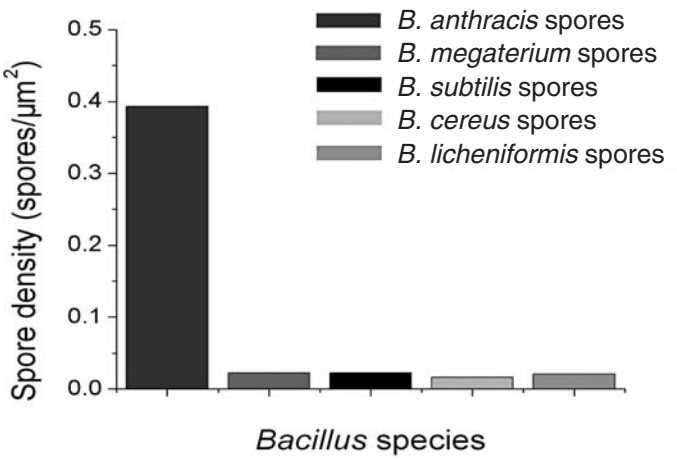



**FIGURE 20** Biosensor. specificity: phage-coated sensors were exposed to solutions containing $10^8$ spores/ml. Density of attached spores were measured using SEM. Tween-20 with 1% BSA was used for blocking [216].

suspension of a different concentration at 30-min intervals. The results of this set of experiments conducted by Wan et al. are shown in Figure 21 [216]. After the frequency of the biosensor is stabilized in water, a small frequency shift was observed after the sensor was exposed to the initial concentrated *B. cereus* suspension ($10^8$ cfu/ml). The frequency shifts were caused by the nonspecific binding between phage and *B. cereus* spores. This is consistent with previous results that showed the JRB7 affinity-selected

**TABLE 9 Summary of Sensitivity and Detection Limits Achieved for E2 Phage Biosensors with Different Dimensions**

| Sensor Dimensions (mm) | Sensitivity (Hz/decade) | Detection Limit (cfu/ml) |
|---|---|---|
| $5.0 \times 1.0 \times 0.015$ | 98 | $10^4$ |
| $2.0 \times 0.4 \times 0.015$ | 161 | 950 |
| $1.0 \times 0.2 \times 0.015$ | 770 | 100 |
| $0.5 \times 0.1 \times 0.015$ | 1150 | 60 |

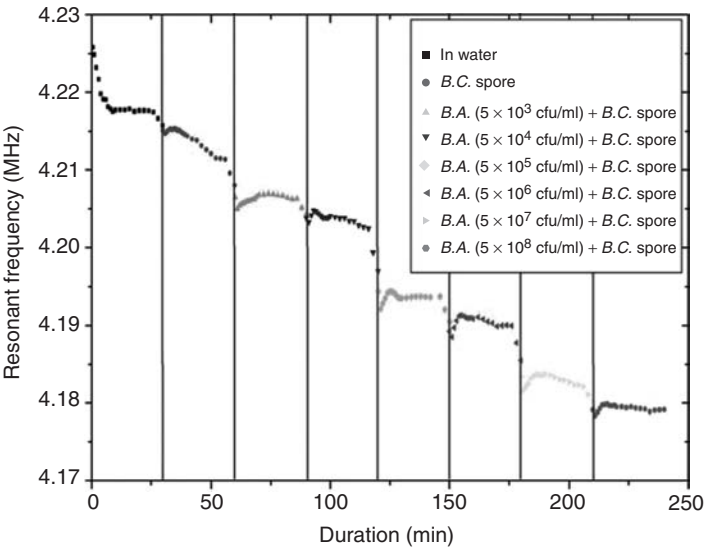



**FIGURE 21** The response curve of a MEP ($500 \times 100 \times 4$ μm) as a function of time and spore concentration in a mixed solution of *Bacillus anthracis* and *Bacillus cereus* spores. The concentration of the *B. cereus* spores is $10^8$ cfu/ml [216].

phage clone does cross-react with the *B. cereus* species. Upon increasing the concentration of *B. anthracis* spores, the JRB7 phage–based ME biosensor showed progressively larger frequency shifts. This was because *B. anthracis* spores were bound to the biosensor's surface even in the presence of a background of $10^8$ cfu/ml of *B. cereus* spores. Compared to total frequency shift caused by the specific binding between the JRB7 phage and *B. anthracis* spores, the frequency shift due to the nonspecific binding is small enough to be negligible.

*4.4.2.2 E2 phage-based ME biosensors.* Lakshmanan et al. [239] used similar experimental methods as Wan et al. to evaluate the specificity of the E2 phage–based ME biosensors by exposing them individually to static suspensions of *S. typhimurium*, *E. coli, S. enteritidis*, and *L. monocytogenes*. In their study, SEM images of 10 random regions of the biosensor surface were taken. The number of bacteria cells bound to those regions was counted. The sensor surface area coverage density (number of cells per unit area) was then calculated and multiplied by the total surface area of the sensor to obtain the total number of bacteria bound to the sensor. Assuming that the average weight of a

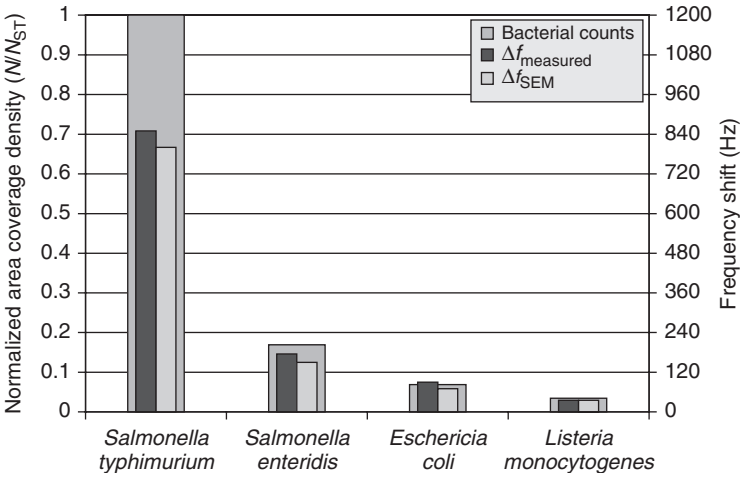



**FIGURE 22** Specificity of phage-immobilized sensors exposed to different pathogens at a concentration of $5 \times 10^8$ cfu/ml. The normalized area coverage density was calculated from SEM photomicrographs of the sensor surface (an average of five sensors each). $\Delta f_{measured}$ and $\Delta f_{SEM}$ are shown on the right side [239].

*S. typhimurium* cell is 2 pg, the total mass change ($\Delta m_{SEM}$) can be obtained. Based on Eq. (5), the theoretical frequency shift caused by $\Delta m_{SEM}$ was calculated as $\Delta f_{SEM}$. Before and after exposure to bacteria pathogens, the frequencies of E2 phage–based biosensors were measured. The frequency shift ($\Delta f_{measured}$) was then calculated and compared with $\Delta f_{SEM}$ obtained above. Figure 22 [239] shows the comparison results of E2 phage–based ME biosensors exposed to different pathogens at a concentration of ($5 \times 10^8$ cfu/ml). The result showed that $\Delta f_{measured}$ and $\Delta f_{SEM}$ have similar values, which demonstrates that the frequency shift of the biosensor was caused by the binding between the E2 phage and bacterial pathogens. The normalized area coverage density shown in Figure 22 was calculated as the ratio of the area coverage density of a certain pathogen ($N_P$) to the area coverage density of *S. typhimurium* ($N_{ST}$). The normalized area coverage density of the biosensors exposed to *S. typhimurium, S. enteritidis*, *E. coli*, and *L. monocytogenes* were 1.00, 0.17, 0.06, and 0.03, respectively. Lakshmanan's results (Fig. 23) showed significantly lower affinity of the immobilized phage to pathogens other than *S. typhimurium*, which demonstrated that E2 phage–based ME biosensors have excellent specificity.

The effect that masking bacteria has on the detection of *S. typhimurium* by the E2 phage–based biosensor was studied. Lakshmanan [239] exposed the E2 biosensors to three different sets of prepared suspensions: (i) *S. typhimurium*, (ii) *S. typhimurium* + *E. coli*, and (iii) *S. typhimurium* + *E. coli* + *L. monocytogenes*. On the basis of the resulting dose–response curve, Lakshmanan constructed a hill plot [212, 215, 220, 240] and determined the binding kinetics of the testing biosensors. The binding valency was similar for all the three prepared suspensions. Overall, Lakshmanan [212] determined the E2 phage–based ME biosensor with the size of $2 \times 0.4 \times 0.015$ mm was capable of detecting small amounts of *S. typhimurium*, even in the presence of high concentrations of masking bacteria. This established that the E2 phage–based ME biosensor could detect *S. typhimurium* with high specificity and selectivity.

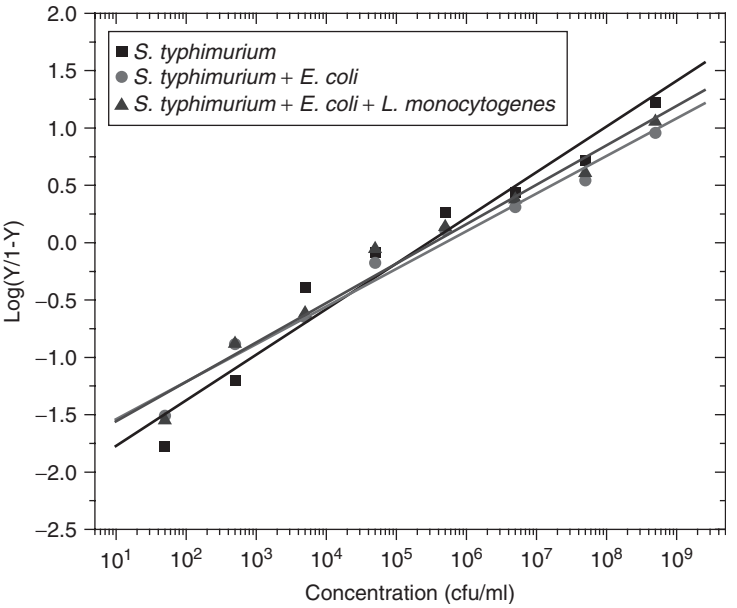



**FIGURE 23** Hill plot constructed from the dose–response curves, showing the ratio of occupied ($Y$) and free phage sites ($1-Y$) as a function of bacterial concentrations in different mixtures. The straight line is the linear least squares fit to the data (*S. typhimurium* (■): slope $= 0.40 \pm 0.03$, $R^2 = 0.97$; *S. typhimurium* + *E. coli* (•): slope $= 0.33 \pm 0.02$, $R^2 = 0.98$; and *S. typhimurium* + *E. coli* + *L. monocytogenes* (▲) slope $= 0.34 \pm 0.02$, $R^2 = 0.97$) [239].

Table 10 summarizes the sensitivity, dissociation constant, and binding valence of the biosensor in the different mixtures. The binding valencies obtained from the hill plots were 2.42, 2.79, and 2.91 for suspension 1, suspension 2, and suspension 3, respectively. This reaffirms the multivalent nature of the phage–*Salmonella* interaction on the biosensors. A summary of results obtained from the real food products detection using E2 phage biosensors are also presented in Table 10 [212].

***4.4.3 Stability of Phage-Based ME Biosensor.*** To evaluate the capability of a biosensor, it is essential to establish the storage life and longevity of the immobilized biorecognition element. Brigati and Petrenko [241] have demonstrated that a phage is more robust than other commonly used biorecognition probes, such as polyclonal and monoclonal antibodies. In order to investigate the stability of phage-based ME biosensors, Wan et al. [216], Lakshmanan [211, 212], and Guntupalli [242] prepared a set of ME biosensors, including JRB7 phage–based ME biosensors, E2 phage–based biosensors, and antibody-based ME biosensors. Three types of biosensors were all incubated under three different temperatures (25, 45, and 65°C). The biosensors were removed at specified times of 1, 2, 3 days and so on, and tested at room temperature by exposing them to the specific target pathogens suspensions (*B. anthracis/S. typhimurium*) at a concentration of $10^8$ cfu/ml. The number of cells/spores bound per unit surface area on the specific biosensor was determined by SEM. Figures 24–26 show the change in bound spore densities, that is, the sensor's binding affinity with storage time at different temperatures for both phage-coated and antibody-coated sensors.

**TABLE 10 The Sensitivity, Dissociation Constant, and Binding Valence of E2 Phage–Based ME Biosensors in Different Bacterial Mixtures**

| Bacterial Mixtures | *S. typhimurium* Detection Sensitivity (Hz/decade) | Binding Valence ($1/n$) | $K_d$(cfu/ml) | $K_{d(\text{apparent})} = K_d^n$ (cfu/ml) |
|---|---|---|---|---|
| S. typhimurium | 161 | 2.42 | 149 | $1.82 \times 10^5$ |
| S. typhimurium + E. coli | 131 | 2.79 | 82 | $2.19 \times 10^5$ |
| S. typhimurium + E. coli + L. monocytogenes | 127 | 2.91 | 87 | $4.41 \times 10^5$ |
| Spiked apple juice | 155 | 2.77 | 89 | $2.51 \times 10^5$ |
| Spiked milk | 118 | 2.5 | 136 | $2.16 \times 10^5$ |

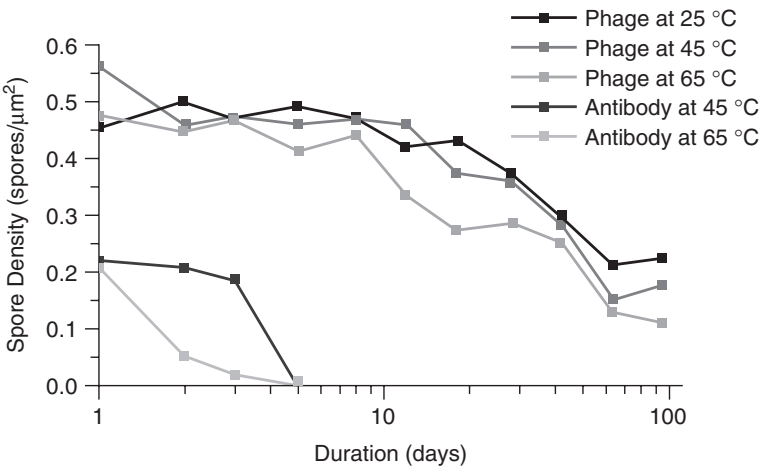



**FIGURE 24** The bound surface spore density, which represents the binding affinity of the specific bioprobes as a function of time at different temperatures for both phage and polyclonal antibody. The antibody-based sensors lost all binding activity after 5 days of storage at 65°C and 45°C [216].

Overall, the results showed a general decrease in the binding affinity of phage-based ME biosensors with increased storage time and temperature. Phage-based ME biosensors have better stability, longevity, and binding affinity to specific target pathogens compared to antibody-based ME biosensors.

Wan et al. [216] observed that after 100 days of storage, the JRB7 phage–based biosensors preserved about 49, 40, and 25% of their original binding affinity, respectively for temperatures of 25, 45, and 65°C. While the antibody-based ME biosensors showed no binding affinity after only 5 days at 65°C and 45°C. SEM images (Fig. 25), where both JRB7 phage–based biosensors and antibody-based biosensors were incubated at a temperature of 65°C and then exposed to the same *B. anthracis* spores suspension

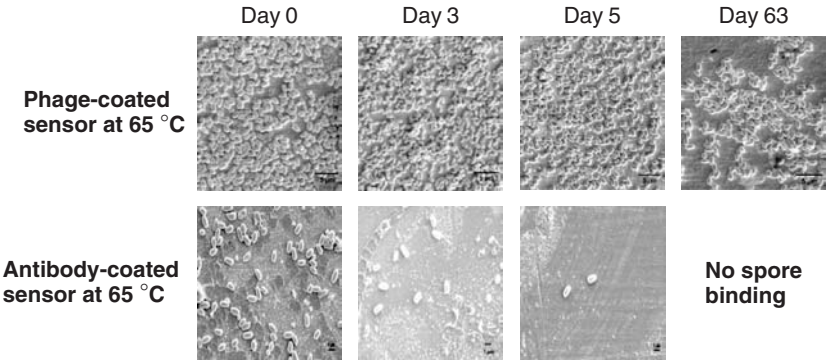



**FIGURE 25** SEM photomicrographs of JRB7 phage-coated sensors and antibody-coated sensors after storage at 65°C. Compared with phage-modified biosensors, the binding affinity of antibody-coated biosensors dropped to zero after being stored at 65°C for 5 days. JRB7 phage-coated biosensors still showed good binding affinity after 2 months [216].

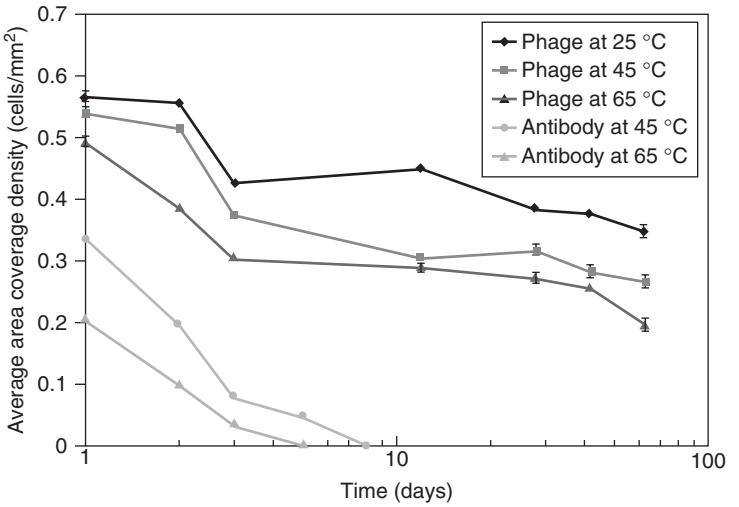



**FIGURE 26** E2 phage–based ME biosensor surface coverage densities (average number of cells per square micrometer) calculated from SEM micrographs of stored magnetoelastic biosensors (25, 45, and 65°C) after exposure to *S. typhimurium* ($5 \times 10^8$ cfu/ml) [239, 242].

($5 \times 10^8$ cfu/ml), demonstrated that the JRB7 phage clone used in this research has a better binding ability than some of the best commercially available antibodies.

Figure 26 shows the study results that compare the longevity of E2 phage–based ME biosensors with antibody-based ME biosensors at three different temperatures (25, 45, and 65°C). Similar to the longevity results from JRB7 phage–based ME biosensors mentioned above (Fig. 24 and 25), the area coverage density (number of bacteria bound to the sensor per unit surface area) of E2 phage–based biosensors was observed to decrease with increasing time and temperature. The E2 phage–based biosensors retained 59, 45, and 33% of their binding affinity at 25, 45, and 65°C, respectively, after a period of 63 days. The antibody-based biosensors showed a rapid loss of binding affinity, with all

binding affinity lost after 8 days at the elevated temperatures of 45 and 65°C. The initial binding affinity of the E2 phage–based biosensors was observed to be much higher than the antibody-based biosensors.

***4.4.4 Detection of S. Typhimurium Bacteria in Food Products.*** Most of the biosensors for food pathogen detection are used in water. It is also essential to establish the field applicability of ME biosensors for applications in other media (i.e. apple juice, milk). Therefore, the work published by Lakshmanan et al. [212, 239] was extended to examine the viability of testing for *S. typhimurium* suspended in the real food product. The biosensors with the size of $2 \times 0.4 \times 0.015$ mm were exposed to milk and apple juice spiked with increasing concentrations of *S. typhimurium* ($5 \times 10^1 - 5 \times 10^8$ cfu/ml). The biosensor response was studied by flowing food liquids containing increasing concentrations of bacteria over the sensors at a flow rate of 50 μl/min. This flow rate was chosen in order to ensure that laminar flow was maintained. Exactly 1 ml of a specific concentration of bacteria in the food liquid was allowed to flow over the sensor (20 min at the specified flow rate). The biosensor's frequency shift was calculated by subtracting the final measured frequency from the initial frequency measured at the introduction of the food liquid.

Figure 27 represents the average response of five different biosensors. Similar dose responses were observed for the biosensor exposed to spiked apple juice and water samples. The resonance frequency shifts obtained for spiked milk samples were lower than that of spiked water and spiked apple juice samples. The dose response was linear over five aliquots of concentrations ($5 \times 10^3$ through $5 \times 10^7$ cfu/ml) for the three different media. The sensitivity of the biosensor was calculated as the slope of the linear region of the dose–response curve (Hz per decade of concentration change). The sensitivity of biosensors exposed to spiked water, apple juice, and milk were 161, 155, and 118 Hz/decade, respectively. The control sensor had a negligible change in resonance frequency in response to even high concentrations of *S. typhimurium*. The control sensor showed a maximum resonance frequency shift of 50 Hz, while a maximum resonance frequency shift of 980 Hz was observed for the biosensor. This significant difference in the measured frequency shifts (control vs. measurement sensor) indicates negligible, nonspecific binding of bacteria to the bare gold surface. SEM photomicrographs of the assayed biosensors were used to provide visual verification of bacterial binding to the sensor surfaces.

***4.4.5 Sequential Detection of S. Typhimurium and B. Anthracis Spores Using Multiple Phage-Based ME Biosensors.*** Utilizing multiple phage-based ME biosensors, Huang et al. [243, 244] demonstrated the simultaneous detection of different pathogens that were sequentially introduced to the measurement system. In their experiments, the detection system included a reference sensor as a control, an E2 phage-coated ME sensor specific to *S. typhimurium*, and a JRB7 phage-coated ME sensor specific to *B. anthracis* spores. The JRB7 and E2 biosensors possessed separate characteristic resonance frequencies; therefore, two different pathogens can be simultaneously monitored and discriminated. In order to prevent nonspecific binding during exposure to multiple analytes, BSA solution was then immobilized on the sensor surfaces to serve as a blocking agent. Huang et al. sequentially exposed this multiple detection system to increasing concentrations of *S. typhimurium* ($5 \times 10^1 - 5 \times 10^8$ cfu/ml) and *B. anthracis* spores ($5 \times 10^1 - 5 \times 10^8$ cfu/ml) suspensions in water. The flow rate was 50 μl/min and, for

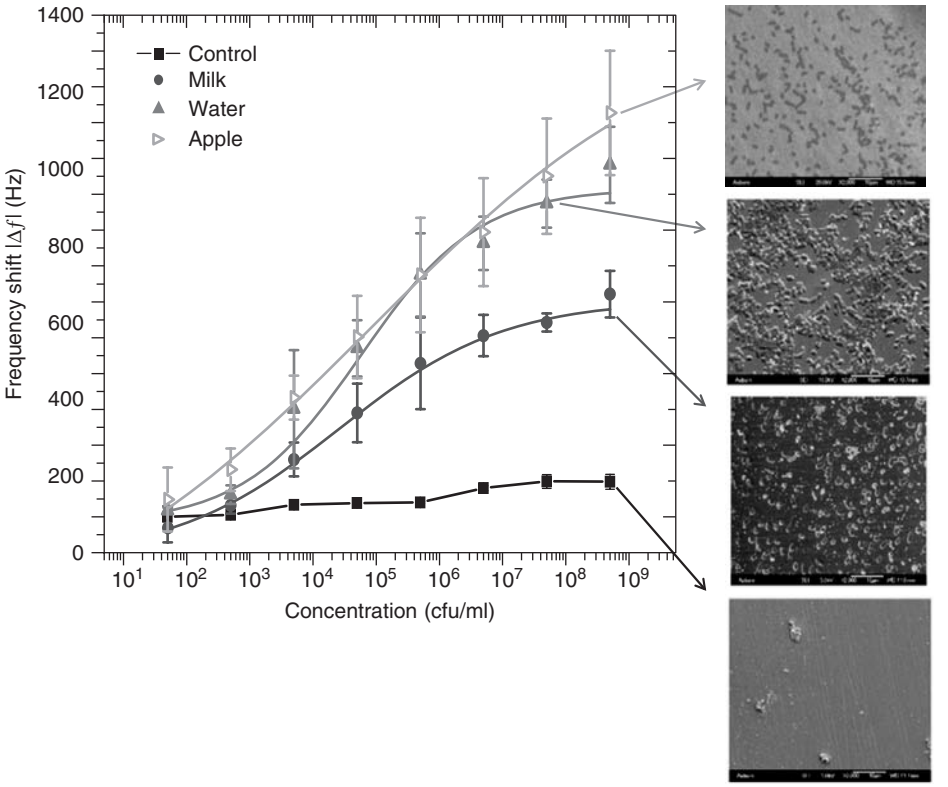



**FIGURE 27** Comparison of the dose responses of magnetoelastic biosensors ($2 \times 0.4 \times 0.015$ mm) when exposed to increasing concentrations ($5 \times 10^1 - 5 \times 10^8$ cfu/ml) of *S. typhimurium* suspensions in water [(▲)$\chi^2 = 0.442$, $R^2 = 0.99$], apple juice [(▼)$\chi^2 = 0.237$, $R^2 = 0.99$], and fat-free milk [(•)$\chi^2 = 0.194$, $R^2 = 0.99$]. Control (■) represents the uncoated (devoid of phage) sensor's response. The curves represent the sigmoid fit of signals obtained.

each concentration, a 1-ml suspension was used. Figure 28 shows the typical response of the multiple phage-based ME biosensors to water, *S. typhimurium*, and *B. anthracis* spore suspensions ($5 \times 10^8$ cfu/ml each) [217]. The steady-state response of all the sensors in water is observed during the first 10 min of the test. After the introduction of *S. typhimurium*, the E2 phage-coated sensor showed a smooth decrease in resonance frequency due to the binding of these bacteria onto the sensor surface. Similarly, the subsequent exposure to a $5 \times 10^8$ cfu/ml *B. anthracis* spore solution caused a sudden drop in the resonance frequency for the JRB7 phage-coated sensor. On exposure to either analyte, the decrease in frequency only occurs when bacteria cells or spores bind to the specific phage on the sensor's surface. Overall, the frequency shift was about 1280 Hz for the E2 phage-coated sensor, and about 1120 Hz for the JRB7 phage-coated sensor for $5 \times 10^8$ cfu/ml analyte solutions.

The SEM photographs (also shown in Fig. 28) of the reference and phage-coated sensors confirmed that the frequency shifts were due to the spores/bacterial cells becoming attached to the corresponding sensors.

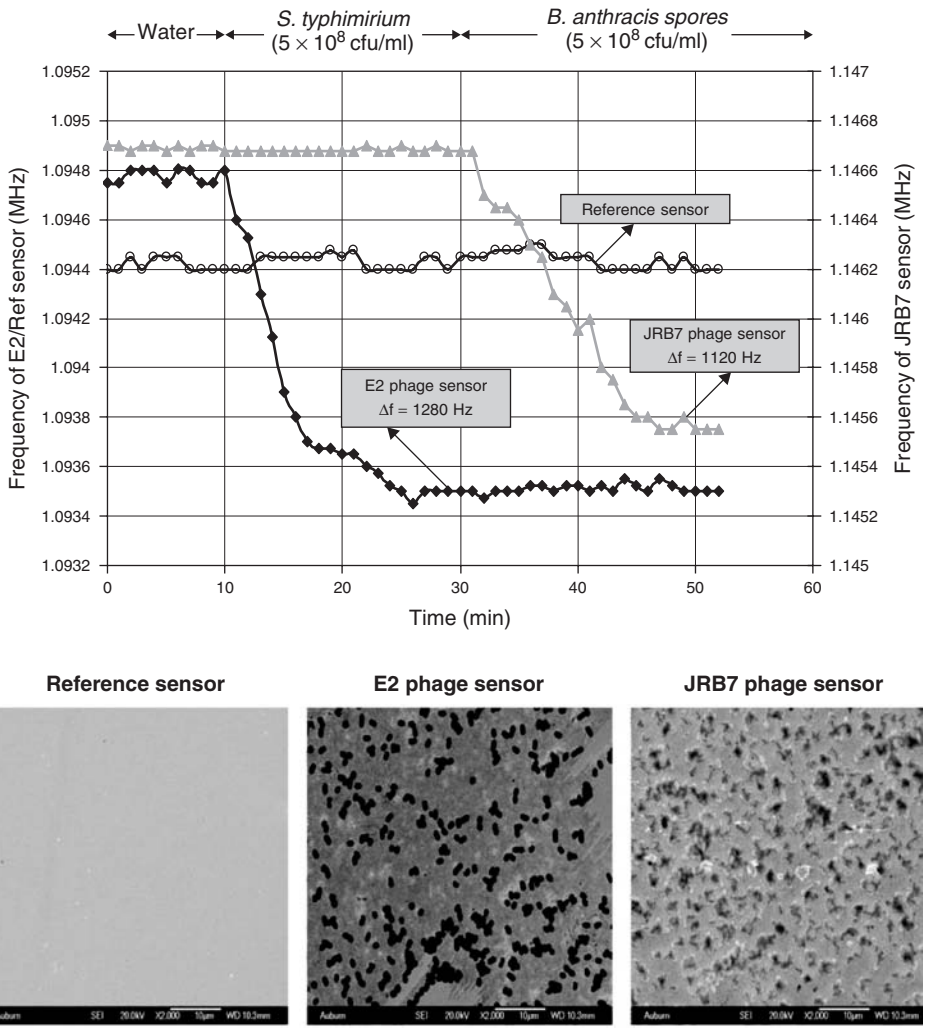



**FIGURE 28** Response curves and SEM pictures for three-diced ME biosensors tested simultaneously when exposed to the bacterial/spores suspension with the concentrations of $5 \times 10^8$ cfu/ml [217].

## 5 OTHER DETECTORS USING PHAGE AS A BIORECOGNITION ELEMENT

### 5.1 Phage Used for Electrochemical Sensing

Bacteriophages have been used as biorecognition elements for other types of biosensors. Neufeld et al. [245] developed a novel amperometric detector by combining phage typing and the related release of an intrinsic enzyme to specifically identify and quantify *E. coli* bacteria. In their work, the enzyme markers ($\beta$-galactosidase), released due to a specific phage-bacteria lytic interaction, react with the substrate *p*-aminophenyl-$\beta$-D-galactopyranoside ($\beta$-PAPG) to produce *p*-aminophenol (PAP).

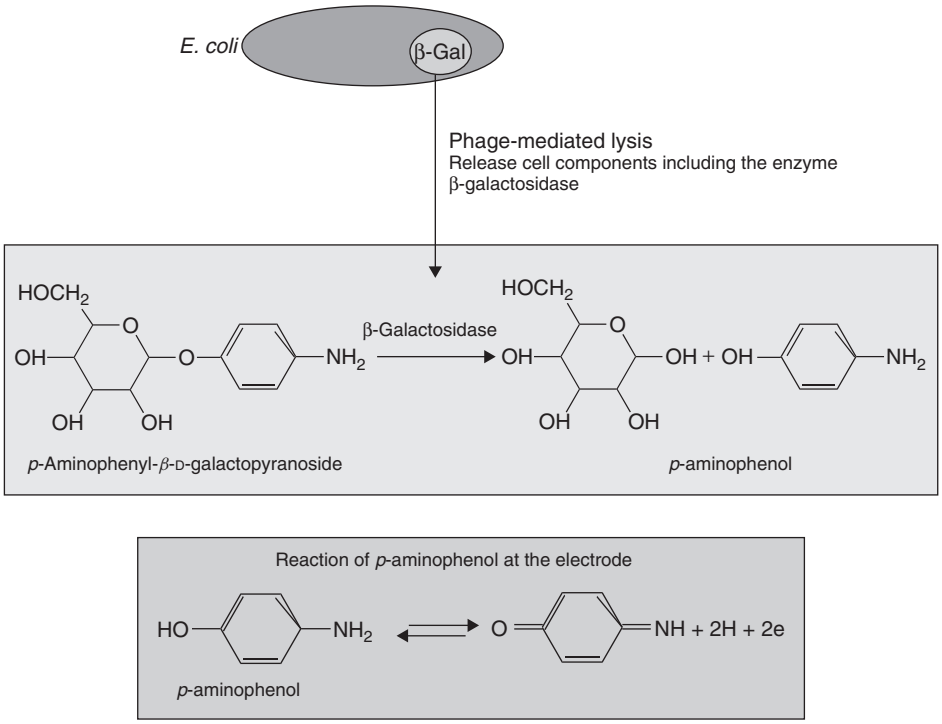



**FIGURE 29** Basic reactions involved in amperometric detection of *E. coli* [245]. In this technique the intrinsic enzyme from the bacteria is released by phage-driven lysis of the cells.

PAP is oxidized at the carbon anode of the amperometric sensor, resulting in an electric current that is proportional to the target bacteria concentration. Figure 29 shows the reaction between enzyme and the substrate that is involved in the detection of *E. coli* using an amperometric biosensor. A similar approach was developed by Yemini [246] for the detection of *B. cereus* and *Mycobaterium smegmatis*. The intrinsic enzymes $\alpha$-glucosidase and $\beta$-glucosidase, released respectively by a specific phage-pathogenic bacteria interaction, catalyzed the hydrolysis of their corresponding substrate to yield PAP. Although the detection limit of this method was 10 cfu/ml, the preincubation step (about 8 h) was required in order to detect the lowest concentration of bacterial suspension. Recently, Seo et al. [247, 248] fabricated a nanowell sensor as potentiometric sensor platform to utilize biochip techniques. After immobilization with a phage, the interaction between target bacteria and the phage results a transitory ion efflux that can be detected by the sensor. This combination provided a rapid pathogen detection technique with good sensitivity and specificity.

## 5.2 Phage Used for Optical Sensing

Affinity-selected phage is a bioprobe used to detect various antigens by labeling with fluorescent/luminescent markers [249]. Goodridge et al. combined fluorescently labeled phage with the antibody-immobilized immunomagnetic beads and successfully detected the *E. coli* O 157:H7 in inoculated ground beef and milk [250, 251]. In their work, the labeled phage interacted with the target pathogen to produce optical signals that are related

to the amount of pathogens present in the food product sample. Goldman et al. [252] employed an optical fiber sensor composed of dye Cy5 labeled phage-displayed peptides as the bioprobe to detect SEB, a causative agent of food poisoning. The phage-displayed peptides used in this method are formed by fusing the binding peptides to the PIII minor protein coat that is located on the tip of the phage capsid. This expression format was less optimal compared with the landscape phage described in Section 4.1.1 above, where the multiple binding sites are realized after modification. The high detection sensitivity of 1.4 ng/well was achieved for this optical fiber method. However, compared to the sensor that utilized antibody as the bioprobe, the signal was weaker and less specific. Blasco et al. [253] and Wu et al. [254] used the phage-mediated release of the enzyme adenylate kinase (AK) as a cell marker for *E. coli* and *Salmonella newport*. In their works, adenosine diphosphate is used as a substrate, while the phage-mediated lysis is used to release AK and adenosine triphosphate (ATP) from the interior of the cells. AK catalyzes to produce large amounts of ATP, which will then react with luciferase to produce luminescence. A detection limit of $10^3$ cfu/ml was reported [253] for this method. Recently, advances in nanotechnology have resulted in a new class of fluorescence-based assays [255–257]. Edgar et al. [258] utilized filamentous phage with surface peptides that were able to interact with the target pathogen cells if there was biotin present in them. Subsequently, quantum dots were used to bind with the phage, and the amount of the target pathogen was analyzed using flow cytometry and fluorescence microscopy.

The examples described above are the indirect phage-based optical methods for foodborne pathogen detection. Direct phage-based methods were also developed where the biological recognition event was measured directly based on the changes in the properties of the light used. Balasubramanian et al. [259] reported a lytic phage-based SPR for the detection of various concentrations of *S. aureus*. In their work, the phage was immobilized onto the gold surface of SPR by physical adsorption. The detection limit of $10^4$ cfu/ml was achieved.

### 5.3 Phages Used for Acoustic Wave Sensing

The combination of phages with AW detectors provides the capability of detecting pathogenic bacteria with high sensitivity and specificity. This advantage makes phage-based AW sensors useful for food safety applications. Petrenko et al. [159] coated a selected phage on a QCM surface for the detection of *S. typhimurium*. Fu et al. [260] immobilized affinity-selected phage on ME MC for the detection of *B. anthracis* spores and *S. typhimurium*.

Table 11 summarizes the literature reports of various assays by using the phage as the biorecognition element for foodborne pathogen detection.

## 6 SUMMARY

Biosensors hold much potential for real-time, field applications to insure the security and safety of our food supply. The development of biosensors is rapidly progressing and within 5 years several biosensors should be commercially available. The development of an alternate to antibody-based detection, that is, phage detection, should greatly improve the robustness and longevity of future commercial biosensors. By using in combination, several different techniques such as biosensors in the field and PCR/ELISA

**TABLE 11 Phage-Based Bioassays for Foodborne Pathogen Detection**

| Transduction | Assay Type and Mechanism | Target | Detection Limit | Reference |
|---|---|---|---|---|
| Amperometric electrode | Phage-induced cell lysis causing release of components (such as $\beta$-galactosidase, $\alpha$-glucosidase, and $\beta$-glucosidase) | *E. coli* (K-12, MG 1655) | 1 cfu/100 ml | 245, 246, 261 |
| | | *B. anthracis* | 10 viable cells/ml | |
| | | *M. Smegmatis* | 1 cfu/ml | |
| Bioluminescence | Luciferase reporter phage | *M. tuberculosis L. monocytogenes* | | 262 |
| Fluorescence | Fluorescently labeled phage in combination with immunomagnetic beads | *E. coli* O157:H7 | $10^2 - 10^3$ cells/ml | 250, 251 |
| Quantum dots | Biotinylated phage and streptavidin conjugated quantum dot | *E. coli* BL-21 | 10 cells/ml | 258 |
| SPR | Affinity-selected phage-immobilized using physical adsorption/SAMs | *S. aureus L. monocytogenes* | | 209, 263 |
| QCM | Phage display technology to engineer display peptides specific to the target analyte. Affinity-selected phage-immobilized using physical adsorption | *S. typhimurium* | 100 cells/ml | 159, 215 |
| Magnetoelastic cantilever | Phage display technology to engineer display peptides specific to the target analyte. Affinity-selected phage-immobilized using physical adsorption | *B. anthracisS. typhimurium* | $10^4$ cells/ml | 260, 264 |
| Magnetoelastic particle resonators | Phage display technology to engineer display peptides specific to the target analyte. Affinity-selected phage-immobilized using physical adsorption | *B. anthracisS. typhimurium* | Depends on size of sensor | 210–212, 216, 217, 221, 232, 264 |

and cultures in the lab, a robust and effective method of detecting food contamination can be implemented.

## REFERENCES


1. Mead, P. S., Slutsker, L., Dietz, V., McCaig, L. F., Bresee, J. S., Sharpiro, C., Griffin, P. M., and Tauxe, R. V. (1999). Food-related illness and death in the United States. *Emerging Infect. Dis.* **5**, 607–625.
2. (2005). *About Foodborne Illness*. Available at http://www.foodborneillness.com/.
3. Altekruse, S. F., Cohen, M. L., and Swerdlow, D. L. (1997). Emerging foodborne diseases. *Emerging Infect. Dis.* **3**, 503–510.
4. Slutsker, L., Altekruse, S. F., and Swerdlow, D. L. (1998). FOODBORNE DISEASES: emerging pathogens and trends. *Infect. Dis. Clin. North Am.* **12**, 199–216.
5. Todd, E. C. (1989). Costs of acute bacterial foodborne disease in Canada and the United States. *Int. J. Food Microbiol.* **9**, 313–326.
6. Voetsch, A. C., Van Gilder, T. J., Angulo, F. J., Farley, M. M., Shallow, S., Marcus, R., Cieslak, P. R., Deneen, V. C., and Tauxe, R. V. (2004). FoodNet estimate of the burden of illness caused by nontyphoidal *Salmonella* Infections in the United States. *Clin. Infect. Dis.* **38**, S127–S134.
7. Berkow, R. (1992). *The Merck Manual of Diagnosis and Therapy 1992*, 16th ed. Merck Publishing Group.
8. Ryan, C. A., Nickels, M. K., Hargrett-Bean, N. T., Potter, M. E., Endo, T., Mayer, L., Langkop, C. W., Gibson, C., McDonald, R. C., and Kenney, R. T. (1987). Massive outbreak of antimicrobial-resistant salmonellosis traced to pasteurized milk. *JAMA* **258**, 3269–3274.
9. (2006). *Multistate Outbreak of E. coli O157 Infections, November-December 2006*. Available at http://www.cdc.gov/ecoli/2006/december/121406.htm.
10. CDC. (1992). The management of acute diarrhea in children: oral rehydration, maintenance, and nutritional therapy. *MMWR Wkly.* **41**(RR–16), 1.
11. CDC. (2005). Preliminary FoodNet data on the incidence of infection with pathogens transmitted commonly through food---10 sites, United States, 2004. *MMWR, Morb. Mortal. Wkly. Rep.* **54**, 352–356.
12. CDC. (2008). Summary of notifiable diseases --- United States, 2006. *MMWR, Morb. Mortal. Wkly. Rep.* **55**, 1–94.
13. CDC. (2003). Multistate Outbreak of *Salmonella* serotype *typhimurium* infections associated with drinking unpasteurized milk --- Illinois, Indiana, Ohio, and Tennessee, 2002–2003. *MMWR, Morb. Mortal. Wkly. Rep.* **52**(56), 613–615.
14. CDC. (2007). Multistate outbreak of *Salmonella* serotype *tennessee* Infections associated with peanut butter --- United States, 2006–2007. *MMWR, Morb. Mortal. Wkly. Rep.* **56**, 521–524.
15. *CDC broadens its investigation of Salmonella outbreak, in USA Today, 2008-06-30*.
16. Lazcka, O., Campo, F. J. D., and Muñoz, F. X. (2007). Pathogen detection: a perspective of traditional methods and biosensors. *Biosens. Bioelectron.* **22**, 1205–1217.
17. Ruiz, J., Nunez, M. L., Diaz, J., Lorente, I., Perez, J., and Gomez, J. (1996). Comparison of five plating media for isolation of *Salmonella* species from human stools. *J. Clin. Microbiol.* **34**, 686–688.
18. Perry, J. D., Ford, M., Taylor, J., Jones, A. L., Freeman, R., and Gould, F. K. (1999). ABC medium, a new chromogenic agar for selective isolation of *Salmonella* spp. *J. Clin. Microbiol.* **37**, 766–768.

19. Perry, J. D., Riley, G., Gould, F. K., Perez, J. M., Boissier, E., Ouedraogo, R. T., and Freydiere, A. M. (2002). Alafosfalin as a selective agent for isolation of *Salmonella* from clinical samples. *J. Clin. Microbiol.* **40**, 3913–3916.
20. Mullis, K. B., and Faloona, F. A. (1987). Specific synthesis of DNA *in vitro* via a polymerase-catalyzed chain-reaction. *Methods Enzymol.* **155**, 335–350.
21. Higgins, J. A., Nasarabadi, S., Karns, J. S., Shelton, D. R., Cooper, M., Gbakima, A., and Koopman, R. P. (2003). A handheld real time thermal cycler for bacterial pathogen detection. *Biosens. Bioelectron.* **18**, 1115–1123.
22. Woof, J. M., and Burton, D. R. (2004). Human antibody-Fc receptor interactions illuminated by crystal structures. *Nat. Rev. Immunol.* **4**, 89–99.
23. Bej, A. K., Mahbubani, M. H., Dicesare, J. L., and Atlas, R. M. (1991). Polymerase chain reaction-gene probe detection of microorganisms by using filter-concentrated samples. *Appl. Environ. Microbiol.* **57**, 3529–3534.
24. Leoni, E., and Legnani, P. P. (2000). Comparison of selective procedures for isolation and enumeration of Legionella species from hot water systems. *J. Appl. Microbiol.* **90**, 27–33.
25. Alocilja, E. C., and Radke, S. M. (2003). Market analysis of biosensors for food safety. *Biosens. Bioelectron.* **18**, 841–846.
26. Gooding, J. J. (2006). Biosensor technology for detecting biological warfare agents: recent progress and future trends. *Anal. Chim. Acta* **559**, 137–151.
27. Brooks, B. W., Devenish, J., Lutze-Wallace, C. L., Milnes, D., Robertson, R. H., and Berlie-Surujballi, G. (2004). Evaluation of a monoclonal antibody-based enzyme-linked immunosorbent assay for detection of *Campylobacter fetus* in bovine preputial washing and vaginal mucus samples. *Vet. Microbiol.* **103**, 77–84.
28. Villari, P., Motti, E., Farullo, C., and Torre, I. (1998). Comparison of conventional culture and PCR methods for the detection of *Legionella pneumophila* in water. *Lett. Appl. Microbiol.* **27**, 106–110.
29. Scotter, S. L., Langton, S., Lombard, B., Schulten, S., Nagelkerke, N., Veld, P. H. I., Rollier, P., and Lahellec, C. (2001). Validation of ISO method 11290 Part 1 Detection of *Listeria monocytogenes* in foods. *Int. J. Food Microbiol.* **64**, 295–306.
30. Churchill, R. L. T., Lee, H., and Hall, J. C. (2006). Detection of *Listeria monocytogenes* and the toxin listeriolysin O in food. *J. Microbiol. Methods* **64**, 141–170.
31. Wagner, M., Moore, A., and Aryel, R. (2006). *Handbook of Biosurveillance*. Academic Press, San Diego, CA.
32. Lequin, R. M. (2005). Enzyme immunoassay (EIA)/enzyme-linked immunosorbent assay (ELISA). *Clin. Chem.* **51**, 2415–2418.
33. Bahna, S. L. (1988). Diagnostic tests for food allergy. *Clin. Rev. Allergy* **6**, 259–284.
34. Peruski, A. H., and Peruski, L. F. Jr. (2003). Immunological methods for detection and identification of infectious disease and biological warfare agents. *Clin. Diagn. Lab. Immunol.* **10**, 506–513.
35. Mansfield, L. P., and Forsythe, S. J. (2001). The detection of *Salmonella* serovars from animal feed and raw chicken using a combined immunomagnetic separation and ELISA method. *Food Microbiol.* **18**, 361–366.
36. Crowley, E. L., O'Sullivan, C. K., and Guilbault, G. G. (1999). Increasing the sensitivity of Listeria monocytogenes assays: evaluation using ELISA and amperometric detection. *Analyst* **124**, 295–299.
37. Croci, L., Delibato, E., Volpe, G., and Palleschi, G. (2001). A rapid electrochemical ELISA for the detection of *Salmonella* in meat samples. *Anal. Lett.* **34**(15), 2597–2607.

38. Blais, B. W., Leggate, J., Bosley, J., and Martinez-Perez, A. (2004). Comparison of fluorogenic and chromogenic assay systems in the detection of *Escherichia coli* O157 by a novel polymyxin-based ELISA. *Lett. Appl. Microbiol.* **39**, 516–522.
39. Sambrook, J., and Russel, D. W. (2001). *Molecular Cloning: A Laboratory Manual*, 3rd ed. Cold Spring Harbor Laboratory Press, Cold Spring Harbor, NY.
40. http://www.horizonpress.com/pcr/.
41. Lund, M., Nordentoft, S., Pedersen, K., and Madsen, M. (2004). Detection of *Campylobacter* spp. in chicken fecal samples by real-time PCR. *J. Clin. Microbiol.* **42**, 5125–5132.
42. Fu, Z., Rogelj, S., and Kieft, T. L. (2005). Detection of *Escherichia coli* 0157:H7 by immuno-magnetic separation and real-time PCR. *Int. J. Food Microbiol.* **99**, 47–57.
43. Castanha, E. R., Swiger, R. R., Senior, B., Fox, A., Waller, L. N., and Fox, K. F. (2006). Strain discrimination among *B. anthracis* and related organisms by characterization of bclA polymorphisms using PCR coupled with agarose gel or microchannel fluidics electrophoresis. *J. Microbiol. Methods* **64**, 27–45.
44. Jensen, G. B., Fisker, N., Sparso, T., and Andrup, L. (2005). The possibility of discriminating within the *Bacillus cereus* group using gyrB sequencing and PCR-RFLP. *Int. J. Food Microbiol.* **104**, 113–120.
45. Reiman, R. W., Atchley, D. H., and Voorhees, K. J. (2007). Indirect detection of *Bacillus anthracis* using real-time PCR to detect amplified gamma phage DNA. *J. Microbiol. Methods* **68**, 651–653.
46. Klein, P. G., and Juneja, V. K. (1997). Sensitive detection of viable *Listeria monocytogenes* by reverse transcription-PCR. *Appl. Environ. Microbiol.* **63**(11), 4441–4448.
47. Daly, P., Collier, T., and Doyle, S. (2002). PCR-ELISA detection of *Escherichia coli* in milk. *Lett. Appl. Microbiol.* **34**, 222–226.
48. Higgins, J. A., Nasarabadi, S., Karns, J. S., Shelton, D. R., Cooper, M., Gbakima, A., and Koopman, R. P. (2003). A handheld real time thermal cycler for bacterial pathogen detection. *Biosens. Bioelectron.* **18**, 1115–1126.
49. Wan, J., King, K., Forsyth, S., and Coventry, M. J. (2003). Detection of *Listeria monocytogenes* in salmon using Probelia polymerase chain reaction system. *J. Food Prot.* **66**, 436–440.
50. Wolffs, P., Knutsson, R., Norling, B., and Radstrom, P. (2004). Rapid quantification of *Yersinia enterocolitica* in pork samples by a novel sample preparation method, flotation, prior to real-time PCR. *J. Clin. Microbiol.* **42**(3), 1042–1047.
51. Perelle, S., Dilasser, F., Malorny, B., Grout, J., Hoorfar, J., and Fach, P. (2004). Comparison of PCR-ELISA and LightCycler real-time PCR assays for detecting *Salmonella* spp. in milk and meat samples. *Mol. Cell. Probes* **18**, 409–420.
52. Lund, M., Nordentoft, S., Pedersen, K., and Madsen, M. (2004). Detection of *Campylobacter* spp. in chicken fecal samples by real-time PCR. *J. Clin. Microbiol.* **42**(11), 5125–5132.
53. Fey, A., Eichler, S., Flavier, S., Christen, R., Hofle, M. G., and Guzman, C. A. (2004). Establishment of a real-time PCR-Based approach for accurate quantification of bacterial RNA targets in water, using *Salmonella* as a model organism. *Appl. Environ. Microbiol.* **70**(6), 3618–3623.
54. Nguyen, T. V., Van, P. L., Huy, C. L., Gia, K. N., and Weintraub, A. (2005). Detection and characterization of diarrheagenic *Escherichia coli* from young children in Hanoi, Vietnam. *J. Clin. Microbiol.* **43**(2), 755–760.
55. Kim, J.-Y., Kim, S.-H., Kwon, N.-H., Bae, W.-K., Lim, J.-Y., Koo, H.-C., Kim, J.-M., Noh, K.-M., Jung, W.-K., Park, K.-T., and Park, Y.-H. (2005). Isolation and identification of *Escherichia coli* O157:H7 using different detection methods and molecular determination by multiplex PCR and RAPD. *J. Vet. Sci.* **6**(1), 7–19.

56. Fu, Z., Rogelj, S., and Kieft, T. L. (2005). Rapid detection of *Escherichia coli* O157:H7 by immunomagnetic separation and real-time PCR. *Int. J. Food Microbiol.* **99**, 47–57.
57. Kim, S., Frye, J. G., Hu, J., Fedorka-Cray, P. J., Gautom, R., and Boyle, D. S. (2006). Multiplex PCR-Based method for identification of common clinical serotypes of *Salmonella enterica* subsp. *enterica*. *J. Clin. Microbiol.* **44**(10), 3608–3615.
58. Nayak, A. K., and Rose, J. B. (2007). Detection of *Helicobacter pylori* in sewage and water using a new quantitative PCR method with SYBR green. *J. Appl. Microbiol.* **103**, 1931–1941.
59. Brightwell, G., Mowat, E., Clemens, R., Boerema, J., Pulford, D. J., and On, S. L. (2007). Development of a multiplex and real time PCR assay for the specific detection of *Arcobacter butzleri* and *Arcobacter cryaerophilus*. *J. Microbiol. Methods* **68**, 318–325.
60. Schonenbrucher, H., Abdulmawjood, A., Failing, K., and Bulte, M. (2008). New triplex real-time PCR assay for detection of *Mycobacterium avium* subsp. paratuberculosis in bovine feces. *Appl. Environ. Microbiol.* **74**(9), 2751–2758.
61. Mendes, C. L., Abath, F. G. C., and Leal, N. C. (2008). Development of a multiplex single-tube nested PCR (MSTNPCR) assay for *Vibrio cholerae* O1 detection. *J. Microbiol. Methods* **72**, 191–196.
62. Cavalcanti, A., Shirinzadeh, B., Zhang, M., and Kretly, L. C. (2008). Nanorobot hardware architecture for medical defense. *Sensors* **8**, 2932–2958.
63. Leonard, P., Hearty, S., Brenan, J., Dunne, L., Quinn, J., Chakraborty, T., and O'Kennedy, R. (2003). Advances in biosensors for detection of pathogens in food and water. *Enzyme Microb. Technol.* **32**, 3–13.
64. Chambers, J. P., Arulanandam, B. P., Matta, L. L., Weis, A., and Valdes, J. J. (2008). Biosensor recognition elements. *Curr. Issues Mol. Biol.* **10**, 1–12.
65. Highfield, P. E., and Dougan, G. (1985). DNA probes for microbial diagnosis. *Med. Lab. Sci.* **42**, 352–360.
66. Kapperud, G., Vardund, T., Skjerve, E., Hornes, E., and Michaelsen, T. E. (1993). Detection of pathogenic *Yersinia enterocolitica* in foods and water by immunomagnetic separation, nested polymerase chain-reactions, and colorimetric detection of amplified DNA. *Appl. Environ. Microbiol.* **59**, 2938–2944.
67. Zhai, J. H., Cui, H., and Yang, R. F. (1997). DNA based biosensors. *Biotechnol. Adv.* **15**, 43–58.
68. Song, S. P., Wang, L. H., Li, J., Zhao, J. L., and Fan, C. H. (2008). Aptamer-based biosensors. *TrAC, Trends Anal. Chem.* **27**, 108–117.
69. Liss, M., Petersen, B., Wolf, H., and Prohaska, E. (2002). An aptamer-based quartz crystal protein biosensor. *Anal. Chem.* **74**, 4488–4495.
70. Minunni, M., Tombelli, S., Gullotto, A., Luzi, E., and Mascini, M. (2004). Development of biosensors with aptamers as bio-recognition element: the case of HIV-1 Tat protein. *Biosens. Bioelectron.* **20**, 1149–1156.
71. Gronewold, T. M. A., Glass, S., Quandt, E., and Famulok, A. (2005). Monitoring complex formation in the blood-coagulation cascade using aptamer-coated SAW sensors. *Biosens. Bioelectron.* **20**, 2044–2052.
72. Litman, G. W., Rast, J. P., Shamblott, M. J., Haire, R. N., Hulst, M., Roess, W., Litman, R. T., Hinds- Frey, K. R., Zilch, A., and Amemiya, C. T. (1993). Phylogenetic diversification of immunoglobulin genes and the antibody repertoire. *Mol. Biol. Evol.* **10**, 60–72.
73. Kabir, S. (2002). Immunoglobulin purification by affinity chromatography using protein A mimetic ligands prepared by combinatorial chemical synthesis. *Immunol. Invest.* **31**, 263–278.
74. Skottrup, P. D., Nicolaisen, M., and Justesen, A. F. Towards on-site pathogen detection using antibody-based sensors. *Biosens. Bioelectron.*, In Press, Corrected Proof.

75. Fratamico, P. M., Strobaugh, T. P., Medina, M. B., and Gehring, A. G. (1998). Detection of *Escherichia coli* 0157:H7 using a surface plasmon resonance biosensor. *Biotechnol. Tech.* **12**, 571–576.
76. Bergwerff, A. A., and Van Knapen, F. (2006). Surface plasmon resonance biosensors for detection of pathogenic microorganisms: strategies to secure food and environmental safety. *J. AOAC Int.* **89**, 826–831.
77. Leonard, P., Hearty, S., Quinn, J., and O'Kennedy, R. (2004). A generic approach for the detection of whole *Listeria monocytogenes* cells in contaminated samples using surface plasmon resonance. *Biosens. Bioelectron.* **19**, 1331–1335.
78. Lee, S. H., Stubbs, D. D., Cairney, J., and Hunt, W. D. (2005). Rapid detection of bacterial spores using a quartz crystal microbalance (QCM) immunoassay. *IEEE Sens. J.* **5**, 737–743.
79. Vaughan, R. D., Carter, R. M., O'Sullivan, C. K., and Guilbault, G. G. (2003). A quartz crystal microbalance (QCM) sensor for the detection of *Bacillus cereus*. *Anal. Lett.* **36**, 731–747.
80. Prescott, L. (1993). *Microbiology*. Wm. C. Brown Publishers.
81. Kutter, E., and Sulankvelidze, A. (2004). *Bacteriophages: Biology and Application*. CRC Press.
82. Grath, S. M., and Sinderen, D. (2007). *Bacteriophage: Genetics and Molecular Biology*, 1st ed. Caister Academic Press.
83. Ackermann, H.-W. (1999). Tailed bacteriophages. The order caudoviurales. *Adv. Virus Res.* **51**, 135–201.
84. Ackermann, H.-W. (2001). Frequency of morphological phage descriptions in the year 2000. *Arch. Virol.* **146**, 843–857.
85. Martin, C. (1988). The application of bacteriophage tracer techniques in southwest water. *Water Environ. J.* **2**, 638–642.
86. *U.S. FDA/CFSAN: Agency Response Letter: GRAS Notice No. GRN 000198*.
87. Mosier-Boss, P. A., Lieherman, S. H., Andrews, J. M., Rohwer, F. L., Wegley, L. E., and Breitbart, M. (2003). Use of fluorescently labeled phage in the detection and identification of bacterial species. *Appl. Spectrosc.* **57**, 1138–1144.
88. McCafferty, J., Griggiths, A. D., Winter, G., and Chiswell, D. J. (1990). Phage antibodies: filamentous phage displaying antibody variable domains. *Nature* **348**, 552–554.
89. Barbas, C. F., Kang, A. S., Lerner, R. A., and Benkovic, S. J. (1991). Assembly of combinatorial antibody libraries on phage surfaces: the gene III site. *Proc. Natl. Acad. Sci. U.S.A.* **88**, 7978–7982.
90. Emanuel, P. A., Dang, J., Gebhardt, J. S., Aldrich, J., Garber, E. A., Hulaga, H., Stopa, P., Valdes, J. J., and Dion-Schultz, A. (2000). Recombinant antibodies: anew reagent for biological agent detection. *Biosens. Bioelectron.* **14**, 751–759.
91. Jasmin Shah, E. W. (2003). Electrochemical biosensors for detection of biological warfare agents. *Electroanalysis* **15**, 157–167.
92. Mello, L. D., and Kubota, L. T. (2002). Review of the use of biosensors as analytical tools in food and drink industries. *Food Chem.* **77**, 237–256.
93. Sukeerthi, S., and Contractor, A. Q. (1994). Applications of conducting polymers as sensors. *Ind. J. Chem.* **33A**, 565–571.
94. Gerard, M., Chaubey, A., and Malhotra, B. D. (2002). Application of conducting polymers to biosensors. *Biosens. Bioelectron.* **17**, 345–359.
95. DeSilva, M. S., Zhang, Y., Hesketh, P. J., Maclay, G. J., Gendel, S. M., and Stetter, J. R. (1995). Impedance based sensing of the specific binding reaction between Staphylococcus enterotoxin B and its antibody on an ultra-thin platinum film. *Biosens. Bioelectron.* **10**, 675–682.

96. Ivnitski, D., Abdel-Hamid, I., Atanasov, P., and Wilkins, E. (1999). Biosensors for detection of pathogenic bacteria. *Biosens. Bioelectron.* **14**, 599–625.
97. Mirhabibollahi, B., Brooks, J. L., and Kroll, R. G. (1990). A semi-homogeneous amperometric immunosensor for protein A-bearing *Staphylococcus aureus* in foods. *Appl. Microbiol. Biotechnol.* **34**, 242–247.
98. Brooks, J. L., Mirhabibollahi, B., and Kroll, R. G. (1990). Sensitive enzyme-amplified electrical immunoassay for protein A-bearing *Staphylococcus aureus* in foods. *Appl. Environ. Microbiol.* **56**, 3278–3284.
99. Brewster, J. D., Gehring, A. G., Mazenko, R. S., Van Houten, L. J., and Crawford, C. J. (1996). Immunoelectrochemical assays for bacteria: use of epifluorescence microscopy and rapid-scan electrochemical techniques in development of an assay for *Salmonella*. *Anal. Chem.* **68**, 4153–4159.
100. Nakamura, N., Shigematsu, A., and Matsunaga, T. (1991). Electrochemical detection of viable bacteria in urine and antibiotic selection. *Biosens. Bioelectron.* **6**, 575–580.
101. Abdel-Hamid, I., Ivnitski, D., Atanasov, P., and Wilkins, E. (1999). Flow-through immunofiltration assay system for rapid detection of *E. coli* O157:H7. *Biosens. Bioelectron.* **14**, 309–316.
102. Ghindilis, A. L., Atanasov, P., Wilkins, M., and Wilkins, E. (1998). Immunosensors: electrochemical sensing and other engineering approaches. *Biosens. Bioelectron.* **13**, 113–131.
103. Brewster, J. D., Gehring, A. G., Mazenko, R. S., Houten, L. J. V., and Crawford, C. J. (1996). Immunoelectrochemical assays for bacteria: Use of epifluorescence microscopy and rapid-scan electrochemical techniques in development of an assay for *Salmonella*. *Anal. Chem.* **68**(23), 4153–4159.
104. Edmiston, A. L., and Russell, S. M. (1998). A rapid microbiological method for enumerating *Escherichia coli* from broiler chicken carcasses. *J. Food Prot.* **61**, 1375–1377.
105. Dill, K., Stanker, L. H., and Young, C. R. (1999). Detection of *Salmonella* in poultry using a silicon chip-based biosensor. *J. Biochem. Biophys. Methods* **41**, 61–67.
106. Che, Y. H., Li, Y., Slavik, M., and Paul, D. (2000). Rapid detection of *Salmonella typhimurium* in chicken carcass wash water using an immunoelectrochemical method. *J. Food Prot.* **63**, 1043–1048.
107. Ruan, C., Yang, L., and Li, Y. (2002). Immunobiosensor chips for detection of *Escherichia coli* O157:H7 using electrochemical impedance spectroscopy. *Anal. Chem.* **74**(18), 4814–4820.
108. Yang, L., and Li, Y. (2006). Detection of viable *Salmonella* using microelectrode-based capacitance measurement coupled with immunomagnetic separation. *J. Microbiol. Methods* **64**, 9–16.
109. Suehiro, J., Hatano, T., Shutou, M., and Hara, M. (2005). Improvement of electric pulse shape for electropermeabilization assisted dielectrophoretic impedance measurement for high sensitive bacteria detection. *Sens. Actuators, B* **109**, 209–215.
110. Gomez-Sjoberg, R., Morisette, D. T., and Bashir, R. (2005). Impedance microbiology-on-a-chip: microfluidic bioprocessor for rapid detection of bacterial metabolism. *J. Microelectromech. Syst.* **14**(4), 829–838.
111. Radke, S. M., and Alocilja, E. C. (2005). A high density microelectrode array biosensor for detection of *E. coli* O157:H7. *Biosens. Bioelectron.* **20**, 1662–1667.
112. Chemburua, S., Wilkinsa, E., and Abdel-Hamidb, I. (2005). Detection of pathogenic bacteria in food samples using highly-dispersed carbon particles. *Biosens. Bioelectron.* **21**, 491–499.
113. Sengupta, S., Battigelli, D. A., and Chang, H. C. (2006). A micro-scale multi-frequency reactance measurement technique to detect bacterial growth at low bio-particle concentrations. *Lab Chip* **6**, 682–692.

114. Delibato, E., Volpe, G., Stangalini, D., Medici, D. D., Moscone, D., and Palleschi, G. (2006). Development of SYBR-Green real-time PCR and a multichannel electrochemical immunosensor for specific detection of *Salmonella enterica*. *Anal. Lett.* **39**, 1611–1625.

115. Varshney, M., Li, Y., Srinivasan, B., and Tung, S. (2007). A label-free, microfluidics and interdigitated array microelectrode-based impedance biosensor in combination with nanoparticles immunoseparation for detection of *Escherichia coli* O157:H7 in food samples. *Sens. Actuators, B* **128**, 99–107.

116. Varshney, M., and Li, Y. (2008). Double interdigitated array microelectrode-based impedance biosensor for detection of viable *Escherichia coli* O157:H7 in growth medium. *Talanta* **74**, 518–525.

117. Theegala, C. S., Small, D. D., and Monroe, W. T. (2008). Oxygen electrode-based single antibody amperometric biosensor for qualitative detection of *E. coli* and bacteria in water. *J. Environ. Sci. Health, Part A* **43**(5), 478–487.

118. Tully, E., Higson, S. P., and O'Kennedy, R. (2008). The development of a 'labeless' immunosensor for the detection of *Listeria monocytogenes* cell surface protein, Internalin B. *Biosens. Bioelectron.* **23**, 906–912.

119. Turner, A. P. F., Karube, I., and Wilson, G. S. (1992). *Biosensors: Fundamentals and Applications*. Mir Publishers, Moscow.

120. Mulchandani, A., and Rogers, K. R. (1998). *Enzyme and Micriobial Biosensors: Techniques and Protocols*. Humana Press, Totowa, NJ.

121. Tran, M. C. (1993). *Biosensors*. Chapman and Hall and Masson, Paris.

122. Mikkelsen, S. R., and Cortón, E. (2004). *Bioanalytical Chemistry*. John Wiley and Sons, Hoboken , NJ.

123. Blum, L. J., and Coulet, P. R. (1991). *Biosensor Principles and Applications*. Marcel Dekker, New York.

124. Sethi, R. S. (1994). Transducer aspects of biosensors. *Biosens. Bioelectron.* **9**, 243–264.

125. Xu, Z., Mulchandani, A., and Chen, W. (2003). Detection of benzene, toluene, ethyl benzene, and xylenes (BTEX) using toluene dioxygenase-peroxidase coupling reactions. *Biotechnol. Prog.* **19**, 1812–1815.

126. Naimushin, A. N., Spinelli, C. B., Soelberg, S. D., Mann, T., Stevens, R. C., Chinowsky, T., Kauffman, P., Yee, S., and Furlong, C. E. (2005). Airborne analyte detection with an aircraft-adapted surface plasmon resonance sensor system. *Sens. Actuators, B Chem.* **104**, 237–248.

127. Homola, J., Yee, S. S., and Gauglitz, G. (1999). Surface plasmon resonance sensors: review. *Sens. Actuators, B Chem.* **54**, 3–15.

128. Schneider, B. H., Edwards, J. G., and Hartman, N. F. (1997). Hartman interferometer: versatile integrated optic sensor for label-free, real-time quantification of nucleic acids, proteins, and pathogens. *Clin. Chem.* **43**(9), 1757–1763.

129. Zhou, C., Pivarnik, P., Auger, S., Rand, A., and Letcher, S. (1997). A compact fiber-optic immunosensor for *Salmonella* based on evanescent wave excitation. *Sens. Actuators, B* **42**, 169–175.

130. Fratamico, P. M., Strobaugh, T. P., Medina, M. B., and Gehring, A. G. (1998). Detection of *Escherichia coli* O157:H7 using a surface plasmon resonance biosensor. *Biotechnol. Tech.* **12**(7), 571–576.

131. Ilic, B., Czaplewski, D., Craigheada, H. G., Neuzil, P., Campagnolo, C., and Batt, C. (2000). Mechanical resonant immunospecific biological detector. *Appl. Phys. Lett.* **77**, 450–452.

132. Ilic, B., Czaplewski, D., Zalalutdinov, M., Craighead, H. G., Neuzil, P., Campagnolo, C., and Batt, C. (2001). Single cell detection with micromechanical oscillators. *J. Vac. Sci. Technol., B* **19**(6), 2825–2828.

133. Oh, B.-K., Kim, Y.-K., Lee, W., Bae, Y. M., Lee, W. H., and Choi, J.-W. (2003). Immunosensor for detection of *Legionella pneumophila* using surface plasmon resonance. *Biosens. Bioelectron.* **18**, 605–611.

134. Bokken, G. C. A. M., Corbee, R. J., van Knapen, F., and Bergwerff, A. A. (2003). Immunochemical detection of *Salmonella* group B, D and E using an optical surface plasmon resonance biosensor. *FEMS Microbiol. Lett.* **222**, 75–82.

135. Lathrop, A. A., Jaradat, Z. W., Haley, T., and Bhunia, A. K. (2003). Characterization and application of a *Listeria monocytogenes* reactive monoclonal antibody C11E9 in a resonant mirror biosensor. *J. Immunol. Methods* **281**, 119–128.

136. Oh, B.-K., Kim, Y.-K., Park, K. W., Lee, W. H., and Choi, J.-W. (2004). Surface plasmon resonance immunosensor for the detection of *Salmonella typhimurium*. *Biosens. Bioelectron.* **19**, 1497–1504.

137. Geng, T., Morgan, M. T., and Bhunia, A. K. (2004). Detection of low levels of *Listeria monocytogenes* cells by using a fiber-optic immunosensor. *Appl. Environ. Microbiol.* **70**, 6138–6146.

138. Taylor, A. D., Yu, Q., Chen, S., Homol, J., and Jiang, S. (2005). Comparison of *E. coli* O157:H7 preparation methods used for detection with surface plasmon resonance sensor. *Sens. Actuators, B* **107**, 202–208.

139. Bae, Y. M., Park, K.-W., Oh, B.-K., Lee, W. H., and Choi, J.-W. (2005). Immunosensor for detection of *Salmonella typhimurium* based on imaging ellipsometry. *Colloids Surf. A, Physicochem. Eng. Asp.* **257–258**, 19–23.

140. Mazumdar, S. D., Hartmann, M., Kampfer, P., and Keusgen, M. (2007). Rapid method for detection of *Salmonella* in milk by surface plasmon resonance (SPR). *Biosens. Bioelectron.* **22**, 2040–2046.

141. Waswa, J. W., Debroy, C., and Irudayaraj, J. (2006). Rapid detection of *Salmonella enteritidis* and *Escherichia coli* using surface plasmon resonance biosensor. *J. Food Process Eng.* **29**, 373–385.

142. Hearty, S., Leonard, P., Quinn, J., and O'Kennedy, R. (2006). Production, characterisation and potential application of a novel monoclonal antibody for rapid identification of virulent *Listeria monocytogenes*. *J. Microbiol. Methods* **66**, 294–312.

143. Taylor, A. D., Ladda, J., Yu, Q., Chena, S., Homola, J., and Jiang, S. (2006). Quantitative and simultaneous detection of four foodborne bacterial pathogens with a multi-channel SPR sensor. *Biosens. Bioelectron.* **22**, 752–758.

144. Geng, T., Uknalis, J., Tu, S.-I., and Bhunia, A. K. (2006). Fiber-optic biosensor employing alexa-fluor conjugated antibody for detection of *Escherichia coli* O157:H7 from ground beef in four hours. *Sensors* **6**, 796–807.

145. Nanduri, V., Kim, G., Morgan, M. T., Ess, D., Hahm, B.-K., Kothapalli, A., Valadez, A., Geng, T., and Bhunia, A. K. (2006). Antibody immobilization on waveguides using a flow-through system shows improved *Listeria monocytogenes* detection in an automated fiber optic biosensor: RAPTOR. *Sensors* **6**, 808–822.

146. Ko, S., and Grant, S. A. (2006). A novel FRET-based optical fiber biosensor for rapid detection of *Salmonella typhimurium*. *Biosens. Bioelectron.* **21**, 1283–1290.

147. Waswa, J., Irudayaraj, J., and DebRoy, C. (2007). Direct detection of *E. coli* O157:H7 in selected food systems by a surface plasmon resonance biosensor. *LWT* **40**, 187–192.

148. Wei, D., Oyarzabal, O. A., Huang, T.-S., Balasubramanian, S., Sista, S., and Simonian, A. L. (2007). Development of a surface plasmon resonance biosensor for the identification of *Campylobacter jejuni*. *J. Microbiol. Methods* **69**, 78–85.

149. Ligler, F. S., Sapsford, K. E., Golden, J. P., Shriver-Lake, L. C., Taitt, C. R., Dyer, M. A., Barone, S., and Myatt, C. J. (2007). The array biosensor: portable, automated systems. *Anal. Sci.* **23**, 5–10.

150. Ramachandran, A., Wang, S., Clarke, J., Ja, S. J., Goad, D., Wald, L., Flood, E. M., Knobbe, E., Hryniewicz, J. V., Chu, S. T., Gill, D., Chen, W., King, O., and Little, B. E. (2008). A universal biosensing platform based on optical micro-ring resonators. *Biosens. Bioelectron.* **23**, 939–944.

151. Ballantine, D. S., White, R. M., Martin, S. J., Ricco, A. J., Frye, G. C., Zellers, E. T., and Wohltjen, H. (1997). *Acoustic Wave Sensors: Theory, Design and Physico-Chemical Applications*. Academic Press.

152. Hummel, R. E. (2001). *Electronic Properties of Materials*, 3rd ed. Springer-Verlag Inc., New York.

153. Auld, B. A. (1973). *Acoustic Fields and Waves in Solids*. Wiley, New York.

154. Lavrik, N. V., Sepaniak, M. J., and Datskos, P. G. (2004). Cantilever transducers as a platform for chemical and biological sensors. *Rev. Sci. Instrum.* **75**, 2229–2253.

155. Thundat, T., Oden, P. I., and Warmack, R. J. (1997). Microcantilever sensors. *Microscale Thermophys. Eng.* **1**, 185–199.

156. Sauerbrey, G. Z. (1959). The use of quartz oscillators for weighing thin layers and for microweighing. *Physik* **155**, 206–222.

157. Kipling, A. L., and Thompson, M. (1990). Network analysis method applied to liquid-phase acoustic wave sensors. *Anal. Chem.* **62**, 1514–1519.

158. Rajakovic, L. V., Cavic-Vlasak, B. A., Ghaemmaghami, V., Kallury, K. M. R., Kipling, A. L., and Thompson, M. (1991). Mediation of acoustic energy transmission from acoustic wave sensors to the liquid phase by interfacial viscosity. *Anal. Chem.* **63**, 615–621.

159. Olsen, E. V., Sorokulova, I. B., Petrenko, V. A., Chen, I. H., Barbaree, J. M., and Vodyanoy, V. J. (2006). Affinity-selected filamentous bacteriophage as a probe for acoustic wave biodetectors of *Salmonella typhimurium*. *Biosens. Bioelectron.* **21**, 1434–1442.

160. Pathirana, S. T., Barbaree, J., Chin, B. A., Hartell, M. G., Neely, W. C., and Vodyanoy, V. (2000). Rapid and sensitive biosensor for *Salmonella*. *Biosens. Bioelectron.* **15**, 135–141.

161. Su, X., Low, S., Kwang, J., Chew, V. H. T., and Li, S. F. Y. (2001). Piezoelectric quartz crystal based veterinary diagnosis for *Salmonella enteritidis* infection in chicken and egg. *Sens. Actuators, B Chem.* **75**, 29–35.

162. Drafts, B. (2001). Acoustic wave technology sensors. *IEEE Trans. Microw. Theory Tech.* **49**, 795–802.

163. Rayleigh, L. (1885). On waves propagated along the plane surface of an elastic solid. *Proc. London Math. Soc.* **17**, 4–11.

164. White, R. M. (1970). Surface elastic waves. *Proc. IEEE* **58**, 1238–1276.

165. Hierlemann, A., and Baltes, H. (2003). CMOS-based chemical microsensors. *Analyst* **128**, 15–28.

166. Binnig, G., Quate, C. F., and Gerber, C. (1986). Atomic force microscope. *Phys. Rev. Lett.* **56**, 930.

167. Thundat, T., and Warmack, R. J. (1994). Thermal and ambient-induced deflections of scanning force microscope cantilevers. *Appl. Phys. Lett.* **64**, 2894.

168. Barnes, J. R., Stephenson, R. J., Welland, M. E., Gerber, C., and Gimzewski, J. K. (1994). Photothermal spectroscopy with femtojoule sensitivity using a micromechanical device. *Nature* **372**, 79–81.

169. Benes, E., Gröschl, M., Burger, W., and Schmid, M. (1995). Sensors based on piezoelectric resonators. *Sens. Actuators, A Phys.* **48**, 1–21.

170. Thundat, T., Chen, G. Y., Warmack, R. J., Allison, D. P., and Wachter, E. A. (1995). Vapor detection using resonating microcantilevers. *Anal. Chem.* **67**, 519–521.

171. Wachter, E. A., and Thundat, T. (1995). Micromechanical sensors for chemical and physical measurements. *Rev. Sci. Instrum.* **66**, 3662–3671.

172. Datskos, P. G., and Sauers, I. (1999). Detection of mercaptoethanol using gold-coated micromachined cantilevers,. *Sens. Actuators, B Chem.* **61**, 75–82.

173. Boisen, A., Thaysen, J., Jensenius, H., and Hansen, O. (2000). Environmental sensors based on micromachined cantilevers with integrated read-out. *Ultramicroscopy* **82**, 11–16.

174. Hansen, K. M., Ji, H.-F., Wu, G., Datar, R., Cote, R., Majumdar, A., and Thundat, T. (2001). Cantilever-based optical deflection assay for discrimination of DNA single-nucleotide mismatches. *Anal. Chem.* **73**, 1567–1571.

175. McGovern, J.-P., Shih, W. Y., and Shiha, W.-H. (2007). In situ detection of Bacillus anthracis spores using fully submersible, self-exciting, self-sensing PMN-PT/Sn piezoelectric microcantilevers. *Analyst* **132**, 777–783.

176. Zhu, Q., Shih, W. Y., and Shih, W.-H. (2007). In-situ, in-water detection of *Salmonella typhimurium* using lead titanate zirconate/gold-coated glass cantilevers at any dipping depth. *Biosens. Bioelectron.* **22**, 3132.

177. Ilic, B., Czaplewski, D., Craighead, H. G., Neuzil, P., Campagnolo, C., and Batt, C. (2000). Mechanical resonant immunospecific biological detector. *Appl. Phys. Lett.* **77**, 450–452.

178. Nickolay, V. L., Michael, J. S., and Panos, G. D. (2004). Cantilever transducers as a platform for chemical and biological sensors. *Rev. Sci. Instrum.* **75**, 2229–2253.

179. Mertz, J., Marti, O., and Mlynek, J. (1993). Regulation of a microcantilever response by force feedback. *Appl. Phys. Lett.* **62**, 2344–2346.

180. Lavrik, N. V., and Datskos, P. G. (2003). Femtogram mass detection using photothermally actuated nanomechanical resonators. *Appl. Phys. Lett.* **82**, 2697.

181. Vashist, S. K. (2007). A review of microcantilevers for sensing applications. *J. Nanotechnol.* **3**, 1–15.

182. Sepaniak, M., Datskos, P., Lavrik, N., and Tipple, C. (2002). Microcantilever transducers: a new approach in sensor technology. *Anal. Chem.* **74**, 568A–575A.

183. Ziegler, C. (2004). Cantilever-based biosensors. *Anal. Bioanal. Chem.* **379**, 946–959.

184. Rugar, D., Mamin, H. J., and Guethner, P. (1989). Improved fiber-optic interferometer for atomic force microscopy. *Appl. Phys. Lett.* **55**, 2588.

185. Ilic, B., Czaplewski, D., Zalalutdinov, M., Craighead, H. G., Neuzil, P., Campagnolo, C., and Batt, C. (2001). Single cell detection with micromechanical oscillators. *J. Vac. Sci. Technol., B* **19**, 2825–2828.

186. Campbell, G. A., and Mutharasan, R. (2008). Near real-time detection of *Cryptosporidium parvum* oocyst by IgM-functionalized piezoelectric-excited millimeter-sized cantilever biosensor. *Biosens. Bioelectron.* **23**, 1039–1045.

187. Campbell, G. A., deLesdernier, D., and Mutharasan, R. (2007). Detection of airborne *Bacillus anthracis* spores by an integrated system of an air sampler and a cantilever immunosensor. *Sens. Actuators, B Chem.* **127**, 376–382.

188. Campbell, G. A., Medina, M. B., and Mutharasan, R. (2007). Detection of *Staphylococcus* enterotoxin B at picogram levels using piezoelectric-excited millimeter-sized cantilever sensors. *Sens. Actuators, B Chem.* **126**, 354–360.

189. Campbell, G. A., Uknalis, J., Tu, S.-I., and Mutharasan, R. (2007). Detect of *Escherichia coli* O157:H7 in ground beef samples using piezoelectric excited millimeter-sized cantilever (PEMC) sensors. *Biosens. Bioelectron.* **22**, 1296–1302.

190. Pyun, J. C., Beutel, H., Meyer, J. U., and Ruf, H. H. (1998). Development of a biosensor for *E. coli* based on a flexural plate wave (FPW) transducer. *Biosens. Bioelectron.* **13**, 839–845.

191. Park, I.-S., Kim, W.-Y., and Kim, N. (2000). Operational characteristics of an antibody-immobilized QCM system detecting *Salmonella* spp. *Biosens. Bioelectron.* **15**, 167–172.

192. Howe, E., and Harding, G. (2000). A comparison of protocols for the optimisation of detection of bacteria using a surface acoustic wave (SAW) biosensor. *Biosens. Bioelectron.* **15**, 641–649.

193. Vaughan, R. D., O'Sullivan, C. K., and Guilbault, G. G. (2001). Development of a quartz crystal microbalance (QCM) immunosensor for the detection of *Listeria monocytogenes*. *Enzyme Microb. Technol.* **29**, 635–638.

194. Kim, N., and Park, I.-S. (2003). Application of a flow-type antibody sensor to the detection of *Escherichia coli* in various foods. *Biosens. Bioelectron.* **18**, 1101–1107.

195. Wong, Y. Y., Ng, S. P., Ng, M. H., Si, S. H., Yao, S. Z., and Fung, Y. S. (2002). Immunosensor for the differentiation and detection of *Salmonella* species based on a quartz crystal microbalance. *Biosens. Bioelectron.* **17**, 676–684.

196. Su, X.-L., and Li, Y. (2004). A self-assembled monolayer-based piezoelectric immunosensor for rapid detection of *Escherichia coli* O157:H7. *Biosens. Bioelectron.* **19**, 563–574.

197. Su, X.-L., and Li, Y. (2005). A QCM immunosensor for *Salmonella* detection with simultaneous measurements of resonant frequency and motional resistance. *Biosens. Bioelectron.* **21**, 840–848.

198. Moll, N., Pascal, E., Dinh, D. H., Pillot, J.-P., Bennetau, B., Rebiere, D., Moynet, D., Mas, Y., Mossalayi, D., Pistre, J., and Dejous, C. (2007). A Love wave immunosensor for whole *E. coli* bacteria detection using an innovative two-step immobilization approach. *Biosens. Bioelectron.* **22**, 2145–2150.

199. Berkenpas, E., Millard, P., and da Cunha, M. P. (2006). Detection of *Escherichia coli* O157:H7 with langasite pure shear horizontal surface acoustic wave sensors. *Biosens. Bioelectron.* **21**, 2255–2262.

200. Petrenko, V. A., Smith, G. P., Gong, X., and Quinn, T. (1996). A library of organic landscapes on filamentous phage. *Protein Eng.* **9**, 797–801.

201. Petrenko, V. A., and Smith, G. P. (2005). Vectors and modes of display. In *Phage Display in Biotechnology and Drug Discovery*, S. S. Sidhu, Ed. CRC Press, Taylor & Francis Group, Bo Raton, FL, p. 714.

202. Smith, G. P., and Petrenko, V. A. (1997). Phage display. *Chem. Rev.* **97**, 391–410.

203. Kehoe, J. W., and Kay, B. K. (2005). Filamentous phage display in the new millennium. *Chem. Rev.* **105**, 4056–4072.

204. Marvin, D. A., Welsh, L. C., Symmons, M. F., Scott, W. R., and Straus, S. K. (2006). Molecular structure of fd (f1, M13) filamentous bacteriophage refined with respect to X-ray fibre diffraction and solid-state NMR data supports specific models of phage assembly at the bacterial membrane. *J. Mol. Biol.* **355**, 294–309.

205. Marvin, D. V. (1998). Filamentous phage structure infection assembly. *Curr. Opin. Struct. Biol.* **8**, 150–158.

206. Petrenko, V. A., and Smith, G. P. (2000). Phages from landscape libraries as substitute antibodies. *Protein Eng.* **13**, 589–592.

207. Petrenko, V. A. (2008). Landscape phage as a molecular recognition interface for detection devices. *Microelectron. J.* **39**, 202–207.

208. Cunningham, A. J. (1998). *Introduction to Bioanalytical Sensors*. Wiley, New York.

209. Nanduri, V., Balasubramania, S., Sista, S., Vodyanoy, V. J., and Simonian, A. L. (2007). Highly sensitive phage-based biosensor for the detection of beta-galactosidase. *Anal. Chim. Acta* **589**, 166–172.

210. Wan, J., Johnson, M. L., Guntupalli, R., Petrenko, V. A., and Chin, B. A. (2007). Detection of *Bacillus anthracis* spores in liquid using phage-based magnetoelastic micro-resonators. *Sens. Actuators, B Chem.* **127**, 559–566.

211. Lakshmanan, R. S., Guntupalli, R., Hu, J., Kim, D.-J., Petrenko, V. A., Barbaree, J. M., and Chin, B. A. (2007). Phage immobilized magnetoelastic sensor for the detection of *Salmonella typhimurium*. *J. Microbiol. Methods* **71**, 55–60.

212. Lakshmanan, R. S., Guntupalli, R., Hu, J., Petrenko, V. A., Barbaree, J. M., and Chin, B. A. (2007). Detection of *Salmonella typhimurium* in fat free milk using a phage immobilized magnetoelastic sensor. *Sens. Actuators, B Chem.* **126**, 544–550.

213. Samoylov, A. M., Samoylova, T. I., Pathirana, S. T., Globa, L. P., and Vodyanoy, V. J. (2002). Peptide biosensor for recognition of cross species cell surface markers. *J. Mol. Recognit.* **15**, 1–7.

214. Olofsson, L., Ankarloo, J., Andersson, P. O., and Nicholls, I. A. (2001). Filamentous bacteriophage stability in non-aqueous media. *Chem. Biol.* **8**, 661–671.

215. Petrenko, V. A., and Vodyanoy, V. J. (2003). Phage display for detection of biological threat agents. *J. Microbiol. Methods* **53**, 253–262.

216. Wan, J., Shu, H., Huang, S., Chen, I.-H., Petrenko, V. A., and Chin, B. A. (2007). Phage-based magnetoelastic wireless biosensors for detecting *Bacillus anthracis* spores. *IEEE Sens. J.* **7**, 470–477.

217. Huang, S., Yang, H., Lakshmanan, R. S., Johnson, M. L., Wan, J., Chen, I. H., Wikle Iii, H. C., Petrenko, V. A., Barbaree, J. M., and Chin, B. A. (2009). Sequential detection of *Salmonella typhimurium* and *Bacillus anthracis* spores using magnetoelastic biosensors. *Biosens. Bioelectron.* **24**, 1730–1736.

218. Yang, L. M. C., Tam, P. Y., Murray, B. J., McIntire, T. M., Overstreet, C. M., Weiss, G. A., and Penner, R. M. (2006). Virus electrodes for universal biodetection. *Anal. Chem.* **78**, 3265–3270.

219. Zhu, H. Y., White, I. M., Suter, J. D., and Fan, X. D. (2008). Phage-based label-free biomolecule detection in an opto-fluidic ring resonator. *Biosens. Bioelectron.* **24**, 461–466.

220. Nanduri, V., Sorokulova, I. B., Samoylov, A. M., Simonian, A. L., Petrenko, V. A., and Vodyanoy, V. (2007). Phage as a molecular recognition element in biosensors immobilized by physical adsorption. *Biosens. Bioelectron.* **22**, 986–992.

221. Huang, S., Yang, H., Lakshmanan, R. S., Johnson, M. L., Chen, I., Wan, J., Wikle, H. C., Petrenko, V. A., Barbaree, J. M., Cheng, Z. Y., and Chin, B. A. (2008). The effect of salt and phage concentrations on the binding sensitivity of magnetoelastic biosensors for *B. anthracis* detection. *Biotechnol. Bioeng.* **101**, 1014–1021.

222. Wan, J. (2008) Development and study of phage-coated magnetoelastic biosensors for the detection of *Bacillus anthracis* sterne spores. *Materials Engineering*, vol. PhD. Auburn University, Auburn, p. 153.

223. Grimes, C. A., and Kouzoudis, D. (2000). Remote query measurement of pressure, fluid-flow velocity, and humidity using magnetoelastic thick-film sensors. *Sens. Actuators, A Phys.* **84**, 205–212.

224. Jain, M. K., Schmidt, S., Ong, K. G., Mungle, C., and Grimes, C. A. (2000). Magnetoacoustic remote query temperature and humidity sensors. *Smart Mater. Struct.* **9**, 502–510.

225. Jain, M. K., Schmidt, S., Mungle, C., Loiselle, K., and Grimes, C. A. (2001). Measurement of temperature and liquid viscosity using magneto-acoustic/magneto-optical sensors. *IEEE Trans. Magn.* **37**, 2767–2769.

226. Ruan, C. M., Zeng, K. F., Varghese, O. K., and Grimes, C. A. (2003). Magnetoelastic immunosensors: amplified mass immunosorbent assay for detection of *Escherichia coli* O157: H7. *Anal. Chem.* **75**, 6494–6498.

227. Shankar, K., Zeng, K. F., Ruan, C. M., and Grimes, C. A. (2005). Quantification of ricin concentrations in aqueous media. *Sens. Actuators, B Chem.* **107**, 640–648.

228. Stoyanov, P. G., and Grimes, C. A. (2000). A remote query magnetostrictive viscosity sensor. *Sens. Actuators, A Phys.* **80**, 8–14.

229. Stoyanov, P. G., and Grimes, C. A. (2000). A remote query magnetostrictive viscosity sensor. *Sens. Actuators* **80**, 8–14.

230. Landau, L. D., and Lifshitz, E. M. (1986). *Theory of Elasticity*. Pergamon Press.

231. Huang, S., Hu, J., Wan, J., Johnson, M. L., Shu, H., and Chin, B. A. (2008). The effect of annealing and gold deposition on the performance of magnetoelastic biosensors. *Mater. Sci. Eng., C* **28**, 380–386.

232. Johnson, M. L., Wan, J. H., Huang, S. C., Cheng, Z. Y., Petrenko, V. A., Kim, D. J., Chen, I. H., Barbaree, J. M., Hong, J. W., and Chin, B. A. (2008). A wireless biosensor using microfabricated phage-interfaced magnetoelastic particles. *Sens. Actuators, A Phys.* **144**, 38–47.

233. Johnson, M. L., LeVar, O., Yoon, S. H., Park, J.-H., Huang, S., Kim, D.-J., Cheng, Z., and Chin, B. A. (2009). Dual-cathode method for sputtering magnetoelastic iron-boron films. *Vacuum* **83**, 958–964.

234. Li, S., Fu, L., Wang, C., Lea, S., Arey, B., Engelhard, M., and Cheng, Z.-Y. (2006). Characterization of microstructure and composition of Fe-B nanobars as biosensor platform. *MRS Proc.* **962E**, 0962–P09–14.

235. Cheng, Z. Y., Li, S. Q., Zhang, K. W., Fu, L. L., and Chin, B. A. (2008). Novel magnetostrictive microcantilever and magnetostrictive nanobars for high performance biological detection. *Adv. Sci. Technol.* **54**, 19–28.

236. Sorokulova, I. B., Olsen, E. V., Chen, I. H., Fiebor, B., Barbaree, J. M., Vodyanoy, V. J., Chin, B. A., and Petrenko, V. A. (2005). Landscape phage probes for *Salmonella typhimurium*. *J. Microbiol. Methods* **63**, 55–72.

237. Brigati, J., Williams, D. D., Sorokulova, I. B., Nanduri, V., Chen, I. H., Turnbough, C. L., and Petrenko, V. A. (2004). Diagnostic probes for *Bacillus anthracis* spores selected from a landscape phage library. *Clin. Chem.* **50**, 1899–1906.

238. Lakshmanan, R. (2008). Phage based biosensors. *Materials Research and Education Center*, Vol. PhD. Auburn University, Auburn.

239. Lakshmanan, R. (2008). Phage based biosensor. *Materials Research and Education Center*, Vol. PhD. Auburn University, Auburn.

240. Guntupalli, R., Lakshmanan, R. S., Hu, J., Huang, T. S., Barbaree, J. M., Vodyanoy, V., and Chin, B. A. (2007). Rapid and sensitive magnetoelastic biosensors for the detection *Salmonella typhimurium* in a mixed microbial population. *J. Microbiol. Methods* **70**, 112–118.

241. Brigati, J. R., and Petrenko, V. A. (2005). Thermostability of landscape phage probes. *Anal. Bioanal. Chem.* **382**, 1346–1350.

242. Guntupalli, R., Lakshmanan, R. S., Wan, J., Kim, D.-J., Huang, T. S., Vodyanoy, V., and Chin, B. A. (2008). Analytical performance and characterization of antibody immobilized magnetoelastic biosensor. *Sens. Instrum. Food Qual.* **2**, 27–33.

243. Huang, S., Li, S. Q., Yang, H., Johnson, M. L., Wan, J., Chen, I., Petrenko, V. A., Barbaree, J., and Chin, B. A. (2008). Optimization of phage-based magnetoelastic biosensor performance. *Spec. Issue Sens. Transducers J. Microsyst. Technol. Appl.* **3**, 87–96.

244. Huang, S., Yang, H., Lakshmanan, R. S., Johnson, M. L., Wan, J., Chen, I. H., Wikle Iii, H. C., Petrenko, V. A., Barbaree, J. M., and Chin, B. A.. Sequential detection of *Salmonella typhimurium* and *Bacillus anthracis* spores using magnetoelastic biosensors. *Biosens. Bioelectron.*, In Press, Corrected Proof.

245. Neufeld, T., Schwartz-Mittelmann, A., Biran, D., Ron, E. Z., and Rishpon, J. (2003). Combined phage typing and amperometric detection of released enzymatic activity for the specific identification and quantification of bacteria. *Anal. Chem.* **75**, 580–585.

246. Yemini, M., Levi, Y., Yagil, E., and Rishpon, J. (2007). Specific electrochemical phage sensing for *Bacillus cereus* and *Mycobacterium smegmatis*. *Bioelectrochemistry* **70**, 180–184.

247. Seo, S., Dobozi-King, M., Young, R. F., Kish, L. B., and Cheng, M. S. (2008). Patterning a nanowell sensor biochip for specific and rapid detection of bacteria. *Microelectron. Eng.* **85**, 1484–1489.

248. Seo, S., Kim, H. C., Cheng, M. S., Ruan, X. C., and Ruan, W. (2006). Microelectrical noise detector for rapid, specific, and sensitive identification of bacteria. *J. Vac. Sci. Technol., B* **24**, 3133–3138.

249. Petty, N. K., Evans, T. J., Fineran, P. C., and Salmond, G. P. C. (2007). Biotechnological exploitation of bacteriophage research. *Trends Biotechnol.* **25**, 7–15.

250. Goodridge, L., Chen, J. R., and Griffiths, M. (1999). The use of a fluorescent bacteriophage assay for detection of *Escherichia coli* O157: H7 in inoculated ground beef and raw milk. *Int. J. Food Microbiol.* **47**, 43–50.

251. Goodridge, L., Chen, J. R., and Griffiths, M. (1999). Development and characterization of a fluorescent-bacteriophage assay for detection of *Escherichia coli* O157: H7. *Appl. Environ. Microbiol.* **65**, 1397–1404.

252. Goldman, E. R., Pazirandeh, M. P., Mauro, J. M., King, K. D., Frey, J. C., and Anderson, G. P. (2000). Phage-displayed peptides as biosensor reagents. *J. Mol. Recognit.* **13**, 382–387.

253. Blasco, R., Murphy, M. J., Sanders, M. F., and Squirrell, D. J. (1998). Specific assays for bacteria using phage mediated release of adenylate kinase. *J. Appl. Microbiol.* **84**, 661–666.

254. Wu, Y., Brovko, L., and Griffiths, M. W. (2001). Influence of phage population on the phage-mediated bioluminescent adenylate kinase (AK) assay for detection of bacteria. *Lett. Appl. Microbiol.* **33**, 311–315.

255. Dubertret, B., Skourides, P., Norris, D. J., Noireaux, V., Brivanlou, A. H., and Libchaber, A. (2002). *In vivo* imaging of quantum dots encapsulated in phospholipid micelles. *Science* **298**, 1759–1762.

256. Sukhanova, A., Devy, M., Venteo, L., Kaplan, H., Artemyev, M., Oleinikov, V., Klinov, D., Pluot, M., Cohen, J. H. M., and Nabiev, I. (2004). Biocompatible fluorescent nanocrystals for immunolabeling of membrane proteins and cells. *Anal. Biochem.* **324**, 60–67.

257. Chan, W. C. W., and Nie, S. M. (1998). Quantum dot bioconjugates for ultrasensitive non-isotopic detection. *Science* **281**, 2016–2018.

258. Edgar, R., McKinstry, M., Hwang, J., Oppenheim, A. B., Fekete, R. A., Giulian, G., Merril, C., Nagashima, K., and Adhya, S. (2006). High-sensitivity bacterial detection using biotin-tagged phage and quantum-dot nanocomplexes. *Proc. Natl. Acad. Sci. U.S.A.* **103**, 4841–4845.

259. Balasubramanian, S., Sorokulova, I. B., Vodyanoy, V. J., and Simonian, A. L. (2007). Lytic phage as a specific and selective probe for detection of *Staphylococcus aureus*-A surface plasmon resonance spectroscopic study. *Biosens. Bioelectron.* **22**, 948–955.

260. Fu, L. L., Li, S. Q., Zhang, K. W., Chen, I. H., Petrenko, V. A., and Cheng, Z. Y. (2007). Magnetostrictive microcantilever as an advanced transducer for biosensors. *Sensors* **7**, 2929–2941.

261. Neufeld, T., Mittelman, A. S., Buchner, V., and Rishpon, J. (2005). Electrochemical phagemid assay for the specific detection of bacteria using *Escherichia coli* TG-1 and the M13KO7 phagemid in a model system. *Anal. Chem.* **77**, 652–657.

262. Banaiee, N., Bodadilla-del-Valle, M., Bardarov, S., Riska, P. F., Small, P. M., Ponce-De-Leon, A., Jacobs, W. R., Hatfull, G. F., and Sifuentes-Osornio, J. (2001). Luciferase reporter mycobacteriophages for detection, identification, and antibiotic susceptibility testing of *Mycobacterium tuberculosis* in Mexico. *J. Clin. Microbiol.* **39**, 3883–3888.

263. Liu, F. F., Luo, Z. F., Ding, X., Zhu, S. G., and Yu, X. L. (2009). Phage-displayed protein chip based on SPR sensing. *Sens. Actuators, B Chem.* **136**, 133–137.

264. Fu, L., Li, S., Zhang, K., Cheng, Z.-Y., and Barbaree, J. (2007). Detection of *Bacillus anthracis* spores in water using biosensors based on magnetostrictive microcantilever coated with phage. *Proc. SPIE* **6556**, 655619.

# MITIGATING PUBLIC HEALTH RISKS FROM AN AGROTERROR ATTACK

CRAIG HEDBERG

*Division of Environmental Health Sciences, University of Minnesota School of Public Health, Minneapolis, Minnesota*

## 1 INTRODUCTION

The public health risks from a potential agroterror attack directed against crops or vegetation could be viewed in a very broad sense as defined by the World Health Organization, or more narrowly in terms of the effects of exposure to specific agents. While it is necessary to consider the social impact of potential agroterrorism attacks when evaluating risk communication strategies for moving from response to recovery, the task of mitigating public health risks needs to start from the perspective of specific agents and exposure pathways.

The first step of mitigation is recognition. The public health system in the United States operates as a highly distributed network of local and state public health agencies that collect information from laboratories, clinicians, and individual citizens. The process of surveillance involves the ongoing collection, analysis, and dissemination of this information to form the basis of public health action [1]. In the surveillance of foodborne diseases this may range from an intervention at a restaurant identified as the source of a highly localized outbreak, to a multistate outbreak investigation involving the Centers for Disease Control and Prevention (CDC) and the federal food safety agencies. Any intentional contamination event would also involve the Department of Homeland Security and law enforcement officials.

## 2 POTENTIAL ROUTES OF CONTAMINATION AND CONSEQUENCES OF AN ATTACK ON CROPS AND VEGETATION

The list of potential agents that could be used in an agroterror attack on crops and vegetation is quite broad. The World Organisation for Animal Health (OIE) publishes a list of animal diseases that are notifiable on an international basis [2]. CDC, similarly maintains a listing of bioterrorism diseases/agents by category [3]. These lists contain a number of infectious agents that could be spread by contamination of crops prior to harvest, at the point of harvest, or during storage and transportation (Table 1). However, the consequences of potential attacks using these agents would be limited by the ability of the terrorists to gain undetected access to the crops and by the stability of the agent on the crop during harvest, transportation, and subsequent processing. For most of these potential agents there is a high degree of uncertainty that an attack would be successful. However, since there could be major consequences from an outbreak associated with

**TABLE 1 Potential Routes of Contamination and Consequences of an Attack on Crops and Vegetation**

| Objectives of Attack | Potential Agents | Routes of Contamination | Consequences |
|---|---|---|---|
| Destruction of crops intended for human consumption or animal feed. | Commercially available herbicides, plant pathogens. | Direct application to crops by hand, water, or aerosol. | Local or regional disruption of supply chains, availability of food or feeds. |
| Contamination of animal feed ingredients with agent intended to harm or kill domestic food animals. | OIE listed diseases transmissible through oral ingestion. | Application to field crops prior to harvest, at the point of harvest, or during storage and transportation. | Direct impact on exposed animals, disruption of trade following diagnosis of disease. |
| Contamination of crops with zoonotic agents intended to harm or kill domestic food animals, and people. | *Bacillus anthracis*, Brucella, Salmonella, Nipah virus. | Application to field crops prior to harvest, at the point of harvest, or during storage and transportation. | Direct impact on exposed animals and humans. Secondary human exposures from affected animals. |
| Contamination of crops and vegetation with bioterrorism agents or diseases intended to harm or kill people. | Botulism toxin, Ricin, *Salmonella typhi*, other foodborne disease agents, chemical toxins, and radiologic agents. | Application to field crops prior to harvest, at the point of harvest, or during storage and transportation. | Direct impact on exposed humans. Possible secondary transmission of typhoid fever, other foodborne disease agents. |

these agents, it is important to understand our ability to recognize and mitigate a potential agroterrorism event.

As described in Table 1, the potential choice of an agent could depend on the intended target for the attack. An attack intended to destroy crops could use a range of commercial herbicides applied directly by hand, water, or aerosol. This type of attack would not even require a high degree of stealth, as once the treatment is applied the consequence would be inevitable. For attacks designed to directly or indirectly affect food, animals, or humans, detection of the contamination event itself would allow for direct abatement of the hazard. The potential for these types of attack is dependent on the availability of an agent and access to a suitable point of contamination. Thus, the relative availability of common foodborne pathogens also increases the likelihood of their use in an agroterror attack.

Most of the relatively few documented intentional contamination events involving food have occurred at the point of retail sale or food service [5]. However, numerous outbreaks of foodborne diseases have resulted from contamination of fresh produce items in the field or at the point of harvest. These serve as useful models for the size and scope of potential agroterror attacks, and for the ability of the public health system to detect and respond to its occurrence.

## 3 DETECTION OF AN EVENT THROUGH FOOD AND ENVIRONMENTAL SAMPLING

Microbiological testing of foods and environmental samples is conducted for a variety of purposes [6]. Testing of food processing lines and environments is generally conducted to monitor critical control points and to validate cleaning and sanitation programs. This type of testing relies on the detection of indicator organisms. Thus, it would not be useful to detect the presence of an intentional contaminant. Pathogen testing of ingredients or end products may be conducted by industry as part of Hazard Analysis Critical Control Point (HACCP) verification, or for lot acceptance purposes mandated by purchasing specifications. Food regulatory agencies sample products in commerce as part of compliance surveillance.

Food monitoring has theoretical potential to prevent an outbreak of disease due to the natural or intentional contamination of foods because it is conducted before the contaminated product reaches consumers [7]. However, many practical issues make it unfeasible to build a robust monitoring program to safeguard the supply of fresh fruits and vegetables. To start with, approximately 70 billion pounds of fresh fruits and vegetables are produced each year in the United States United States Department of Agriculture, Economic Research Service (USDA, ERS). Given the large number of potential introduction points for contamination, some prior knowledge of actual threats would be needed to guide sample selection and test methods. In contrast to many natural contamination events, it is thought that intentional events will involve relatively high levels of contamination. While this will reduce the need for sensitivity in the test methods, it is still likely that the distribution of the agent in the sample will be uneven. In addition, the food matrix and inhibitory substances in the sample could further reduce the sensitivity of the assay [7]. Although an in-line monitoring system for potential bioterrorism agents may be feasible for milk or other fluids, no such system is likely to be useful for fresh produce items.

## 4 DETECTION OF AN EVENT THROUGH MONITORING OF ANIMAL POPULATIONS

Animals represent a potential end target for intentional contamination of crops. Animal feeds could be contaminated with agents intended to directly harm food animal populations or to serve as a transmission pathway for zoonotic diseases to humans. Because of the high population densities of confined animal feeding operations (CAFOs), such an attack would likely result in a localized outbreak of disease among the animals that would be recognized by producers. Depending on the severity of the disease in the animals, diagnostic evaluation by veterinarians supported by state veterinary diagnostic laboratories (VDL) would likely be initiated. In conjunction with the National Veterinary Services Laboratory, in Ames, Iowa, the state VDL would work to identify the agent, and if it were an OIE listed disease, report the event to state and federal animal health officials [8].

Intentional contamination of crops or vegetation could also result in contamination of pet foods. Because pet foods tend to be widely distributed using similar distribution channels as human foods, these events would not be detected because of the localized outbreaks that would be associated with CAFOs. Events involving chemical agents or toxins

would likely resemble the outbreak of illnesses associated with melamine contamination [9]. Detection of this event required the clinical recognition of kidney failure occurring among cats and dogs that consumed a particular brand of pet food. A second example of the impact of pet food contamination was the occurrence of a multistate outbreak of Salmonella serotype Schwarzengrund infections in humans. At least 62 persons from 18 states were infected as a result of direct or indirect exposure to Salmonella-contaminated dry dog food [4]. Interestingly, no illnesses were reported among the dogs in the households. The detection of this event highlights the importance of human disease surveillance systems to detect and mitigate public health risks associated with animal feed as well as human foods.

## 5 DETECTION OF AN EVENT THROUGH HUMAN DISEASE SURVEILLANCE

Given our limited ability to detect contaminated food products before they enter commerce, the interval between the occurrence of a food system event, its detection, and the subsequent response by the public health system is a key determinant of the potential impact. Most foodborne outbreaks are localized and are investigated and controlled by local or state public health authorities. However, as demonstrated by the dog-food associated Salmonella Schwarzengrund outbreak, multijurisdictional events may be large, widespread, and require coordination between multiple state and federal agencies.

In the United States, foodborne disease surveillance is generally conducted under the authority of communicable disease reporting rules [10]. These rules are established under individual state laws, and vary by states. In many states, responsibility for foodborne disease surveillance is assigned to local health jurisdictions. In some states it is either shared between local and state levels or retained by the state. Disease reporting rules typically identify a list of specific diseases that should be reported to local or state officials when they are clinically diagnosed or confirmed by laboratory testing. The lists of reportable diseases vary by state, but typically include diseases for which some specific public health intervention is needed. The states and CDC have developed a list of diseases for which information should also be collected on a national basis. Table 2 lists selected nationally notifiable diseases that may be transmitted by food. States voluntarily report to CDC the numbers of these cases reported at the state level. However, due to state privacy laws, and federal Health Information Privacy Assurance Act (HIPAA) regulations, identifying information from individual cases is not generally reported to CDC.

Three main types of surveillance have been used for the detection of foodborne disease infections and outbreaks (Table 3). These include consumer complaints, pathogen-specific surveillance, and syndromic surveillance.

Most foodborne outbreaks are identified as a result of consumer complaints. These complaints are generated after two or more people become ill with similar symptoms after sharing meal(s) together. In most cases the complaints are made within a couple days following onset of symptoms, and the complainants have usually not sought medical care or had any laboratory testing done. Occasionally the complaint will be made after an individual consulted a health care provider and was given a diagnosis of “food poisoning”, and rarely, will a health care provider notify public health officials that they suspect a patient may be part of a foodborne outbreak. While complaints are a timely way of identifying outbreaks associated with individual events or establishments, complaint

**TABLE 2 Selected Nationally Notifiable Diseases which may be Foodborne. From CDC [4]**

- Anthrax (gastrointestinal)
- Botulism (foodborne)
- Cholera
- Cryptosporidiosis
- Cyclosporiasis
- Giardiasis
- Hemolytic uremic syndrome, postdiarrheal
- Hepatitis A, acute
- Listeriosis
- Salmonellosis
- Shiga toxin-producing *Escherichia coli* (STEC)
- Shigellosis
- Typhoid fever

systems are generally operated by local public health agencies with no aggregation of data on the state or federal levels. These independent complaint systems are unlikely to detect multijurisdictional events of the type that may be expected from intentional contamination of a food product at the point of production. To do so would require linking multiple outbreak events to a common agent and then to a common food item or production source.

One important quality of complaint-based detection systems is the ability to identify a new disease causing agent. Because the occurrence of the outbreak is based on similar symptoms occurring following a common exposure, the investigation of the outbreak can also involve a detailed laboratory-based search for the agent. For example, *Escherichia coli* O157:H7 was identified as a foodborne pathogen following the investigation of several outbreaks of bloody diarrhea associated with fast-food hamburger restaurants [11].

In contrast to the flexibility of complaint-based surveillance to identify new agents, pathogen-specific surveillance involves the reporting of individual cases of diseases such as *Salmonella enterica* or *E. coli* O157:H7. Because molecular subtyping of these organisms can be conducted to provide a very specific case definition, it is possible to link cases over a multistate area to a potential common source. CDC has established a public health laboratory-based molecular subtyping network for foodborne disease surveillance (PulseNet). PulseNet combines standardized methods for subtyping foodborne disease pathogens by pulsed-field gel electrophoresis (PFGE) with electronic file sharing to provide a national framework for pathogen-specific surveillance [12]. Specific exposure information must be separately obtained through follow-up interviews with individual cases. PulseNet also provides opportunities for linking data on pathogens identified as part of food, animal, or environmental monitoring programs to enhance human disease surveillance.

The third major type of surveillance for food event detection involves the monitoring of clinical events independently of a specific etiology. This is called *syndromic surveillance* because it tracks the occurrence of disease by manifestation of symptoms such

**TABLE 3 Characteristics of Outbreak Detection Systems Used in Foodborne Disease Surveillance, and their Potential to Mitigate Public Health Risks from an Agroterror Attack**

| Characteristic | Consumer Complaints | Pathogen-specific Surveillance | Syndromic Surveillance |
|---|---|---|---|
| Diagnostic information | Set of symptoms experienced by persons following a common food exposure. | Diagnosis of specific foodborne agent. May include detailed subtype information to facilitate cluster detection. | Increased occurrence of disease (e.g. diarrhea) in reference population, without identification of specific agent. |
| Exposure information | Common food exposure—subject of complaint. Additional exposure information may be obtained through interview at time of initial complaint. | Demographic information reported. Specific exposure information may be obtained through follow-up interview. | Identity, demographics, and contact information regarding individuals may be obtained by review of records following signal detection. Specific exposure information may be obtained through follow-up interview. |
| Outbreak types detected | Outbreaks associated with facilities or events. Can detect outbreaks caused by new or unknown agents. | Local or widespread outbreaks caused by specific pathogen under surveillance. | Outbreaks involving unusual clinical manifestations suggesting a new disease, or very large, community-wide outbreaks due to norovirus. |
| Potential to mitigate public health risks from agroterror attack | Multiple outbreak events could be linked to a common agent and then to a common food item or production source. | Widely dispersed, individual cases could be linked to a common food item of production source. | Cases with new disease syndrome may be linked to a common food item or production source. |

as diarrhea. As seen in the example of kidney failure in dogs and cats associated with melamine-contaminated pet food, surveillance for unusual syndromes can be very useful. However, syndromic surveillance for gastrointestinal illness has not proved effective at detecting specific foodborne disease events. For example, in 2001, the New York City Department of Health implemented a surveillance system for gastrointestinal illness seen in hospital emergency departments [13]. Over a period of 3 years, 98 citywide signals indicating increased occurrence of gastrointestinal illness were received. Seventy-five percent of these occurred during seasonal outbreaks, and none of the 49 actual outbreaks of gastrointestinal disease reported to the City Health Department during this time period was detected by the syndromic surveillance system [13]. Thus, this surveillance was neither sensitive nor specific for the occurrence of foodborne outbreaks, and unlikely to be useful for mitigating public health risks associated with an agroterror event.

## 6 OUTBREAK INVESTIGATIONS: THE ROLE OF EPIDEMIOLOGIC METHODS TO RAPIDLY IDENTIFY THE SOURCE AND GUIDE CONTROL STRATEGIES

Many of the agents responsible for outbreaks of foodborne disease may also be transmitted by other routes, such as waterborne, zoonotic, and person-to-person. It is not always possible to determine the route of transmission by identifying the agent or the clinical presentation of the outbreak. Thus, identifying the route of transmission is an important objective in many outbreak investigations and is critical for implementing effective control measures. The overall goal of an outbreak investigation should be to rapidly obtain sufficient information to implement specific interventions to abate the outbreak, or to determine that no specific interventions are warranted.

The process of epidemiology involves the careful description of events and comparison of rates between groups. In foodborne outbreak investigations this involves comparing food histories between outbreak-associated cases and a comparison group of controls who do not appear to be part of the outbreak.

The epidemiological investigation proceeds as follows:

(a) An outbreak case definition is established based on characteristics of the agent that led to detection of the outbreak. For many bacterial pathogens this is based on PFGE patterns or other reproducible molecular characteristics.
(b) Outbreak-associated cases are characterized by person, place, and time to identify patterns that may be associated with particular food items or diets.
(c) Individual cases are interviewed as soon as possible, with a standardized "trawling questionnaire" to identify potential common exposures.
(d) "Trawling questionnaire" exposure frequencies are compared against FoodNet Atlas of Exposures to identify the suspect food item.
(e) Nonill community controls or nonoutbreak-associated cases are interviewed to obtain detailed exposure information to be used in a case-comparison analysis of exposures.
(f) Brand names and product code information for prepackaged food items are documented; distribution sources for commodity food items are identified.
(g) Exposure information is analyzed to compare cases with relevant comparison groups (e.g. nonill controls or nonoutbreak-associated cases) to implicate the food item or nonfood exposure source.

Using these methods, commercial ice cream was identified as the source of a nationwide outbreak of *Salmonella enteritidis* infections within 2 days of the start of the investigation, and 10 days before the outbreak strain of Salmonella was isolated from intact packages [14]. More recently, pot pies were identified as the source of a nationwide outbreak caused by a monophasic Salmonella strain within 2 days of the start of a multistate case-control study, even though pot pies had not been identified by previous hypothesis generating interviews [15]. Furthermore, details of the exposure histories provided important clues to identify how the products became contaminated.

The speed with which outbreak investigations are conducted depends on the agent, the number of cases associated with the outbreak, and where the cases occur. Since

most foodborne illness investigations are conducted by local or state public health or food regulatory agencies, the resources available to the agency and the motivation of the agencies staff are important considerations. In a study of the timeliness of enteric disease surveillance in six US states, the median interval from onset of symptoms to collection of stool sample was 3 days for *E. coli* O157:H7 and 4 days for Salmonella [16]. Cases of both pathogens were reported from the clinician to the health department 2 days after the culture result was available. Approximately half of the *E. coli* O157:H7 cases, but only 20% of Salmonella cases were contacted by the health department on the same day the report was received. The differences in response between Salmonella and *E. coli* O157:H7 are a clear reflection of the increased public health importance that is placed on *E. coli* O157:H7. Differences in response to sporadic infections also affect the speed with which outbreaks are identified. In the same timelines study, the median interval from onset of symptoms to outbreak detection was 8 days for outbreaks due to *E. coli* O157:H7 and 16 days for outbreaks due to Salmonella. These time intervals reflect delays both in conducting interviews and in PFGE subtyping.

Because of the importance of molecular subtyping to outbreak detection and response, the speed with which public health agencies respond to detected clusters of cases determines the potential to mitigate the public health risks from an outbreak. In 2001, the National Food Safety System (NFSS) Project, Outbreak Coordination and Investigation Workgroup published guidelines to improve coordination and communication among multiple states and federal public health and food regulatory agencies investigating multistate foodborne outbreaks.

From 1998 to 2003, 56 multistate outbreaks with known etiology were investigated. Of these, 31 (55%) were due to Salmonella and 10 (18%) were due to *E. coli* O157:H7. These accounted for 4% of Salmonella and 7% of *E. coli* O157:H7 outbreaks reported to CDC's Foodborne Outbreak Response and Surveillance Unit during this time period. However, these estimates do not account for other outbreaks with multistate distributions of cases that were not identified as multistate outbreaks. Since surveillance methods employed at the state level are not tracking exposure sources, *per se*, it is important that public health officials account for outbreaks with multistate distributions of cases from a common exposure, as well as outbreaks resulting from multistate exposures.

The median intervals (and ranges) from onset to outbreak recognition were 18 (8–19) days for *E. coli* O157:H7 and 23 (10–48) days for Salmonella. Median intervals (and ranges) from onset to outbreak recognition were 21 (2–24) days for outbreaks detected by complaint, 10 (5–12) days for case report and follow-up, and 22 (7–48) days for PFGE subtype.

Median intervals (and ranges) from outbreak recognition to intervention were 7 (1->72) days for outbreaks investigated by a single state and 18 (6–62) days for multistate outbreak investigations. Interventions were made within 8 days in 8 of 21 multistate outbreaks reviewed. Investigations were conducted primarily by single states in six (75%) of these. Thus, where individual states can take a lead role in multistate outbreak investigations, this appears to be a more efficient investigation strategy. Strong leadership by individual states in multistate investigations will promote faster and better targeted mitigation strategies.

## 7 MITIGATING PUBLIC HEALTH RISKS: MOVING FROM RESPONSE TO RECOVERY

Following an attack on the food system, there will be several key elements involved in the move from response to recovery. Most importantly, these include the size, scope, and severity of the event. However, the speed with which such an attack is recognized and controlled will certainly affect all of these measures. In this regard, enhancing the capacity of our foodborne disease surveillance system to rapidly investigate all foodborne disease outbreaks will be critical to positioning our food system for a rapid recovery from an agroterrorism event.

Communication with the public will be critical in our efforts to recover from an agroterrorism event. The public will look for assurance that we have identified the problem, effectively abated it, and developed plans to prevent its recurrence. The effectiveness of these communication strategies will depend on how well our investigations address these issues. Rapid and comprehensive epidemiologic investigations with detailed exposure assessments will be critical to finding the answers of when and where the attacks occurred, if not always the who and why.

## 8 SUMMARY AND CONCLUSIONS

The threat of an agroterrorism attack against crops and vegetation poses a great risk to public health and the integrity of the food supply. Our ability to keep contaminated foods and animal feeds out of the marketplace is limited. The lessons we can take from our experience investigating large widely distributed outbreaks are directly relevant to the challenges of agroterrorism.

Our detection methods must be sensitive and our investigation methods specific. We must conduct our investigations with a sense of urgency and the belief that we can make a difference. Epidemiology can be a powerful tool to detect events, identify their source, and mitigate their consequences.

## ACKNOWLEDGMENT

Research included in this paper was supported by the US Department of Homeland Security (Grant number N-00014-04-1-0659), through a grant awarded to the National Center for Food Protection and Defense at the University of Minnesota. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author and do not represent the policy or position of the Department of Homeland Security.

## REFERENCES

1. Centers for Disease Control and Prevention (2001). Updated guidelines for evaluating public health surveillance systems. *MMWR Morb. Mortal. Wkly. Rep.* **50**(RR13), 1–35.
2. World Organization for Animal Health (2008). *Diseases Notifiable to the OIE*, Accessed on-line May 27, 2008. http://www.oie.int/eng/maladies/en_classification2008.htm?e1d7.

3. Centers for Disease Control and Prevention (2008). *Bioterrorism Agents/Diseases- by Category*, Accessed on-line May 27, 2008.http://emergency.cdc.gov/agent/agentlist-category.asp.
4. Centers for Disease Control and Prevention (2008). Multistate outbreak of human *salmonella* infections caused by contaminated dry dog food — United States, 2006—2007. *MMWR Morb. Mortal. Wkly. Rep.* **57**(19), 521–524.
5. Sobel, J., Khan, A. S., and Swerdlow, D. L. (2002). Threat of a biological terrorist attack on the US food supply: the CDC perspective. *Lancet* **359**(9309), 874–880.
6. International Commission on Microbiological Specifications for Foods (2002). Microbiological hazards and their control. In *Micro-organisms in Foods:7. Microbiological Testing in Food Safety Management*, Kluwer Academic/Plenum Publishers, New York, pp. 1–19.
7. Besser, J. M. (2006). Systems to detect microbial contamination of the food supply. *Institute of Medicine Forum on Microbial Threats. Addressing Foodborne Threats to Health: Policies, Practices, and Global Coordination, Workshop Summary*, The National Academies Press, Washington, DC, pp. 178–189.
8. US Department of Agriculure (2008). *Animal and Plant Health Inspection Service, National Center for Animal Health Surveillance*, Accessed on-line May 27, 2008.http://www.aphis.usda.gov/vs/ceah/ncahs/.
9. Burns, K. (2007). Events leading to the major recall of pet foods. *J. Am. Vet. Med. Assoc.* **230**(11), 1600–1620.
10. Centers for Disease Control and Prevention (2008). Summary of notifiable diseases—United States, 2006. *MMWR Morb. Mortal. Wkly. Rep.* **55**(53), 1–94.
11. Riley, L. W., Remis, R. S., Helgerson, S. D., McGee, H. B., Wells, J. G., Davis, B. R., Hebert, R. J., Olcott, E. S., Johnson, L. M., Hargrett, N. T., Blake, P. A., and Cohen, M. L. (1983). Hemorrhagic colitis associated with a rare Escherichia coli serotype. *N. Engl. J. Med.* **308**(12), 681–685.
12. Swaminathan, B., Barrett, T. J., Hunter, S. B., Tauxe, R. V., and CDC PulseNet Task Force (2001). PulseNet: the molecular subtyping network for foodborne bacterial disease surveillance, United States. *Emerging Infect. Dis.* **7**(3), 382–389.
13. Balter, S., Weiss, D., Hanson, H., Reddy, V., Das, D., and Heffernan, R. (2005). Three years of emergency department gastrointestinal syndromic surveillance in New York City: what have we found? *MMWR Morb. Mortal. Wkly. Rep.* **54**(Suppl), 175–180.
14. Hennessy, T. W., Hedberg, C. W., Slutsker, L., White, K. E., Besser-Wiek, J. M., Moen, M. E., Feldman, J., Coleman, W. W., Edmonson, L. M., MacDonald, K. L., and Osterholm, M. T. (1996). A national outbreak of Salmonella enteritidis infections from ice cream. The investigation team. *N. Engl. J. Med.* **334**(20), 1281–1286.
15. Centers for Disease Control and Prevention (2008). *Investigation of Outbreak of Human Infections Caused by Salmonella I 4,[5],12:i:-, Accessed on-line May 27, 2008*. http://www.cdc.gov/salmonella/4512eyeminus.html.
16. Hedberg, C. W., Greenblatt, J. F., Matyas, B. T., Lemmings, J., Sharp, D. J., Skibicki, R. T., and Liang, A. P. (2008). Enteric disease investigation timeline study work group. timeliness of enteric disease surveillance in 6 US states. *Emerging Infect. Dis.* **14**(2), 311–313.

## FURTHER READING

Hedberg, C. W. (2007). The epidemiology of foodborne diseases. In *Food Microbiology: Fundamentals and Frontiers*, 3rd ed., M. P. Doyle, L. R. Beuchat, and T. J. Montville, Eds. ASM Press, American Society for Microbiology, Washington, DC, pp. 519–533.

Crutchley, T. M., Rodgers, J. B., Whiteside, H. P. Jr., Vanier, M., and Terndrup, T. E. (2007). Agroterrorism: where are we in the ongoing war on terrorism? *J. Food Prot.* **70**(3), 791–804.

Madden, L. V., and Wheelis, M. (2003). The threat of plant pathogens as weapons against U.S. crops. *Annu. Rev. Phytopathol.* **41**, 155–176. Epub 2003 Apr 18. Review.

Scholthof, K. B. (2003). One foot in the furrow: linkages between agriculture, plant pathology, and public health. *Annu. Rev. Public Health* **24**, 153–174. Epub 2002 Oct 23. Review.

# PROCESSING AND PACKAGING THAT PROTECTS THE FOOD SUPPLY AGAINST INTENTIONAL CONTAMINATION

SCOTT A. MORRIS

*University of Illinois at Urbana-Champaign, Urbana, Illinois*

## 1 INTRODUCTION

Too often, the first reaction to a social problem is to attempt to find a technical solution, when technology cannot overcome social problems, only their means and circumstances. Although there are some processing and packaging steps that can be taken to indicate intentional contamination of food, it is not possible to add a simple, inexpensive component to existing systems to prevent a determined attack: real solutions are always imperfect, often more complex and usually more difficult.

Quite apart from malicious human efforts, nature has been attempting to contaminate food products since the first drying and salting of grains, meats and vegetables provided for a longer-duration food supply, and most food processing operations have a culture of quality that is intrinsically designed to work against these threats. Many of the efforts in large-scale food contamination have been directed at detection of outbreaks of food poisoning in the population and then remediation after an outbreak occurs. The food industry, which is usually quite careful about quality and safety, already has coding and recall management practices in place. These have historically worked very well after problems are detected, but assume that the producer is acting in good faith; that the inspection, notification and recall systems operate as they are supposed to; and that the product itself is not counterfeit.

Packaging, which is intrinsically designed to protect the product against many natural and man-made hazards, may protect against pilferage or low-level postprocessing contamination of products, but the most that can be achieved for many products at any practical cost and production level is an indication of tampering. Additionally, the requirements for global outsourcing of manufactured products, ingredients and components; global markets for finished goods, the persistent push to minimize the

costs of ingredients and packaging systems; ceaseless just-in-time logistics systems that have replaced warehouses; and perpetual demands to maximize productivity impede many types of proactive contamination prevention.

As a result of these and other factors that are discussed in this article, there is no magic gadget that can be added to the food processing packaging and distribution system to make it perfectly safe against intentional contamination. What can be done is to assess and manage risks responsibly and appropriately, implement detection steps and improvements in technology where needed to make contamination difficult at all points in the food system, and to ensure that a response system that is capable of remediating problems on a timely basis is in place. This would represent a substantial improvement on the current system.

## 2 PROCESSING

Intentional contamination or destruction of the food supply, usually through "agroterrorism" (malicious disruption at the crop level) has been a historic strategy for the disruption of populations and a long-standing fear during wartime. In a world increasingly occupied with asymmetric warfare on many different levels, the threat of a subtle toxin or custom-tailored organism pervading the food system is an increasingly viable threat. These agents may be introduced at some point in the manufacturing and distribution process, between harvesting the raw commodity and consuming the finished product, in order to reach a much larger percentage of the population with less chance of detection than with simple package tampering.

Food processing systems are designed to produce a product that is safe and stable within its distribution environment. That environment might range from long-term shelf-stable foods such as cans, jars and Meals, Ready to Eat (MRE) rations for the military to shorter-duration products such as dairy products, bagged salads and refrigerated "fresh" pasta. Historically, processing has involved either altering the food to make it inhospitable to spoilage organisms with processes such as drying or pickling, or applying thermal sterilization (and moderate toxin denaturation in some cases) followed by containment in a hermetically sealed container that prevents recontamination. Newer preservation methods have involved controlling the temperature throughout the distribution cycle to retard growth, and alternative methods of sterilization and containment have been developed, but the principle remains essentially the same.

The implementation of Hazard Analysis and Critical Control Point (HACCP) requirements for food processing plants has provided tools to find and manage vulnerabilities to naturally occurring hazards. HACCP can also provide optimal points for assaying for contaminants or inspection for disrupted seals or counterfeit goods, if analytical tools are available that can detect the agent used. Increased registration and security requirements for food processing plants have reduced access to the production facilities and the use of operational risk management (ORM) strategies taken from the aerospace industry (which faces critical dangers as a matter of course) have provided tools to help develop situationally appropriate safeguards [1]. Balancing this are high employee turnover rates and the difficulty of documenting workers, the broad range of ingredients from multiple sources that may be shipped without tamper indication or verification systems, as well as reliance on Certificates of Analysis for ingredient safety rather than verifiable in-house testing. Many of these factors leave the system open to attack.

On a larger scale, processed food production is run on a "Just-in-Time" paradigm that distributes product as quickly as possible and makes "catching" contaminated products before sale very difficult if there is any delay between detection of contamination or illnesses and the issuance of a recall and warnings. This delay may allow a contaminated product to be distributed and consumed by a broad segment of the population, turning a containable incident into a debacle. An example of this is discussed subsequently.

### 2.1 Counterfeit Products and Ingredients

Counterfeit products in the United States precede the revolutionary war; one of the complaints Britain had against its colonies was that British containers were being refilled and resold with a variety of products of dubious quality. Indeed there is evidence that colonists imported empty bottles from Britain for the sole purpose of counterfeiting or mimicking British products [2]. Since then, most counterfeit products have been concentrated around objects of small physical size, difficulty of verification and very high value which maximizes the return/risk benefit for the counterfeiter. Counterfeit designer watches are much more lucrative that counterfeit potato chips and counterfeit pills are very easy to make and immensely profitable. Because of this, governmental anticounterfeiting efforts in the food, drug and cosmetic milieu have been prominently focused on the pharmaceutical industry due to the immediate harm done to the consumer, although the cosmetics industry faces a booming expansion in counterfeit, copycat and "parasite" goods, that are often severely contaminated (and often attract buyers who are not willing to pay for the "real thing" but are unaware of the risks) [3, 4].

Counterfeiting of drugs in the United States has become an item of considerable concern since diluted and nonsterile Procrit® and Epogen®, were held responsible for deaths and illnesses in 2002 and Lipitor® tablets in 2003 were found to be counterfeit [5–7]. This has been addressed by increased requirements for verification and distribution traceability, something that the pharmaceutical industry had avoided on a cost basis for some time but is finally coming into practice with bar codes and other technical additions in Europe and elsewhere [8].

Counterfeiting (or product swapping) of foods items has long been a problem with luxury items such as high-value spirits, wines and foods. Counterfeiting of more general foods is less likely unless there is a combination of high financial or tactical value and ease of manufacturing counterfeits [9]. One of the food categories that shows an ongoing problem with counterfeiting is seafood, of which approximately 80% is imported into the US. Because seafood is difficult to identify after processing, it has been misrepresented for years and can be deliberately mislabeled as a high-value species to increase profitability. This fraudulent mislabeling carries the risk of illness or death from both intrinsically toxic species, and species that have absorbed dietary toxins. In 2007, a seafood importer was found to have mislabeled seafood containing puffer fish (which carry tetrodotoxin, a potent neurotoxin with no antidote) as monkfish [10]. Subsequent congressional inquiries highlighted the low rate and poor coordination of safety or security inspection in seafood imports [11].

## 3 PACKAGING

Packaging plays three general primary functions in modern consumer usage; protection, utilization and communication. While the protection function is often thought of

as protecting a product against damage or contamination, in the case of a particularly dangerous material (nuclear fuel rods, for instance) the primary purpose is just the reverse—protection of the general environment against the product itself. Beyond that, the most fundamental function of nearly any type of food packaging is to protect the product against postprocessing contamination and quality loss. Since Mother Nature is constantly providing clever and relentless threats to degrade or contaminate products, packaging has always had a role to play in this regard, and the intentional human element is a very small component of the challenges that most food packaging resists on a continuing basis.

From a security standpoint, packaging can thus be thought of as implicitly resisting intentional contamination to a large degree, but with the added utility of potentially being able to indicate when intentional tampering has occurred, either as an intrinsic feature of the design or as a result of an added component or design feature. This capability is usually balanced against the perception of packaging as an expense to be minimized during high speed production, and the requirement that the indicator must be both robust and accurate.

Packaging also has the capability of communicating, most often using label copy or other printed material but other communication measures may be used as well. Part of a security system for particularly vulnerable assets may thus involve communicating a verification code, as well as displaying an intact tamper-evident device, although these approaches have many weaknesses as well.

Finally, packaging must have some utility. It is possible to create an impenetrable package for food products, but they would be prohibitively expensive, difficult to mass-produce on the astronomical scale required for some food packages (the United States alone consumes more than a quarter-trillion packaged soft drinks per year), and would defeat use by the consumer.

### 3.1 Packaging and Safety Assurance

For packaging systems, the assurance of a product's integrity and safety is involved in several roles—borrowed from cryptography—that can be described as authentication, integrity and non-repudiation [12]. The first of these, authentication, is the assurance that the product is that which is described on the label and not a counterfeit from another producer. As is discussed in more detail, this is the more likely scenario for a broad-scale breach of food integrity at the ingredient level, since it is both easier to implement and more effective in disrupting entire segments of the food supply.

The second, integrity, assures the customer that the product in the package has not been modified after production whether by the substitution of other goods or contamination of the existing product. There are historical precedents for this, the most notorious being the contamination of Tylenol in the 1980s that led to stricter requirements for over-the-counter (OTC) drug packaging and began the process of tamper-indicating packaging components. Although this particular method of disrupting consumer confidence in a product may be somewhat effective and is very expensive to the product manufacturer, it is less effective at inflicting actual widespread harm or disrupting sales of a broad class of products since tampering is typically tightly confined to a single geographic region or product.

The final function, non-repudiation, ensures that the original manufacturer cannot deny producing the product (in effect, verifying that they have produced it). Non-repudiation is seldom considered in manufacture of physical items, but warrants discussion since it

bears directly on the issue of plausible deniability by a manufacturer that the product is not something that they are responsible for, and are therefore absolved both from the responsibility for its production and from any liability from the harm it caused. In a litigious economy that is increasingly outsourcing its consumer goods and many kinds of food from a broad multitude of globally distributed manufacturing operations and contract operations, this issue may prove increasingly important.

### 3.2 Requirements for Tamper Evidence

The first tamper-evident requirements were applied to OTC drugs after the Tylenol tampering episode in 1982. Few, if any, of these devices provide substantial protection against even a marginally skillful person with modest resources; this is a favorite challenge for clever students who generally have little trouble with them. While other countries that have adopted tamper-evident packaging requirements have been much more specific in their material, structure and printing requirements [13], current regulations for OTC drugs in the United States simply demand that

> "Each manufacturer and packer who packages an OTC drug product (except a dermatological, dentifrice, insulin, or lozenge product) for retail sale shall package the product in a tamper-evident package ... having one or more indicators or barriers to entry which, if breached or missing, can reasonably be expected to provide visible evidence to consumers that tampering has occurred [14]."

Many of the tamper-evident and "freshness" seals on foods and pharmaceuticals can be defeated quite easily, although they do provide indication of pilferage to consumers (and a very good seal for many products, at the expense of annoyance at having to remove them). Unfortunately, there is no legal requirement for tamper evidence or counterfeiting protection in the food supply chain beyond due diligence, good manufacturing practices, record-keeping and perhaps quality assurances for ingredients and components. There are only voluntary guidelines and similarly worded guidelines for food importers, dairy processors, and general food producers, processors and transporters to address this issue:

> "inspecting incoming products and product returns for signs of tampering, contamination or damage (for example, abnormal powders, liquids, stains, or odors, evidence of resealing, compromised tamper-evident packaging) or "counterfeiting" (inappropriate or mismatched product identity, labeling, product lot coding or specifications, absence of tamper-evident packaging when the label contains a tamper-evident notice), when appropriate." [15–17]

While these guidelines urge reliance on broadly based ORM strategies rather than singular technical devices—an effective strategy when properly implemented—one of the most prominent weaknesses in the integrity of the food supply is the specter of unremediated, ingredient-level contamination. Tampering with a single product may destroy sales of that particular product until the crisis is resolved, but tampering with a commodity-level ingredient can result in a broadly distributed incident that not only harms consumers but can destroy confidence in the entire class of materials.

### 3.3 Tamper Indication Devices

Some tamper indicators have been successfully used for many years. The vacuum in traditional canned foods has been seen to be an indication of both physical and microbial

integrity, and consumers are almost universally aware that a swollen or damaged can or a jar with without a vacuum should be discarded. As packaging moves to lower cost and more material-efficient structures, the indications of integrity are much simpler; for example, an undamaged or unopened pouch or aseptic pack, but there is no secondary indicator (such as vacuum) to indicate integrity and the seals are easily duplicated or repaired after tampering.

By contrast, a package that is intrinsically difficult to construct, fill and seal such as a modern soft drink can, provides a much higher degree of resistance to intentional contamination. The delicacy of the structure, pressurized contents and single-use opening would require the use of extremely specialized equipment and processes to duplicate effectively. While this is not completely unlikely, since everything from nuclear reactor parts to hundred dollar bills are counterfeited on a regular basis [18, 19], it raises the stakes considerably and drives serious tampering efforts toward a more efficient, upstream means of disrupting food supplies. Many of the most effective tamper evidence devices are integral parts of the package that must be visibly and irreversibly damaged to gain access to the contents of the package. The most annoying of these can actually restrict access to everyone—the theft-resistant clamshell packaging around small electronic devices is a good example—but they are effective. Some of these date back before the Tylenol incidents created a flurry of new devices, and were intended to prevent pilfering, or dilution of alcoholic beverages [20]. Newer developments are aimed at a broader market, but operate in a similar manner of permanently locking or fusing together during assembly and requiring obvious destruction to access the contents. For tamper evidence to really come into its own, it must be something other than an afterthought in a product component that is often regarded as an annoying expense to be minimized while choosing among standardized components and processes. Designed-in rather than added-on tamper evidence that requires irreversible disruption of the basic package structure to gain access to the product would be a considerable improvement for many stock package types and components.

### 3.4 Add-On Indicators

Add-on indicators are usually shrink bands around the package closure, a tape seal that may include a holographic pattern, laminate, or other optical feature that is relatively hard to duplicate by a casual tamperer, or a seal under the main closure that is inductively fused to the container and must be removed before the product can be used. Hidden coding on the package or optical microparticulate taggants in the product itself may also be added to make tampering or counterfeiting more difficult. This will deter casual pilfering or tampering but is unlikely to defeat the use of duplicate packages or other more complex attacks. Often these seal indicators can be "lifted"; removed and transferred to another package as well.

Most of the add-on indicators are very low cost and require very few resources to defeat. Moreover, consumers are not readily aware of them unless they create a nuisance factor. Most consumers would presume that a first squeeze of catsup that occurred without stopping to remove the seal to be a blessing. Further, since there are few requirements and no standardization, a case or shipment of bottles with a uniform type of seal added to the entire lot after contaminating the product would not be recognized as different or as unsafe. What is required is a move to higher design standards, already achieved in many industries from automobiles to electronics, where quality of tamper evidence is

designed in from the start rather than added as an afterthought. This, like the soda can, will require a much higher level of infrastructure to duplicate, and will therefore further deter the casual tamperer.

Unfortunately, tampering indicators and particularly add-on tamper indication such as holographic films and patterned adhesive tapes suffer from a form of the "banknote paradox". They need to be so well standardized that they are well known to the users (and can easily be spotted when something is amiss), but that standardization makes their counterfeiting more beneficial since there will be a wider range of products for them to be used on. This in turn drives the engraving and printing of banknotes into an ever-escalating spiral of elegant anticounterfeiting technology with counterfeiters often close behind (or in some cases ahead of) the legitimate users. For a single-use item that must be of minimal cost such as antitampering tape, bands or stickers—primarily added to demonstrate due diligence—the same kind of spiral could drive it out of existence. Manufacturers are already increasing the level of printing sophistication and therefore, cost in some types of seals.

The main reason that this has not been a substantial problem to date is that there have been few store-level malicious tampering attacks. Also there is little direct benefit from counterfeiting the tamper evidence devices (unlike counterfeiting currency), and obviously damaged products produced by clumsy tamperers are not recognized as such and are quickly discarded at some point in the distribution chain as having been damaged in transit or during display.

### 3.5 Proactive Devices

Although still experimental, work has been done to develop packaging structures and materials that will actively indicate other conditions that pose a threat to the safety of products. In the food industry, there is a great deal of interest in indication of microbial growth and temperature abuse. Temperature abuse, which may result in spoilage, must integrate time and ambient temperature exposure to create a thermal profile. This has been achieved relatively inexpensively with electronic devices, but most devices that have been marketed use a chemical reaction analog that attempts to mimic the heat transfer and thermodynamic properties of the product-package system. Other RFID-based devices have been developed to indicate tampering via RFID signal, or use GPS data to report or record distribution route disruption but are typically used on large, high-value products. On-package indicators that are accurate and cheap enough to be widely used are still being pursued and must meet an extraordinarily low price level.

Similarly, work is being done on indicators that use binding-site chemistry to indicate specific spoilage organisms or toxins, but these suffer from the threat of false-positive indication as well as their own specificity; a broad spectrum detector would require a broad array of specific indicators and would be complex and prone to a high false-positive rate. Single-hazard detectors are finding potential markets in rapid detection testing for production systems to provide fast, accurate quality control and indication of contamination [21]. Having rapid detection methods will lower the cost and increase the accuracy of screening for some hazards to the point where even small manufacturers can have a good degree of product safety assurance based on their own data, rather than assurances from suppliers that deflect liability. This would be an enormous "grass roots-level" improvement for detection, interruption and containment of contamination episodes.

### 3.6 Optical Systems

Since many of the systems rely on customer inspection, specialized readers may not be available, but there is a wide range of sealing materials and devices that can aid in authentication as well as tamper detection if properly constructed. These usually depend on specialized printing processes and materials that require technical sophistication to produce, which will reduce the likelihood of casual counterfeiting and tampering, but as with the $100 "supernotes", are not impossible to duplicate given sufficient resources. Indeed, many of the "speciality" features such as color-shifting inks and fracture-evident dyes can be approximated with materials purchased in art supply stores. Holographic images, microprinting, frequency-specific pigments or additives that react to certain wavelengths of light and may change when damaged, and retroreflective or interferometric imagery that may contain both overt and covert features—often requiring a specialized viewer to resolve—can reduce counterfeiting or alteration. Many similar features are used to authenticate drivers' licenses.

### 3.7 Physical "Token" Systems and RFID

Wax and clay seals date into prehistory as a means of guaranteeing the authenticity of documents and products, and the inclusion of a physical verification token that is difficult to reproduce might offer some protection against counterfeit products. Software from major manufacturers has often been shipped with a complex authenticity seal that includes activation codes useable only with that copy. RFID devices carrying an authentication code encrypted in memory also have been proposed but neither of these systems, nor most systems relying on a physical object, eliminate the problems of "lifting"—removal of the token or indicator from one product to use in another—very well, and are still too expensive for individual consumer food package use. Additionally, some simpler RFID systems are quite easily cloned or have their encryption broken, even at a distance, and are the subject of a great deal of controversy because of their widespread use in passports, bank cards and other devices [22–24].

### 3.8 Product Authentication

For products such as pharmaceuticals that are increasingly targets of counterfeiters and potentially targets for attack, authentication systems have begun to be implemented. For food products, most of which already carry batch coding of some type, there is less impetus for these both because of complexity and cost. These systems typically depend on one or several systems for authentication which may include bar codes, special printing features such as moiré images and light-frequency-specific inks and product taggants that require a reader to translate, or numeric codes that can be verified via websites.

A more intriguing possibility lies with the potential to trap contaminated products during distribution or at the final point of sale by interfacing with inventory or point of purchase data systems to flag products as they are being shipped, shelved, and checked out of the store. This would require that current Universal Product Code (UPC) coding schemes include batch number information, but would also return low-cost data about batch shelf-time and turnover of product, something that still is often tediously hand-collected by manufacturer's representatives in stores.

### 3.9 Multipart Authentication

Many secure systems already require multipart identification and authentication. The combination of usernames and passwords on e-mail accounts is a good example. Similarly, the addition of secure authentication methods for encrypted data transfer systems such as PayPal® and others have made electronic commerce possible. Modern combinations of identification and authentication have made the use of private information fairly secure.

For packaged goods, it may be possible to utilize a matched coding system where customers or retailers can authenticate code numbers against batch numbers to verify their authenticity [25]. Similar systems have been used to activate software, cell phones and credit cards for some time. In theory, this could be almost entirely automated and only require a web page lookup for authentication, although this might present other vulnerabilities (website hacking or posting a false authentication webpage and then printing the counterfeit product with the false webpage's address to fool the consumer). The addition of additional features (such as product type, size, count that should be present in the validated product) can add another layer of security since a mismatch of product type or size even with an authenticated code would immediately raise suspicions.

The problem with these types of systems that may be quite useful with relatively low-volume items like pharmaceuticals, is the sheer quantity of material that is handled. Very few busy people will spend time authenticating a week's worth of groceries for a large family, and restaurant operations would be even more hectic than they are already. Instead, most consumers (if they consider it at all) depend on the historical use of media dissemination of information about product recalls based on lot numbers or code systems already used by manufacturers. While this is useful to consumers when problems are spotted and disseminated properly, it does not help to prevent the initial outbreak often required to flag the problem along with the attendant illnesses.

### 3.10 Security and the Base Rate Fallacy

For a security authentication or tamper evidence system to be acceptable, it must both very reliably detect attacks and even more reliably reject "false alarms" and it is usually the latter condition that is hardest to satisfy. Much as a smoke alarm that goes off at the slightest provocation is quickly disabled, safety indicators or systems that are constantly inaccurate are quickly disabled, discarded or ignored. Given the billions of units of packaged food handled daily, even an improbably small percentage of false alarms can cause large numbers of people to ignore the indicators or, worse, to panic over many perfectly good products being flagged. For example; if a detection system has a 0.1% false-positive rate, and the rate of actual occurrence (tampering or contamination) is one in a billion units, surveying a billion units will trigger 1,000,001 alarms (one "true" alarm plus 1,000,000 "false" alarms) and will still only give a one in a million chance of being correct.

For this reason, nearly all attempts at safety measures to ensure rigorous 100% inspection and validation in food manufacturing fail, and indeed this is the reason that many medical tests are repeated after a serious condition is diagnosed [26]. Risk management therefore becomes more a matter of building security into the system beforehand using ORM principles, rather than relying solely on inspecting it after the product is completed, a lesson taken from the "Total Quality Management" (TQM) principles that transformed Japanese manufacturing into exemplars of production quality [27].

## 4 SYSTEM FLEXIBILITY AND RESPONSE

While postprocess contamination is an ongoing concern, the realities of the tactical effectiveness of a contamination, package tampering or counterfeiting episode must be considered in a larger context of both, effectiveness in disrupting confidence in the food supply and ease of implementation. For an attacker to be effective these are both highly desirable results and a food safety system must likewise work to minimize these benefits.

As has previously been discussed, the ability of the existing food safety system to respond in an appropriate and timely manner is a primary component of any food system's security. While it may be minimally possible to shut down an airport in the event of a person bypassing security screening, it would be impossible to shut down the entire food production system. Additionally, few food customers would endure the kind of security screening required at airports to buy a liter of milk on their way home from work. Thus, access control for the food system is only feasible at the production and transportation level, although communication and indicators can be used at the consumer level.

Most retail-level food tampering is either accidental damage or the result of pilfering, often the result of putting candy and cereals on low shelves that children can easily reach. These and other "naturally" spoiled products are usually discarded or held for replacement on discovery by the store staff unless there is an obvious, recurring problem that requires contact with the manufacturer. This provides very little systemic information to guess where failed attempts at malicious tampering may have occurred.

It is difficult to determine under the best of circumstances which of those problems may have been caused by shipping damage, in-store damage or pilfering, or might have been the result of an attempt at malicious tampering. It is similarly unrealistic to expect every food retailer to accurately diagnose and report problems with every unsaleable product they discard. Thus we are left with examining those cases which are clearly the result of contamination or tampering, unfortunately too often involving incidents of injury, illness or death. Once the determination of a contamination or tampering outbreak has occurred, the resilience and responsiveness of the system is an utterly critical part of providing a timely response that does not shut down the entire national food supply.

Because of this, good security systems avoid "brittleness" that is, abrupt shutdown of the asset they are designated to protect when an incident occurs and to fail to or isolate the problem in a "resilient" fashion (i.e. a timely, useful and resource-efficient manner) [28]. Designing these responses in all types of industries is an ongoing, adaptive process (and is somewhat predictive in the best situations) that seeks to minimize the contamination or failure "space" after an incident while maintaining as much of the surrounding network of supply as possible [29]. Unfortunately, incidents that have occurred highlight the fragmented, opaque, uncoordinated, and unresponsive nature of the food safety system which makes it highly vulnerable to a systemic attack even using very simple methods.

### 4.1 Cascading Failure in the Food Processing and Packaging System

Cascading failure is generally defined as a failure that triggers a succession of downstream failures in other elements in a system of some type, such as a failure at a single electrical switching station that triggers a more massive power outage [30]. The food industry processes and combines a myriad of both naturally occurring and synthetic materials to provide our modern diet and this provides a target-rich environment for intentional contamination. Fortunately, nature has preceded this by providing a huge

range of naturally occurring hazards ranging in scale from oxidation to vermin. The food processing industry has had mechanisms in place for many years to inspect critical points during production and then initiate recalls in the event of accidental misprocessing or contamination. It generally works quite well if used in a timely manner.

However, for a response system to be effective it must be used and it must actually respond. Beginning before the events of 9/11, the Government Accounting Office has repeatedly highlighted the fragmented, uncoordinated and resource-poor nature of the food safety system with regard to intentional contamination [31–34]. Additionally, the opacity of the system contributes to delay and inaction. Under current regulations, disclosure of internal safety audits to government officials are not required, and recalls must be requested from company officials, slowing notification and adding delay during outbreaks of contamination [35]. This delay and restriction slows the response of the food safety system, adding to the severity of outbreaks and threatening whole commodity sectors when simple product recalls might have sufficed. No simple change or device for the processing or packaging technology can overcome this. A culture of quality and safety improvement based on improved practices, technology and regulation will have the biggest impact.

### 4.2 Safety System Failure Case Study: Peanut Corporation of America

The incidents of Peanut Corporation of America (PCA) intentionally shipping salmonella-contaminated peanut butter ingredients to other packers and food manufacturers showed the infrastructural weaknesses that may occur when safety measures break down. Inspectors of the plant failed to change practices at the facility, despite a similar incident beginning in 2004, in a similar processing plant owned by Con Agra only 75 miles away that had gone uncorrected for three years after notification of the FDA by a whistleblower, and subsequent company refusal to release test results. Con Agra's problems were only addressed when illnesses were finally reported, and even then their test records were never made public [36]. Although Con Agra completely rebuilt and improved its facility and operating procedures, PCA continued to operate with apparent impunity until deaths and illnesses were reported in 2008–2009, and the failure cascaded outward [37, 38]. A second PCA plant in Texas that was operated producing other nut products was never inspected at all, since it was never registered with the Texas Department of Agriculture although it shipped products nationally. As health problems came to light, other food manufacturers that used ingredients supplied by PCA were abruptly forced to recall nearly 4000 distinct products at tremendous expense, depressing peanut product sales by nearly 25% [39–41].

Many of these products had depended on the supplier's assurance—either informally or with Certificates of Analysis—to ensure the safety of their ingredients (or at least the absolution of liability) since many small operations do not have the capacity to do safety analyses. Thus, a supplier who ships contaminated product as an ingredient that is subsequently used in a plethora of other products highlights both the complexity and vulnerability of the food manufacturing system, and how a brittle failure could cripple an entire commodity sector by destroying public confidence.

From this we can see how an intentional incident could easily be caused by simple contamination or counterfeiting of a commonly used ingredient that is distributed through a system where the safety measures have broken down or are being ignored. Since food ingredients are not subject to even the minimal regulatory requirements of tamper

evidence applied to other products, and since there is often very little distinctive printing or packaging involved, the potential for contamination and counterfeiting are enormous. Often the only motivation for ingredient manufacturers to supply validation or tamper evidence features is the threat of involvement in legal action, and so as with consumer products, they tend toward the minimums necessary to prove due diligence on the part of the supplier. This may be a numbered tag or seal that must match the invoice that may have been sent separately by e-mail or fax; an excellent start, but hardly proof against a diligent tamperer.

## 5 CONCLUSION

While there are many types of technology that are being developed to make the food production and packaging system more secure, most of these fail in some aspect of reliability, simplicity, dependability, or consumer recognition. To balance this, the food processing, packaging and distribution industries have been fighting a pitched battle against numerous naturally occurring hazards on an ongoing basis for centuries. This has provided some remedial mechanisms for dealing with contamination incidents once they are detected and reported. The most useful practical approach is to assess threats accurately and manage risks appropriately, implement practical and useable detection methods where needed to make contamination difficult at all points in the food system, and to ensure that a response system that is both capable and operational is in place to contain and remediate intentional incidents on a timely basis.

An ORM strategy may provide a very good measure of prevention against casual tampering, but will likely not prevent a carefully targeted attack, particularly from intentionally contaminated ingredients that are created at a high level and widely distributed to product manufacturers. On-package detectors and tamper indication can "keep honest people honest" and give some indication of contamination, but are subject to all kinds of errors and lack of consumer awareness. There is a need for better design and a higher degree of upstream integration of tamper evidence in the package design process, rather than simply discharging fiduciary duty with adhesive tape and shrink wrap.

Detection methodologies, while being developed for rapid detection in plant operations and other inspections, may never pass into in-package use because of the combination of cost, possible toxicity, specificity of test and unacceptable false-positive rates. These can be extremely useful in the detection of contamination during spot checks as ingredients move from supplier to production lines. This is a function that has been abandoned in many operations in favor of "paper" assurances that avoid liability, creating enormous security loopholes; besides, small-manufacturer testing could be an enormously lucrative market for testing-kit manufacturers. Validation of products via multipath (package coding plus lookup lists on-line) might allow retail checkout or consumer screening of products once alerts have been sounded, but are unlikely to be used on a persistent basis by many consumers in the course of their day-to-day lives except as a spot check in the event of well-publicized recalls.

Finally, remediation systems exist, and can work quite well if used properly. A well-publicized recall can remove products from circulation very quickly, though perhaps at the cost of some good product being discarded. For a broad class of alerts such as the peanut butter outbreaks discussed in this article, it could also cause a depression in the sales for that particular item, but these are typically short-lived phenomena and

might be considered an acceptable and insurable security cost. Most importantly, if the detection-remediation system continues to be opaque, failing to act or delaying action for a very long time as it has done very badly in the given case and others, an outbreak may proliferate for months or even years until the symptoms, illnesses or deaths accumulate to a significant level, and the massive response is cripplingly brittle rather than adaptive. As has been too-adequately demonstrated, there is little difference in method between a malicious manufacturer operating for profit and a malicious fabricator trying to generate the public fear that is the hallmark of terrorism.

## REFERENCES


1. Federal Aviation Administration (2008). *FAA Systems Safety Handbook. Chapters 3,15 and Appendices e and h are recommended*. Available at http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/.
2. Hine, T. (1995). *The Total Package: The Evolution and Secret Meanings of Boxes, Bottles, Cans, and Tubes*. Little, Brown, & Co., New York, pp. 49–50.
3. (November 28, 2003). *Counterfeit Cosmetics Challenge Market Cosmetics Design Magazine*. Available at http://www.cosmeticsdesign.com/Products-Markets/Counterfeit-cosmetics-challenge-market.
4. (October 12, 2007). *The Truth About Fake Beauty*. Available at http://www.beautyheaven.com.au/article/perfume-the-foul-scent-of-a-fake.
5. U.S. Food and Drug Administration (2003). *Counterfeit Procrit*. Available at http://www.fda.gov/ForConsumers/ByAudience/ForPatientAdvocates/HIVandAIDSActivities/ucm125089.htm.
6. U.S. Food and Drug Administration (2002). *Important information about counterfeit EPOGEN*. Available at http://www.fda.gov/ForConsumers/ByAudience/ForPatientAdvocates/HIVandAIDSActivities/ucm125109.htm.
7. U.S. Food and Drug Administration (2005). *Counterfeit Drugs" Statement of Randall W. Lutter, Ph.D., Acting Associate Commissioner for Policy and Planning Food and Drug Administration before the Senate Subcommittee on Criminal Justice, Drug Policy, and Human Resources, Committee on Government Reform, November 1*. Available at http://www.fda.gov/NewsEvents/Testimony/ucm112670.htm.
8. Taylor, P. (2008). *EFPIA Says Traceability Pilot Will Start Next Year*. Available at http://www.outsourcing-pharma.com/On-your-radar/Patient-safety/EFPIA-says-traceability-pilot-will-start-next-year.
9. Bertrand, K. (2009). *Improve Security Through Packaging. Food Processing February 14, 2009*. Available at http://www.foodprocessing.com/articles/2006/027.html.
10. US Food and Drug Administration (2007). *FDA Warning on Mislabeled Monkfish*. Available at http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/2007/ucm108920.htm.
11. Government Accounting Office (2007). *Seafood Fraud: FDA Program Changes and Better Collaboration among Key Federal Agencies Could Improve Detection and Prevention*. Available at http://www.gao.gov/new.items/d09258.pdf.
12. Schneier, B. (1996). *Applied Cryptography*. John Wiley & Sons, New York, pp. 1–3.
13. (2003). *Code of Practice for the Tamper Evident Packaging (TEP) of Theraputic Goods*, 1st ed.. Australian Government Department on Health and Ageing, Therapeutic Goods Administration. Available at http://www.tga.gov.au/DOCS/pdf/tepcop.pdf.
14. *21 CFR 211.132 Current Good Manufacturing Practices for Finished Pharmaceuticals*. Available at http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=211.132.

15. FDA (2007). *Guidance for Industry. Importers and Filers: Food Security Preventative Measures Guidance*. Available at http://www.fda.gov/Food/FoodDefense/FoodSecurity/default.htm.
16. FDA (2007). *Guidance for Industry, Food Producers, Processors, and Transporters: Food Security Preventive Measures Guidance*. Available at http://www.fda.gov/Food/GuidanceComplianceRegulatoryInformation/GuidanceDocuments/FoodDefenseandEmergencyResponse/ucm083075.htm.
17. FDA (2007). *Dairy Farms, Bulk Milk Transporters, Bulk Milk Transfer Stations and Fluid Milk Processors: Food Security Preventive Measures Guidance*. Available at http://www.fda.gov/Food/GuidanceComplianceRegulatoryInformation/GuidanceDocuments/FoodDefenseand EmergencyResponse/ucm083049.htm.
18. EPRI Nuclear Executive Update (March, 2009). *Growing Risk of Counterfeit Items Emphasizes Need for Industry Guidance*. Available at http://mydocs.epri.com/docs/CorporateDocuments/Newsletters/NUC/2009-03/3a.html.
19. Mihm, S. (2006). *No Ordinary Counterfeit*. *New York Times* July 23. Available at http://www.nytimes.com/2006/07/23/magazine/23counterfeit.html?_r=1&scp=1&sq=No%20Ordinary%20Counterfeit&st=cse.
20. (1913). U.S. Patent 1,065,211. Bottle-Stopper. www.uspto.gov.
21. FDA (2003). *Testing for the Rapid Detection of Adulteration of Food, Report to Congress*. Available at http://webharvest.gov/peth04/20041021081954/www.fda.gov/oc/bioterrorism/report_congress.html.
22. *Hacker War Drives San Francisco RFID Cloning Passports. Engadget, 2/2/09*. Available at http://www.engadget.com/2009/02/02/video-hacker-war-drives-san-francisco-cloning-rfid-passports/.
23. Chris Paget's talk on drive-by RFID cloning. Available at http://video.google.com/videoplay?docid=-282861825889939203, with slides Available at uploads/paget_shmoocon_edl.ppt.
24. (2005). *RFID Chips in Car Keys and Gas Pump Pay Tags Carry Security Risks*. Press Release Johns Hopkins University. Available at http://www.jhu.edu/news_info/news/home05/jan05/rfid.html.
25. Johnston, R. G. (2004). *LAUR-04-8055 An Anti-Counterfeiting Strategy Using Numeric Tokens*. Available at http://www.fda.gov/OHRMS/DOCKETS/DOCKETS/05n0510/05N-0510-EC4-Attach-1.pdf.
26. Elmore, J. G., et al. (1998). Ten-year risk of false positive screening mammograms and clinical breast examinations. *N. Engl. J. Med.* **338**(16), 1089–1096. Available at http://www.ncbi.nlm.nih.gov/pubmed/9545356.
27. *BPIR.com History of Quality*. Available at http://www.bpir.com/total-quality-management-history-of-tqm-and-business-excellence-bpir.com.html.
28. Haimes, Y. Y., et al. (2008). Homeland security preparedness: balancing protection with resilience in emergent systems. *Syst. Eng.* **11**(4), P287–P308.
29. Beal, J. (2003) *Near-Optimal Distributed Failure Circumscription* AI Memo 2003-017. Massachusetts Institute of Technology Artificial Intelligence Laboratory. Available at ftp://publications.ai.mit.edu/ai-publications/2003/AIM-2003-017.pdf.
30. Dobson, I., et al. (2007). *Complex Systems Analysis of Series of Blackouts: Cascading Failure, Critical Points, and Self Organization*. Chaos 17, 026103 (1–12). American Institute of Physics. Available at http://eceserv0.ece.wisc.edu/~dobson/PAPERS/dobsonCHAOS07.pdf.
31. U.S. Government Accounting Office (1999). *Food Safety: Agencies Should Further Test Plans for Responding to Deliberate Contamination*. Available at http://www.gao.gov/new.items/rc00003.pdf.
32. U.S. Government Accounting Office (2003). *Voluntary Efforts are Under Way, but Federal Agencies Cannot Fully Assess their Implementation*. Available at http://www.gao.gov/new.items/d03342.pdf.

33. U.S. Government Accounting Office (2007). *Federal Oversight of Food Safety: High-Risk Designation Can Bring Needed Attention to Fragmented System*. Available at http://www.gao.gov/new.items/d07449t.pdf.

34. *U.S. Government Accounting Office (2008). Federal Oversight of Food Safety: FDA has Provided Few Details on the Resources and Strategies Needed to Implement its Food Protection Plan*. Available at http://www.gao.gov/new.items/d08909t.pdf.

35. Harris, G. (2009). *Peanut Product Recall Took Company Approval. New York Times. February 3, 2009*. Available at http://www.nytimes.com/2009/02/03/health/policy/03peanut.html.

36. *Moss, M. (2009). Peanut Case Shows Holes in Safety Net. New York Times, February 9, 2009*. Available at http://www.nytimes.com/2009/02/09/us/09peanuts.html.

37. Harris, G. (2009). *Peanut Products Sent out Before Tests. New York Times, February 12, 2009*. Available at http://www.nytimes.com/2009/02/12/health/policy/12peanut.html.

38. Centers for Disease Control (2009). *Investigation Update: Outbreak of Salmonella typhimurium Infections, 2008–2009. Update for April 29, 2009 (FINAL web update)*. Available at http://www.cdc.gov/salmonella/typhimurium/update.html

39. Cook, C. (2009). *Peanut Recall's Ripples Feel Like Tidal Wave for Some Companies. New York Times February 26*. Available at http://www.nytimes.com/2009/02/26/business/smallbusiness/26sbiz.html.

40. Martin, A., and Robbins, L. (2009). *Fallout Widens as Buyers Shun Peanut Butter. New York Times February 7th*. Available at http://www.nytimes.com/2009/02/07/business/07peanut.html.

41. Harris, G. (2009). *Peanut Recall Leads to Criminal Investigation. New York Times January 31*. Available at http://www.nytimes.com/2009/01/31/health/31peanut.html?_r=1.

# EARLY DETECTION AND DIAGNOSIS OF HIGH-CONSEQUENCE PLANT PESTS IN THE UNITED STATES

KITTY F. CARDWELL AND WILLIAM J. HOFFMAN
*United States Department of Agriculture, Washington, D.C.*

## 1 EARLY DETECTION AND DIAGNOSIS OF HIGH-CONSEQUENCE PLANT PESTS IN THE UNITED STATES

There exists well-documented historic precedent of the intentional use of biological organisms as weapons to strike against a target enemy either directly (human pathogens) or by

adversely impacting its agricultural security (animal and plant pathogens) [1–3]. Government sponsored research into the development of biological weapons for use against humans, livestock, and crops was prevalent during the early decades of the twentieth century. Most government bioweapons programs included research on the culture and testing of disease agents intended specifically for use against livestock and food crops. There is concern because no elaborate delivery technologies or methods are necessary for clandestine, economically targeted bioweapon attacks on agricultural crops [2]. Many exotic plant pathogens are already highly infectious with high reproductive potential that facilitate rapid exponential epidemic development when environmental conditions are favorable [3, 4]. Furthermore, plant pathogens are generally not infectious to human handlers; inocula are available from infected crops around the world; and collection, increase, and delivery to a target crop and region is not technologically difficult. The US National Research Council concluded in a 2002 report that the potential and (consequences of) deliberate bioterrorism attacks directed at US agriculture needs to be recognized as a serious threat to the United States and its agricultural economy [3, 5]. Bioterrorism is perhaps the most extreme example of the larger issue of invasive species of exotic pests and pathogens to new areas as a result of deliberate or inadvertent human activity or of more ”natural” spread [2].

Agricultural emergencies, whether deliberately caused or natural, follow the same notional phases as any disaster, including biological and chemical attacks on agriculture, animals, or civilians. Phase 1 includes detection and diagnosis; phase 2 involves a systematic monitoring to characterize and delimit the area of outbreak and mitigation in the outbreak area; and phase 3 is the longer-term response and recovery activities. This article concerns phase 1—early detection and diagnosis of a new biological threat to agriculture or valuable natural resources [6].

In the United States, there are an estimated 1 billion acres of crop, forest, and range lands. It is physically impossible to closely monitor all of this area to achieve early detection of newly introduced pests or pathogens. As such, these resources make strategically and tactically attractive targets to those who would strive to provoke food shortages, loss of valued ecosystem, economic damage either through loss of trade or loss of competitiveness, public loss of confidence in food safety and security, or direct damage to humans and/or animals [3]. Agricultural crops are particularly vulnerable due to ease of access and to the logistical challenges of continuous surveillance. In 2004, an estimated 155 million acres were planted with corn and soybeans, alone. Numerous other crops are grown over large acreages and/or are high-dollar intensively grown specialty crops such as grapes, citrus, and vegetables.

Because of the challenges of surveillance over such a vast area, there is the potential of a long lag time between the introduction of a pathogen or pest (intentional or natural) and the detection. Likewise, any delay in diagnostic processing once detected, would further delay appropriate response. For example, citrus canker, a bacterial disease of oranges, is believed to have been in Florida at least 2 years before it was detected and diagnosed [7]. Likewise, the emerald ash borer, a devastating invasive insect pest of ash trees, was estimated to have been in Michigan 5 years before it was discovered near Detroit, Michigan [8]. During this time, these pests and diseases spread to the extent that there is little hope that containment and eradication can be successful. Once an exotic or invasive organism has been detected, the need for intensive monitoring and sample diagnosis during a phase 2, also creates significant logistical challenges. Successful execution of a

monitoring, early detection, and diagnosis program improves the chances of responding quickly, minimizing impact, and reducing time to total recovery.

The purpose of this article is to explore the technical and infrastructural challenges to early detection, and rapid and accurate diagnosis of high-consequence exotic pests and pathogens.

## 2 DETECTION: MONITORING AND SURVEILLANCE

High-consequence pest monitoring and surveillance is a series of activities that combines biological science and human performance. This section will examine three different subsets of these efforts: formal human (active) systematic surveillance, nonformal human (passive) surveillance, and remote or automated surveillance. The terms *formal* and *nonformal*, indicate the level of government oversight and organization. These activities will be analyzed using a variation of Gilbert's behavioral engineering model [9]; examining the capacity, knowledge, and motivation of the individuals and organizations involved.

### 2.1 Formal (Active) Human Surveillance

Formal human active surveillance of high-consequence exotic crop pests are led by the US Department of Homeland Security (DHS)'s Customs and Border Inspection (CBI) Program and the United States Department of Agriculture (USDA)'s Animal and Plant Health Inspection Service (APHIS). These organizations work together in surveillance attempts designed to *exclude* pests from coming into the country. APHIS works to *monitor* regulatory pest problems for domestic establishment [10].

***2.1.1 Exclusion.*** The homeland security act of 2002 transferred federal agricultural port inspection responsibility from APHIS' Plant Protection and Quarantine (PPQ) division to the DHS-CBI [11]. The bulk of these activities to exclude 6000 miles of borders and 100,000 miles of shoreline [12] take place at 317 border inspection stations, 161 of which are staffed with agricultural specialists [11]. The daily traffic across these borders includes 1.1 million people, 45,000 trucks, 550 vessels, 2500 aircraft, and 341,000 personal vehicles [12]. Each day, an average of 1145 food product seizures take place as a result of short range electronic surveillance, interviews, canine sweeps, and hand searches. APHIS conducts an extensive training program and procedure manual development, provides guidance on inspection targeting and alert notification, and collaborates on port of entry review in order to bolster Customs and Boarder Patrol (CBP) efforts [11]; and thus remains involved with border pest exclusion.

*Capacity.* While efforts of the CBP agricultural specialists are laudable, there are two important reasons why they cannot possibly exclude all high-consequence pests and pathogens from entering the country. First, not all such pests enter the United States through registered border crossings. This includes pests that may enter the country naturally through the air or are carried by those crossing the border illegally [13]. Second, to intercept those pests and pathogens that do go through the inspection process, additional requirements would be needed to include fumigation of all manner of conveyances from countries where target pests are found as well as more intensive questioning and inspection of foreign visitors and returning citizens [14].

*Knowledge.* The CBP agricultural specialists are adequately trained [11] to carry out their mission. However, cross agency communication has impeded implementation of procedure manual updates and agricultural pest alerts. This has caused delays in getting timely information to those on agricultural homeland security's front lines [11].

*Motivation.* Legislators, farm organizations, and the National Plant Board have argued that agricultural border protection would be better off with the USDA, a department more focused on pest exclusion and food security [15–17]. Agricultural pest exclusion is one of many important priorities of CBP, an organization focused on the broad mission of ensuring safety and security while facilitating trade and travel. Within CBP, agricultural related border security competes for resources in an extremely broad and high consequence threat pool. District CBP agricultural liaisons provide regular communication to field managers, which helps pest exclusion receive the operational focus it deserves [11].

After a high-consequence crop pest does cross the US border, detection depends on domestic monitoring systems, both formal and nonformal surveillance activities.

***2.1.2 Monitoring.*** The USDA estimates that introduced plant pests account for annual agricultural losses of $41 billion and it provides leadership for monitoring domestic and regulated pests. An important formal monitoring program is the Cooperative Agricultural Pest Survey (CAPS) operated by APHIS. The CAPS provides resources to state departments of agriculture in all 50 states and 3 US territories to track more than 400 pests [18]. Approximately 40 of these pests are identified as national priorities by the CAPS program and the balance are proposed as local priorities. Detected high-consequence crop pests that are subject to regulatory action are immediately reported by CAPS survey participants to APHIS/PPQ emergency programs staff and are sent for confirmation by that group's national identification services. All survey data is submitted to the National Agricultural Pest Information System to contribute to national analysis.

Soybean rust, a serious soybean pathogen, was detected late in 2004. Prior to the 2005 soybean growing season, the USDA developed a sentinel plot based surveillance system to monitor disease progress throughout the year and provide near real-time information for pest managers. This has developed into the integrated pest management Pest Information Platform for Extension and Education (ipmPIPE), a partnership funded by the USDA and client industry, and managed by the cooperative extension systems across the country [19].

*Capacity.* In 2006, the CAPS program distributed approximately $5 million to all of the states and US territories combined. The state departments of agriculture participants in the CAPS program have lamented that the cooperative agreements they receive can only fund one survey coordinator and a few survey programs [18]. Similarly, the ipmPIPE has yet to achieve a stable funding source for the $2.277 million needed for core operations. While these efforts are highly leveraged through state government and land grant university funds, this level of funding does not purchase the type of capacity needed to thoroughly and systematically monitor high-consequence pests.

*Knowledge.* These programs thoughtfully set national priorities and the decentralized nature provides the ground truths from the states and regions. State departments of

agriculture and state cooperative extension service's often work hand in glove with land grant university researchers so that pest monitoring programs are informed by timely research [21].

*Motivation.* State Plant Regulatory Officers who participate in the CAPS program are the lead state government officials in PPQ issues. These individuals are highly motivated to monitor plant pests and correct problems before they are uncontrollable. Cooperative extension officials are motivated to collect data from an academic perspective and to act as an information hub in service to their clientele. This motivation is particularly keen when their clientele faces an imminent threat. However, focus on such a threat could draw attention away from other vulnerable pathways.

### 2.2 Nonformal (Passive) Human Surveillance

There are many people involved with crop pest management who are not involved with government sponsored surveillance. Approximately 90% of row crops and vegetable acres are scouted for endemic weeds, insects, and/or diseases that routinely threaten their crop's profitability. The vast majority of this scouting is performed by owner operators. Approximately 10% of the row crop acreage is scouted by chemical dealers and a similar amount is scouted by independent crop consultants. Certified Crop Advisor (CCA) utilization increases significantly for vegetable and other high-value crops [22].

During the last 5 years, cooperative extension services have conducted a campaign to incorporate exotic and invasive weed, insect, and disease detection into normal scouting activities. Training "first detectors", an activity led in part by the National Plant Diagnostic Network (NPDN), includes instruction on (i) the importance of high-consequence exotic plant pest detection; (ii) what scouts should do if they see something they do not recognize; and (iii) exotic pests that crops scouts should be on the lookout for in addition to routine pests. Many training participants were added to a first detector "registry" that will allow the NPDN to alert them based on recent pest finds and conditions favorable to disease presence [23]. Timely communications from the NPDN, coupled with information from the ipmPIPE, farm press county extension agents, and other information sources, could help crop scouts keep alert for exotic pests as they perform regular scouting activities.

*Capacity.* In addition to the operators of the 2 million US farms [24], there are 14,000 certified crop advisors [25] who make regular continuing education a part of their professional development. These crop advisors include chemical manufacturer representatives, chemical retailers, extension agents, and independent consultants. This is a massive capacity for nonformal surveillance if it can be properly marshaled, that has the potential to provide more surveillance samples than could be diagnosed. Therefore, diagnostic capacity must be maintained and improved as nonformal surveillance develops.

*Knowledge.* Reaching this prospective surveillance force with timely and crop specific information is a significant challenge. While the aforementioned groups who typically participate in the CCA program have made great progress as information conduits, providing information to growers and other pest management players is a limiting factor in nonformal surveillance.

*Motivation.* Growers are profit motivated and must attend to a complex set of details within a crop year if their bottom line is to be optimized. While some exotic pests

**TABLE 1 The degree of challenge (high, medium, or low) associated with national workforce capacity, knowledge, and motivation related to plant pest detection strategies**

| Strategy | Capacity | Knowledge | Motivation |
|---|---|---|---|
| Offshore and border monitoring for exclusion | *High*: extensive borders, coastline, and import volume | *Medium*: inter-and intra governmental communications | *Medium*: Agricultural pest detection competes with other priorities |
| Formal domestic monitoring | *High*: large geographic area to cover | *Low*: well established formal agricultural education system | *Low*: local and state-based practitioners driven by local economy and client needs |
| Nonformal domestic monitoring | *Medium*: first detector volume can create overwhelming diagnostic surge | *High*: large and diverse population needing real-time information | *Medium*: profit impact of exotic pest(s) must be clear to first detectors |

may pose a threat to the current year's yield, they may not be the bottom line threat that first comes to mind.

A summary of the challenges for each of the types of surveillance activities is found in Table 1. The remainder of the article will discuss how risk analysis, remote electronic or automated surveillance, increasing laboratory throughput, and diagnostic networks are integral to surveillance programs.

## 3 ESTIMATING RISK TO ORIENT SURVEILLANCE

The surveillance systems mentioned in the previous sections are highly dependent on human resources, which are dependent on the capacity, knowledge, and motivation of system players. Whether it is DHS and APHIS inspectors at points of entry, county extension agents monitoring sentinel plots, industry experts, university extension specialists conducting mobile surveillance, or farmers and their advisors walking into fields to take samples, a large number of trained people are required in the field. For best results their efforts must be coordinated [21, 26] and guided by the best available information about risk. Given that the largest constraint to monitoring agricultural resources in the United States is the tremendous area that must be covered, and that human resources are limited, ideal monitoring systems must also rely on technology(ies) capable of anticipating threat and risk levels and automated detection processes. In this section we will discuss risk/threat evaluation techniques and remote sensing technologies that promote efficient and timely field-based surveillance by delivering biological and/or probability information prior to physical field scouting.

### 3.1 Threat analysis

There are a range of approaches to threat analysis beginning with monitoring offshore pest movements [27], aerobiological modeling [28] and pathway analyses to determine

possible modes of arrival [29–36], population dynamic models to assess threat of given plant pathogens as biological weapons [4], and disease progress models linked to climate models and geographic information systems (GIS) to predict probability of infection/establishment and direction of spread once introduced [3, 37].

### 3.2 Pathway Analyses

Pathways of pest entry and spread are anticipated and assigned risk values by pathway analyses [38]. These analyses assign probabilities to natural entry, deliberate or unintentional introduction, establishment in the environment, rate of spread, and epidemic potential. Pathways can include commodity and seed trade, movement of plants and animals, conveyances that harbor hitchhiking biota; people who smuggle, travel with native plants or plant parts, traffic in traditional medicinal plants, or intend to commit sabotage; and packing materials (particularly wood), potting media, even garbage. Target pests analyzed by APHIS are primarily regulatory threats as established by pest risk analyses. Knowing the most probable entry pathway(s) allows APHIS and DHS to focus interception efforts critical points. An indicator of deliberate introduction of a damaging pest would be if it were to occur outside of the most probable entry pathways [39].

### 3.3 Models

Plant pests and pathogens that are amenable to increase by scaled-up *in vitro* production, are stabile in storage, easy to transport and deliver are most likely to be developed as biological weapons. Whether the delivery results in establishment, dispersal, and damage, however, depends on the disease triangle: availability of susceptible host, climatic factors, and the inherent biology and physical characteristics of the organism [3, 4, 28]. The probability of any of these processes can be analyzed using mathematical models to assess risk of damage by a biological agent were it to be introduced intentionally. The most basic models used to assess potential impact of an introduced organism are "simple interest" (in the case of point source introductions of high levels of initial inoculum) or "compound interest" (where there would be cycles of inoculum build up over time) [3]. In the simple interest model, high risk is assigned to organisms that have highly effective inoculum (a high ratio of infection achieved over total inoculum propagules) over the broadest possible range of environments (which includes host genetics). For the compound interest model, high risk is assigned to those organisms that have a high rate of reproduction and infection over a broad range of possible environments. In this model, low amounts of inoculum could be introduced and would be hard to detect until an epidemic was fully blown, potentially causing impact in an area much larger than the original inoculation points.

Modeling to assess risk of an invasive pest/pathogen (intentionally produced as a bioweapon or inadvertent), which establishes and damages the population growth rate ($R$), is the driving variable. Persistence of an organism over season can also be a function of $R$ as overseason survival is a probability function of mortality of progeny. Thus high $R$ pests and pathogens are generally assessed as higher risk of becoming endemic under appropriate climatic conditions, particularly if the dispersal is aerobiological. High $R$ pests with a persistent overseasoning structure, that is a structure that ensures durability of the propagule, are the most likely to become established.

***3.3.1 Aerobiological Models.*** Aerobiology is the study of the physical process of movement of organisms from one geographic location to another by floating, soaring, or flying through the atmosphere [28]. Pests and pathogens that disperse long distances readily are most likely to have wide-spread impact. Many plant pests and pathogens are physically designed for long-distance aerial transport, and these are subject to the dynamic but definable routes created by planetary airflows [28]. Aerobiological models are used to predict when and where a target organism might reach a location, and this helps establish the "normal" probability of appearance by natural processes. Many organisms that move long distances in the air, also move locally between the infected source and new locations. For the purpose of surveillance advisories, the probability of arrival of a given invasive organism to a new location can be forecast once host availability and climate variables are integrated with the knowledge of the biology of the organism. Likewise, an unknown source of origin can be estimated by a trace backwards of atmospheric pathways. The most widely used atmospheric transport model for aerobiological applications is the National Oceanic and Atmospheric Administration (NOAA)'s HYSPLIT (hybrid single-particle Lagrangian integrated trajectory) model. Both APHIS and PIPE use this type of modeling [3, 24, 37].

***3.3.2 Weather-based GIS and Disease/Pest Warning Models.*** Climate-based disease and pest forecast models are dependant upon accurate climatological data on a meaningful geographic scale. Precision of climate data such as 24/7 temperature, dew point, and duration at or below dew point is a function of density of weather station data loggers and edaphic/topographic conditions of a region [40]. Relatively flat terrain such as the great plains and Midwestern region of the United States can expect reasonable precision of forecast with fewer data points over a larger scale. Conversely, complex topography can present highly diverse conditions on a fine scale. Thus, climate-based disease forecast in areas such as the Pacific northwest must take into account topography, altitude driven temperature and dew point variations, precipitation shadows, and so on. A denser network of weather data stations is required and interpolation between these cannot be generalized. Customized climate forecasts can be developed for specific production zones.

Once climate model uncertainties and errors are understood, accurate disease severity forecasts can be generated based on biological characteristics of the organism or a proxy with similar attributes and known environmental parameters (Figure 1). The primary attribute that describes epidemiologic potential of an organism is its fitness or basic reproductive number (R), defined as a mean of new infections that result from an individual infection locus, or basically, the average number of progeny that an individual produces on a susceptible host under average (climatic) conditions [4, 41, 42]. Modelers understand how the R of each organism is affected by a range of climatic conditions. Some plant pathogens are highly dependent on climatic conditions during the process of infection of the host; so the probability of infection is a function of a threshold of effective inoculum and promoting climatic conditions. Other organism attributes that relate to R are length of latency or incubation, and short- to long-term progeny survival.

***3.3.3 Population Dynamics Models:.*** Pest/pathogen population dynamics models can incorporate the final side of the triangle, the host. Host plant growth can be modeled based on factors such as phenology, degree days, and precipitation. The within- and between-season dynamic between host plant and pathogen can be simulated using reciprocal, coupled differential equation models [4, 44, 45]. The susceptible host is the essential

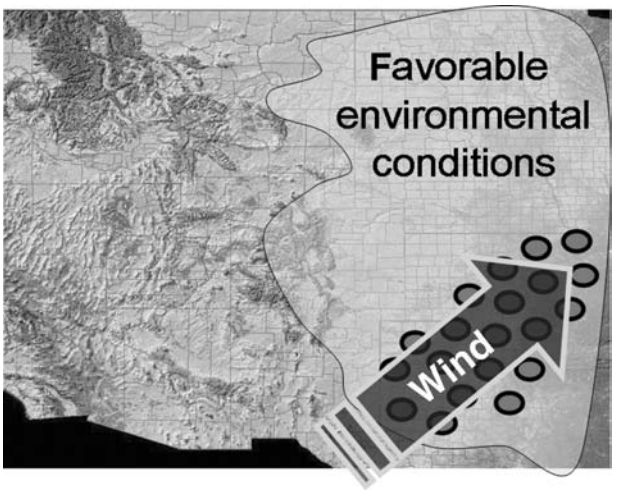



**FIGURE 1** Mitigation efforts are most efficiently implemented when ground and remote surveillance inform aerobiological and HYSPLIT models to predict likely disease spread.

environment for the pathogen to develop, and successful development of the pathogen may have deleterious effects on its host. Strain composition and virulence diversity in populations tend to be well understood. Some pathogens are highly mutable and exist in populations polymorphic in virulence and aggressive on their host. These are managed by shifting host plant resistance to new varieties as resistance is defeated. In the presence of these types of pathogens, host resistance may break down gradually, over several years, or abruptly resulting in significant crop losses. Any sudden shift in virulence under these conditions could not be easily attributable; however, highly mutable pathogen populations are among some of the most destructive in the world. Other classes of pathogens have more stable population composition so that resistant varieties are more durable. Any sudden shift in virulence or aggressiveness of this type of pathogen would raise questions about how/why it happened, and often can be attributable to the specific introduction of a different strain.

***3.3.4 Syndromic Analysis:.*** Intentional introduction of a plant pest or pathogen is likely to result in a pattern of disease outbreak that does not conform with the expected [3]. Pests and pathogens that are airborne and expected to fall out of air currents should distribute in a normal or random pattern across a predictable geographic swath. If the pattern of discovery is discrete and geographically distinct, this would fall outside of the expected and raise suspicion. Delivery of spores via a ground sprayer would result in a nonrandom disease presentation, such as in a line pattern along a fence row or road [3]. Other anomalies would be temporal and based on the likelihood of severity of outbreak at any given time. These anomalies are evaluated in real time on the basis of current diagnostic data, such as generated by NPDN labs (Figure 2), against the backdrop of historic data and/or climate-based forecast models of disease and pest outbreak. An outbreak that is too severe, too early in a growing season is a temporal anomaly [39]. Any departure from usual in disease or pest outbreak aggressiveness, severity, or incidence should trigger an investigation. Any change in intensity of mycotoxin production, particularly in the absence of a corresponding causal climatic factor, should be immediately investigated.

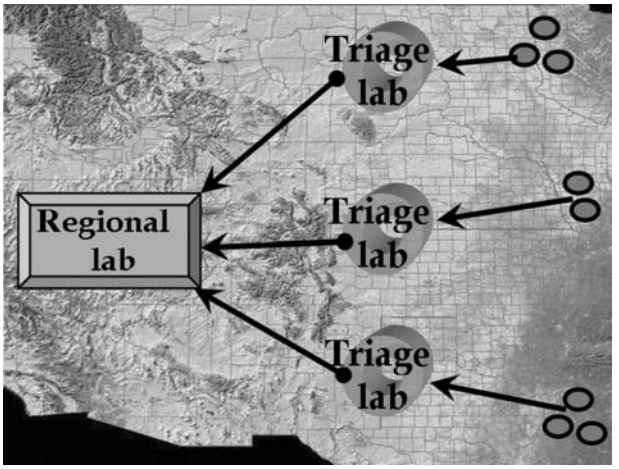



**FIGURE 2** Syndromic analysis of data collected at state-based (triage) diadnostic laboratories. Triage labs conduct preliminary analysis. Regional and national labs perform confirmatory assays.

It is paramount that analysts are trained, and automated analytical software developed to identify such anomalies, and that background data be archived in a format that is standardized for analysis.

### 3.4 Remote or Automated Surveillance

Another way to supplement and focus monitoring and surveillance to narrow down the search parameters to manageable dimensions is to develop and deploy remote and/or automated sensing devices. This not only has the greatest immediate potential to supplement active surveillance capacity but also a long-term potential to supplement passive surveillance and exclusion.

The research community is developing parameters required for detection, for example, specific nucleic acid, proteomic, or spectral signatures of specific organisms [6]. Technologies for monitoring and notification about biological organisms in plant systems must be sensitive enough to identify the signature at very low concentrations, be associated with understanding of effective inoculum levels on available hosts (infectivity relative to environment), and be prompt enough to effect a successful control response. Ideally, such sensing devices could be designed to emit a signal to a remote monitor when a positive reaction or detection has occurred [45]. However, most sensors for environmental biological monitoring still require at least some human manipulation such as substrate collection and transport for laboratory analysis. For example, fungal spores can be collected in outdoor aerial traps [46, 47], water traps [48], indoor suction traps [49] (Zhou). Krupa et al. have used the National Oceanic Atmospheric Deposition (NADP)/National Trends Network (NTN) water traps to monitor rain-deposited soybean rust in samples of rainwater [50, 51]. As few as two soybean rust spores can be detected with polymerase chain reaction (PCR) in rainwater samples collected in NOAA, National Atmospheric Deposition Program traps [51, 52]. Although spore capture has not yet been significantly correlated with crop disease, spores have been detected as far north as Canada.

Nevertheless, atmospheric trapping of specific plant pathogens can only be a useful monitoring tool if there is no bottle neck in sample analysis. In the absence of *in situ*

analysis systems, all remote trap samples must be collected and returned to the lab for processing. Therefore, the last aspect that we deal with in this paper is actually one of the most rate limiting aspects of all surveillance and monitoring programs, that of laboratory throughput capacity.

## 4 DIAGNOSTICS

### 4.1 Laboratory Throughput

Whether by trapping, sentinel plot, mobile random survey, systematic survey, or by heightened awareness of a cadre of public and private first detectors, the consequence of regular monitoring can be an exponential increase in the numbers of samples requiring rapid diagnostic analysis [53].

When there is an emergency, and either a high-consequence biological agent or a new find of other high-consequence or quarantined pest has been detected, a surge of samples flowing into laboratories can be expected. Sampling needed to characterize and delimit an important outbreak, can result in a surge of samples and quickly overwhelm the capacity of the laboratory to process the material opportunely. This is especially true when those who develop the sampling plans, for active surveillance either before or after first detection, do so without consideration of existing surge capacity.

Surge management is dependent on human resources, physical space, reagent, and equipment availability within a laboratory [39, 54]. Table 2 shows a comparison of the three most common diagnostic methods for plant pathogen diagnosis. Traditional (incubation, microscopy, and taxonomic identification), molecular, and antibody-based diagnostics form the basis of the standard operating procedures (SOPs) that are developed for plant pathogen Select Agents and other high-consequence pathogens and pests. All plant diagnostic clinics are prepared for the traditional cultural diagnostic tests, and may use these as a first-order assay in the absence of a risk alert or other indication of unusual outbreak. PCR and immunoassay techniques are relatively quicker, more accurate, and preferred for high-consequence diagnostics. However, during a sample surge these techniques may be limited due to the level of training and testing (certification) required for personnel and inadequate supply of reagents [54]. Often, diagnostic confirmation requiring a high level of confidence will employ various technologies concurrently. An example of this was the SOP developed for diagnosis of the Sudden Oak Death pathogen, *Phytophthora ramorum*, which allowed for cultural, immunological, and nested PCR methods, depending on the level of capability and accreditation of the lab [55–57].

The challenges to large-scale screening of agricultural biological samples have been demonstrated both in simulated and actual surge events (refer to ICLN chapter). Individual laboratories, by themselves, can become overwhelmed in the case of a sudden influx of samples. Fulfilling the US biodefense strategy requires that laboratory response systems become capable of detecting biological agents from large numbers of samples quickly and cost effectively [54]. Alternative options exist, which range from investing in automated biological agent testing systems to increasing the throughput of national laboratories [53, 54, 58], to developing cascade protocols whereby diagnostic laboratories experiencing a surge can distribute samples over a network of laboratories significantly increasing the number of technical hours that can be brought to bear. Either of these options requires a national investment and would be effective regardless of the original cause of the surge (from intentional to natural).

**TABLE 2 Comparison of Diagnostic Methods**

| Variables | Traditional | Immunoassay | PCR |
|---|---|---|---|
| Personnel needed | 4 | 2 | 4 |
| Analysis time | 2–10 d | 2 h | 12 h |
| Throughput/day | >100 | | >200 |
| Upfront costs | Modest | | Moderate |
| Sustained costs | Low | | Low |
| Confidence | Agent may not grow on media | Are specific to genus with high confidence, can be very specific to viral strains | Cross contamination moderate, high human error |
| Key characteristics | Ultimate diagnostic tool for confirmation | Quick assay to confirm presence/absence of specific genera | Flexible conditions for assay development |
| Pros | Gold standard, positive identification of organisms | Confirmation and diagnosis inexpensive, relatively simple; monoclonal antibodies can be developed to be general or specific, polyclonal antibodies can be developed quickly | High system flexibility, protocols easily modified, detects killed organisms |
| Cons | Toxins not detected, very slow, may require more extensive testing, agent may not grow in artificial media, unable to detect killed organisms | Multiple steps increase opportunity for human error | Many opportunities for human error, flexibility increases the opportunity for applying wrong protocol |
| | | Variability in access to standard pathogens/ clonal cell lines among manufacturers, more strain specificity with monoclonal antibodies, but there are no standard US cell lines. | |

## 4.2 US Laboratory Network System

The NPDN [20] is a hub and spoke system of non-Federal laboratories distributed across the United States and territories, with varying capacity to effect determinant diagnoses (Figure 3). Every state and territory has at least one public diagnostic laboratory (Land Grant University plant clinic and/or State Department of Agriculture regulatory laboratory) which is a member of the NPDN. There are five regional hub laboratories that, in addition to processing samples submitted from within their state, coordinate diagnostics

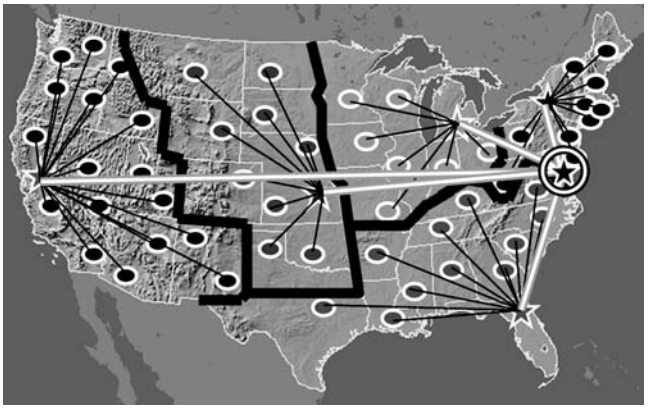


**FIGURE 3** The "hub and spoke" structure of the NPDN allows: (i) regional coordination; (ii) surge overflow, and (iii) national sample triage.

and information flow within each region. All of the laboratories are linked by a secured messaging system designed to alert diagnosticians of an increased risk of seeing a specific high-consequence biological agent. Protocols are in place for every state defining communications and information pathways and sampling flow operating procedures. By employing this network of existing public plant diagnostic laboratories, the United States has increased surge capacity for a moderate Federal investment.

Some NPDN laboratories are PCR trained and certified; others will be able to provide triage by examining and eliminating lower-consequence endemic pests and pathogens. However, when a triage laboratory receives a sample that it suspects to be an agent of national concern (whether homeland security or regulatory quarantine), the communications protocol for that state and region kicks into operation. One aspect of that protocol is to consult with the regional hub diagnostician and/or the specified Federal Reference Laboratory for the suspect agent. All presumptive positive samples of regulatory agents are forwarded to APHIS PPQ National Identification Services Laboratories for confirmatory diagnosis (Figure 4).

All NPDN labs have digital diagnostics capability that allows real-time viewing of the same diagnostic features in two or more geographically separate laboratories via the Internet (Figure 5). This distance consultation provides first detectors and state diagnosticians local access to national diagnostic expertise in real time. Digital diagnostics have proven to reduce overall laboratory burden through triage, while improving diagnostic turn-around time on critical, presumptive high-consequence samples [23].

## 5 CONCLUSIONS

The United States have over a billion acres of food, fiber, feed, and fuel production agriculture. Agriculture and forestry products combined are a cornerstone of the North American economy, providing social stability through food security and natural environments. Production agriculture is also being tapped to produce combustible fuels, exponentially increasing its overall value to producers and the American people. US agriculture could be considered a large, soft target to those who would want to strike at

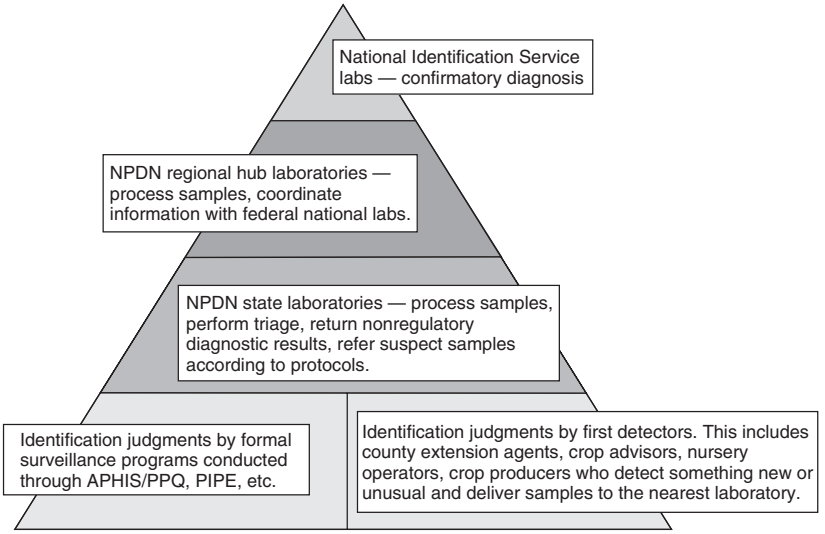



**FIGURE 4** Diagnostic and triage hierarchy for US plant pest detection.

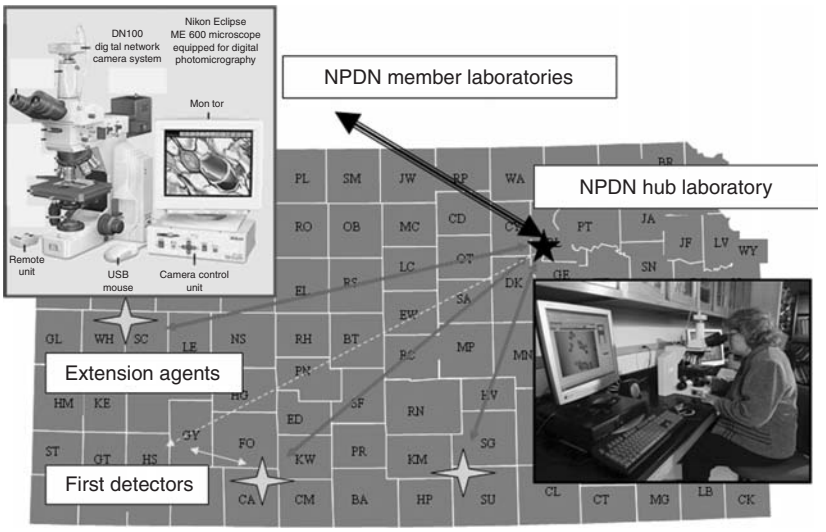



**FIGURE 5** All NPDN member laboratories and properly equipped county extension offices can receive distance diagnostic support through digital image sharing on a state, regional, and national level.

the economy, the social stability, or the sense of safety of the US citizenry. It would be technically easy to do this.

Early detection and diagnosis of pests and diseases of plants is the best way to limit spread and impact, whether they arrive naturally or are introduced deliberately. This article has described the US plant pest detection and diagnostic systems. These systems are good, but vulnerability has increased due to globalization, terrorism, and the increasing

value of agricultural products around the world. This increasing vulnerability will exacerbate current challenges. Therefore, it is in the country's best interest to pursue research and infrastructural improvements to foster the security of that system.

### 5.1 Research

Monitoring and surveillance needs:

- improved biologically based survey, sentinel, and sampling protocols
- field-based diagnostic kits
- ongoing threat and pathway analyses
- epidemiology and aerobiology
- syndromic analysis—the study of populations within communities and environments
- remote/automated surveillance (microarrays and conductors).

Diagnostic needs:

- additional validated diagnostic assays
- automation systems.

### 5.2 Infrastructure

Planning and practice are essential to ensure an effective response to urgent public health threats [39]. This is true also for plant health threats. Integral to planning are education and policy. Needs are as follows:

- highly trained agricultural officials at ports of entry whose mission is a Cabinet-level priority;
- a new cadre of people educated in Agriculture Homeland Security that includes regulatory sciences, pathway and risk analysis, diagnostics, forensics;
- field workers, particularly growers, crop advisors, extension agents, who are knowledgeable about diseases that could be the result of use of biological agents, how to distinguish from the norm, and what to do when they encounter something suspicious.
- quantitative biological scientists, epidemiologists, aerobiologists, and so on, for plant-based agriculture
- alert and knowledgeable clinicians and laboratory diagnosticians, vital to disease surveillance efforts and recognition of new diseases and syndromes; and
- automated laboratory high throughput equipment and operating procedures.

## REFERENCES

1. Arnon, S. S., Schechter, R., Inglesby, T. V., Henderson, D. A., Bartlett, J. G., Ascher, M. S., Eitzen, E., Fine, A. D., Hauer, J., Layton, M., Lillibridge, S., Osterholm, M. T., O'Toole, T., Parker, G., Perl, T. M., Russel, P. K., Swerdlow, D. L., and Tonat, K. (2001). Botulinum toxin as a biological weapon: Medical and Public Health Management. *JAMA* **285**(8), 1059–1070.

2. Dudley, J. P., and Woodford, M. H. (2002). Bioweapons, biodiversity, and ecocide: potential effects of biological weapons on biological diversity. *Bioscience* **52**(7), 583–592.
3. Nutter, F. S., and Madden, L. V. (2005). Plant diseases as a possible consequence of biological attack. In M. S. Bronze, and R. A. Greenfield, Eds. *Biodefense: Principles and Pathogens*, Horizon Bioscience, Norwich, Chapter 23.
4. Madden, L. V., and Vandenbosch, F. (2002). A population-dynamics approach to assess the threat of plant pathogens as biological weapons against annual crops. *Bioscience* **52**(1), 65–74.
5. Madden, L. V., and Wheelis, M. (2003). The threat of plant pathogens as weapons against US crops. *Annu. Rev. Phytopathol*. **41**, 155–176.
6. Fitch, P. J., Raber, E., and Imbro, D. R. (2003). Technology challenges in responding to biological or chemical attacks in the civilian sector. *Science* **302**, 1350–1354.
7. Gottwald, T., Graham, J., and Schubert, T. (2002). Citrus canker: the pathogen and its impact. *Plant Health Prog*. doi:10.1094/PHP-2002-0812-01-RV.
8. ARS (2004). *Biology and Control of Emerald Ash Borer*, Retrieved on May 30, 2008 from http://www.ars.usda.gov/research/projects/projects.htm?accn_no=407426&showpars=true&fy=2004.
9. Gilbert, T. (1996). *Human Competence: Engineering Worthy Performance (Tribute edition)*, The International Society for Performance Improvement, Silver Spring, MD.
10. United States Department of Agriculture Animal and Plant Health Inspection Service (2007). *Pest Detection*. Retrieved March 30th, 2008 from http://www.aphis.usda.gov/plant_health/plant_pest_info/pest_detection/index.shtml.
11. United States General Accounting Office (2006). *Homeland Security: Management and Coordination Problems Increase the Vulnerability of US Agriculture to Foreign Pests and Disease (GAO-06-044)*, Retrieved March 30th, 2008 from http://www.gao.gov/new.items/d06644.pdf.
12. Grode, J. (2005). American Seed Trade Association, Washington, DC. Retrieved March 30th, 2008 from http://www.amseed.com/ppts/Homeland_Security.ppt#256,2,American%20Seed%20Trade%20Association%20Washington, %20D.C.
13. United States Department of Agriculture Animal and Plant Health Inspection Service (2002). *Questions and Answers About the Plant Protection Act*, Retrieved March 30th from http://www.aphis.usda.gov/lpa/pubs/fsheet_faq_notice/faq_phact.html.
14. Preslar, D. (2000). *The Role of Disease Surveillance in the Watch for Agro-terrorism or Economic Sabotage*, Retrieved March 30, 2008 from: http://www.fas.org/ahead/bwconcerns/agroterror.htm.
15. National Plant Board (2002). *Proceedings of 2002 National Plant Board 76th Annual Meeting*, Duluth, MN Retrieved March 30th, 2008 from http://www.nationalplantboard.org/docs/2002_NPB_Annual_Meeting_Proceedings_Final.pdf.
16. Durbin, R. (2007). *Senators Durban and Feinstein Introduce Bill to Transfer Responsibility for Agricultural Inspections from DHS back to USDA*, Retrieved March, 30th, 2008 from http://durbin.senate.gov/record.cfm?id=270685.
17. San Joaquin Farm Bureau Federation (2007). *Ag wants Border Inspection Returned to USDA*, Retrieved July 29th, 2007 from http://www.sjfb.org/thismonth/border.html.
18. United States Department of Agriculture Animal and Plant Health Inspection Service (2005). *The Cooperative Agricultural Pest Survey: Detecting Plant Pests and Weeds Nationwide*, Retrieved May 30, 2008 from http://www.aphis.usda.gov/publications/plant_health/content/printable_version/pub_phcapsdetecting.pdf.
19. Southern Region Integrated Pest Management Center (2008). *IPM PIPE: About*, Retrieved March 30th, 2008 from http://www.ipmpipe.org/about.cfm.
20. Stack, J., Cardwell, K. F., Hammerschmidt, R., Byrne, J., Loria, R., Snover-Clift, K., Baldwin, W., Wisler, G., Beck, H., Bostock, R., Thomas, C., and Luke, E. (2006). The National Plant Diagnostic Network. *Plant Dis*. **9**, 128–136.

21. Southern Plant Board (2006). *Resolution Number 8: Enhanced Funding of the Cooperative Agricultural Pest Survey Program Based on State-level Pest Introduction Risk Analysis*, Retrieved March 30, 2008 from http://www.nationalplantboard.org/docs/resolution_spb_2006_8_caps.pdf.
22. United States Department of Agriculture National Agricultural Statistics Service (2006). *Wisconsin Pesticide Use*, Retrieved March 30th, 2008 from http://www.nass.usda.gov/Statistics_by_State/Wisconsin/Publications/Miscellaneous/pest_use_06.pdf.
23. National Plant Diagnostic Network (2007). *National Plant Diagnostic Network: a record of accomplishment*, Retrieved May 30th, 2008 from https://www.npdn.org/library/viewdocument.pdf?filetype=pdf&documentId=6431.
24. United States Department of Agriculture National Agriculture Statistics Service (2004). *2002 Census of Agriculture*, Retrieved March 30th, 2008 from http://www.nass.usda.gov/census/census02/volume1/us/CenV1US1.txt.
25. National Association of Independent Crop Consultants (2008). *About the NAICC*, Retrieved March 30th, 2008 from http://www.naicc.org/about_naicc.cfm.
26. Isard S. A., Russo J. M., DeWolf E. D. (2006). The establishment of a national pest information platform for extension and education. *Plant Health Prog*. Retrieved May 30, 2008 from http://www.plantmanagementnetwork.org/php/elements/sum2.aspx?id=5508.
27. Balaam, R. J., United States Department of Agriculture Animal and Plant Health Inspection Service Offshore Pest Information System (2004). *Proceedings, XV USDA Interagency Research Forum on Gypsy Moth and Other Invasive Species*. Retrieved May 30, 2008 from http://www.fs.fed.us/ne/newtown_square/publications/technical_reports/pdfs/2005/332%20papers/balaam332.pdf.
28. Isard, S. A., Gage, S. H., Comtois, P., and Russo, J. M. (2005). Principles of the atmospheric pathway for invasive species applied to soybean rust. *Bioscience* **55**, 851–861.
29. National Academy of Sciences (2002). *Predicting Invasions of Nonindigenous Plants and Plant Pests*, National Academy Press, Washington, DC, p. 194 (See chapter 2).
30. Andow, D. A. (2003). Pathway-based risk assessment of exotic species invasion. In *Invasive Species, Vectors and Management Strategies*, G. M. Ruiz, and J. T. Carlton, Eds. Island Press, Washington, DC, pp. 439–455.
31. Kiritani, K., and Yamamura, K. (2003). Exotic insects and their pathways for invasion. In *Invasive Species, Vectors and Management Strategies*, G. M. Ruiz, and J. T. Carlton, Eds. Island Press, Washington, DC, pp. 44–67.
32. Mack, R. V. (2003). Global plant dispersal, naturalization, and invasion: pathways, modes and circumstances. In *Invasive Species, Vectors and Management Strategies*, G. M. Ruiz, and J. T. Carlton, Eds. Island Press, Washington, DC, pp. 3–30.
33. Auclairr, A. N., Fowler, G., Hennessey, M. K., Hogue, A. T., Keena, M., Lance, D. R., McDowell, R. M., Oryang, D. O., and Sawyer, A. J. (2005). Assessment of the risk of introduction of *Anoplophora glavripennis* (Coleoptera: Cerambycidae) in municipal solid waste from the quarantine area of New York City to landfills outside of the quarantine area: a pathway analysis of the risk of spread and establishment. *J. Econ. Entomol*. **98**(1), 47–60.
34. Work, T. T., McCullough, D. G., Cavey, J. F., and Komsa, R. (2005). Arrival rate of nonindigenous insect species into the United States through foreign trade. *Biol. Invasions* **7**, 323–332.
35. Liebhold, A. M., and Work, T. T. McCullough, D. G., and Cavey, J. F. (2006). Airline baggage as a pathway for alien insect species invading the United States. *Am. Entomol*. **52**(1), 48–54.
36. Worner, S. P., and Gevrey, M. (2006). Modelling global insect pest species assemblages to determine risk of invasion. *J. Appl. Ecol*. **43**(5), 858–867.

37. Nutter, F. W. Jr, Rubsam, R. R., Taulor, S. E., Harri, J. A., and Esker, P. D. (2002). Geospatially-referenced disease and weather data to improve site specific forecasts for Stewart's will disease of corn in the U.S. corn Belt. *Comput. Electron. Agric*. **37**, 7–14.

38. Hennessey, M. K. (2004). Quarantine pathway pest risk analysis at the APHIS Plant Epidemiology and Risk Analysis Laboratory. *Weed Technol*. **18**, 1484–1485.

39. Rotz, L. D., and Hughes, J. M. (2004). Advances in detecting and responding to threats from bioterrorism and emerging infectious disease. *Nat. Med. Suppl*. **10**(12), 130–136.

40. Coop, L. B. (2007). *U. S. Degree-day Mapping Calculator*, Version 3.0. Oregon State University Integrated Plant Protection Center, Web Site Publication E.07-05-1: http://pnwpest.org/cgi-bin/usmapmaker.pl.

41. Zadoks, J. C. (1999). Reflections on space, time and diversity. *Annu. Rev. Phytopathol*. **7**, 1–17.

42. Vanderplank, J. E. (1963). *Plant Disease: Epidemics and Control*, Academic press, San Diego.

43. Edelstein-Keshet, L. (1988). *Mathematical Models in Biology*, The Random House/Birkhauser mathematics Series, New York, NY.

44. Smith, J. M. (1971). *Mathematical Ideas in Biology*, Cambridge at the University Press, p. 152.

45. Babin, M., Cullen, J., Roesler, C. S., Donaghay, P. L., Douchette, G. J., Kahru, M., Lewis, M. R., Scholin, C. A., Sieracki, M. E., and Sosik, H. M. (2005). New approaches and technologies for observing harmful algal blooms. *Oceanography* **18**, 210–227.

46. Schmale, D. G. III, Shah, D. A., and Bergstrom, G. C. (2005). Spatial patterns of viable spore deposition of *Gibberella zeae* in wheat fields. *Phytopathology* **95**(5), 472–479.

47. Falacy, J. S., Grove, G. G., Mahaffee, W. F., Galloway, H., Glawe, D. A., Larsen, R. C., and Vandemark, G. J. (2007). Detection of *Erysiphe necator* in air samples using the polymerase chain reaction and species-specific primers. *Phytopathology* **97**(10), 1290–1297.

48. Krupa, S., Bowersox, V., Claybrooke, R., Barnes, C., Szabo, L., Harlin, K., and Kurle, J. (2006). Introduction of soybean rust urediniospores into the Midwestern United States-a case study. *Plant Dis*. **9**, 1254–1259.

49. Zhou, G., Whong, W.-Z., Ong, T., and Chen, B. (2000). Development of a fungus-specific PCR assay for detecting low-lever fungi in an indoor environment. *Mol. Cell. Probes* **14**, 339–348.

50. Lamb, D., and Bowersox, V. (2000). The national atmospheric deposition program: an overview (2000). *Atmos. Environ*. **3**(11), 1661–1663.

51. Barnes, C. W., Szabo, L. J., Isard, S. A., Ariatti, A., Tenuta, A. U., Hambleton, S., Tropiano, R., Bowersox, V. C., Claybrooke, R., and Lehmann, C., (2008). Patterns of Phakopsora pachyrhizi Spore Deposition Detected in North America Rain and Their Use to Calibrate IAMS Soybean Rust Forecasts in 2007 [abstract]. *Phytopathology*. **98**, 518.

52. National Oceanic and Atmospheric Administration, Atmospheric Research Laboratory (2005). *NOAA ARL HYSPLIT Model*, Retrieved May 30, 2008 from www.arl.noaa.gov/ready/hysplit4.html.

53. Byrne, K. M., Fruchey, I. R., Bailey, A. M., and Emanuel, P. A. (2003). Automated biological agent testing systems. *Expert Rev. Mol. Diagn*. **3**(6), 759–768.

54. Emanuel, P. A., Fruchey, I. R., Bailey, A. M., Dang, J. L., Niyogi, K., Roos, J. W., Cullin, D., and Emanuel, D. C. (2005). Automated screening for biological weapons in homeland defense. *Biosecur. Bioterror*. **3**(1), 39–50.

55. Osterbauer, N., Trippe A. (2005). *Comparing Diagnostic Protocols for Phytophthora ramorum in Rhododendron*, Plant Management Network, http://www.aphis.usda.gov/ppq/ispm/pramorum/pdf_files/pcrprotocol4.pdf.

56. USDA-APHIS. (2004). *PCR Detection and DNA Isolation Methods for Use in the Phytophthora ramorum National Program*, http://www.aphis.usda.gov/plant_health/plant_pest_info/pram/downloads/pdf_files/cultureprotocol6-07.pdf.

57. USDA-APHIS. (2004). *Guidelines for isolation by culture and morphological identification of Phytophthora ramorum*, online: http://www.aphis.usda.gov/ppq/ispm/pramorum/pdf_files/pcrprotocol4.pdf.

58. Layne, S. P., and Beugelsdijk, T. J. (2003). High-throughput laboratories for homeland and national security. *Biosecur. Bioterror*. **2**(1), 123–130.

# MITIGATING CONSEQUENCES OF PATHOGEN INOCULATION INTO PROCESSED FOOD

JAMES S. DICKSON

*Department of Animal Science, Iowa State University, Ames, Iowa*

## 1 INTRODUCTION

Pathogens occur in processed foods as a result of the natural occurrence of these organisms, and also as a result of failures in both processing and sanitation. The intentional introduction of pathogens into processed foods is an unlikely but plausible event, given an individual or individuals with sufficient motivation. The response to either an accidental or intentional event would be similar, although there would be more significance to an intentional event. However, the basic response would include the recovery of the affected products, a reevaluation of the process, and a public relations effort to restore public confidence in the specific food type or processor.

## 2 SCIENTIFIC OVERVIEW

### 2.1 Processed Foods

The processing of foods ranges from very minimal to technologically advanced. An example of minimal processing would be fresh vegetables, such as green beans. In this case, the food is simply washed to remove physical contaminants, and may be prepackaged for retail sale. Alternatively, some foods, such as canned vegetables, may be processed and preserved to a degree that they are shelf stable and ready-to-eat. Because

of the diversity of food types and processing, the potential for an intentional introduction of pathogens is great.

***2.1.1 Historical Precedence.*** Upon leaving the post of Secretary of the US Department of Health and Human Services, Secretary Thompson commented "I, for the life of me, cannot understand why the terrorists have not, you know, attacked our food supply because it is so easy to do, and we are importing a lot of food from the Middle East, and it would be easy to tamper with that." [1]. There have been historical examples of deliberate contamination of food products in the United States. Perhaps the largest incident was in State of Oregon in 1984 [2], where *Salmonella* was deliberately introduced into salad bars at local restaurants. In this case, the incident was intended to affect the outcome of a local election. In another incident, a disgruntled employee deliberately contaminated muffins and doughnuts with *Shigella dysenteriae* and left them in an employee break room [3]. Potassium cyanide has been used to contaminate over-the-countermedications on several occasions, leading to the deaths of several unsuspecting consumers [4]. One of the earlier documented cases of this type of product tampering or contamination was an incident which occurred in Chicago in 1982, where seven people died after ingesting deliberately contaminated products [5]. Although some of these contamination events were attempts to gain financially from the event (extortion), the motivation for the Chicago event is still unknown.

***2.1.2 Potential Biological Agents.*** Biological agents that could be used as potential contaminants include bacteria, viruses, and parasites. In addition, microbial toxins could also be introduced into processed foods [6]. The information needed to select, isolate, identify, and cultivate these organisms is readily available within the public domain. Bacterial agents are more likely to be used as deliberate contamination agents, simply because a person with rudimentary microbiological skills and facilities, along with equipment and supplies purchased from readily available sources, can produce sufficient quantities of bacteria to be used to deliberately contaminate foods. The techniques and requirements to produce sufficient quantities of viruses and parasites would require more sophisticated skills and facilities.

Bacterial agents may be divided into two general categories: those which cause infections and those which cause intoxications. Infectious agents require the presence of a live organism. Since most of these bacterial agents are sensitive to heat, they would be most effective with foods that do not undergo thermal processing or a final cooking step. The historical example of *Salmonellae* introduced into salad bars [2] illustrates this point. Bacterial toxins can also be produced, albeit in crude form, with rudimentary skills and facilities. Some bacterial toxins are heat stable, which would allow them to be used in foods that do undergo thermal processing. In 1989, mushrooms were held under conditions, which allowed for the growth and toxin production by *Staphylococcus aureus*. These mushrooms were subsequently canned, destroying the live bacteria, but allowing the toxin to remain present and cause illness [7]. The mushrooms were grown and canned in another country and then imported into the United States, where the illnesses occurred.

***2.1.3 Food Processing Systems—Threat Assessment.*** Food processing may be separated into several distinct phases: production, processing, secondary processing, distribution, sale, and consumption. In addition, transportation is a critical factor at all stages, as food is often produced in one location and then distributed nationally or internationally.

Most production sites have minimal security, and are often located in rural settings, where there is a relatively low population density. This leaves the production sites vulnerable to intentional contamination, as most of these locations are easily accessed by a determined individual or group of individuals. Intentional contamination could be carried out at most of these locations with a minimal risk of detection.

Processing and secondary processing facilities also offer opportunities for intentional contamination to a determined individual or group of individuals. Although most food processing establishments review potential employees prior to hiring, it is quite possible for an individual or individuals with criminal intent to become employed at a food processing facility. There have been several video recordings demonstrating insanitary or inhumane conditions made in secret inside meat processing facilities in the last few years, and it has been suggested that some of these videos may have been made by individuals who sought employment at the facility, specifically to record the video. If an individual can obtain employment with the intent of secretly recording a video, then an individual motivated to deliberately contaminate food could also presumably obtain employment.

Virtually, all types of food processing systems incorporate steps during processing to assure the safety of the food product. Although these are designed to address naturally occurring contamination, they are also well suited to address intentional contamination. The more comprehensive food safety systems are based on either the Hazard Analysis Critical Control Point system (HACCP) [8] or the International Organization for Standardization [9]. The disadvantage of these programs is that they are well documented within the processing establishment, and are therefore readily available. A determined individual would be able to evaluate such systems, and devise a way of introducing contamination in a manner that would not allow rapid detection.

The food distribution network raises additional concerns. The opportunities for intentional contamination increase, as the food may pass through a series of transportation and storage stages and is potentially available for a variety of individuals to have access to. As with processing, these individuals could conceivably be either employees of the transportation and storage companies or simply determined individuals who gain unauthorized access to the food. A further concern with the distribution network is that most if not all of the microbiological testing of foods is done at the processing level, meaning that foods contaminated during distribution would be unlikely to be tested before they reach the consumer.

Foods may be exposed to potential intentional contamination at the point of preparation (food service) or retail sale. At retail, the food is accessible not only by employees of the retail establishment but also by other consumers. It would be very difficult to identify and stop a determined individual from entering a retail establishment and deliberately contaminating food, especially produce that is presented for sale without primary packaging. Previous product tampering cases have involved contamination at the point of sale, and have proved to be difficult to stop.

Foods that undergo less processing fall into a higher risk category. Several foods of this type of minimally processed food have been involved in naturally occurring foodborne illnesses in recent years, including lettuce [10] and spinach [11]. Since these types of foods rarely receive additional processing by the consumer before consumption, any pathogen introduced has the potential to cause human illness.

***2.1.4 Avoidance Strategies.*** The primary assumption for evaluating a deliberate contamination event is that it would be carried out by an individual or individuals with criminal intent. Because of this, most of the avoidance strategies are based on controlling access of unauthorized individuals to food production and processing areas. Physical security of the food production or processing locations is the first step in avoiding a deliberate contamination event. As previously mentioned, food production sites are difficult to secure, although there are some notable exceptions. Some concentrated animal feeding operations for dairy cattle, poultry, and swine have elaborate physical security measures in place, primarily to prevent the unintentional introduction of animal diseases. These biosecurity measures secure the facility and rigidly control personnel access to the animals. By their nature, locations producing grain crops, leafy green vegetables, or other produce are virtually impossible to secure against unintentional access because of the size of the land mass associated with the growth of these crops.

Most food processing and secondary food processing establishments have some degree of physical security. Most are surrounded by perimeter fences and have sufficient exterior lighting to provide for visual examination of the premises. Many employ security guards to regulate access to nonpublic areas of the processing establishment. However, there are practical limitations to all of these measures. There are many people who are not employees of a company, but who have legitimate business within a food processing establishment. These would include, but not be limited to, delivery persons, maintenance and construction personnel, contract pest control and sanitation personnel, customers, and suppliers. Given the intent, any of the individuals could potentially have access to food products.

Persons employed by the food production or processing industry have been previously mentioned as potential threats for deliberate contamination. Preemployment screening is vital for many reasons, but even more so to avoid potential contamination. Employees should verify previous employment, and addresses, to assure that the applicant does have a documented history of employment. In addition, preemployment drug screening is widely used to verify that the individual is not currently using illegal drugs. Employees should be adequately trained in the general aspects of food safety, and the impact of a foodborne disease outbreak should be made clear as part of the training. Large foodborne disease outbreaks from natural sources have forced companies to go out of business, resulting in all of the employees becoming unemployed. Emphasizing this point to all employees makes employees more aware, and may result in the reporting of an odd or unusual event witnessed by one of the employees. This empowers employees to become part of the internal monitoring system, and may alert management to an event before the food leaves the processing facility.

## 3 RESPONSE TO AN INCIDENT

The response to an intentional food contamination event would most likely follow a similar pattern as the response to a naturally occurring contamination event. Regrettably, unless a specific threat has been communicated from the individuals responsible or another method has given some warning, the first indication of a deliberate contamination event would be through public health departments. Standard epidemiological investigations and syndromic surveillance should indicate a common source for the disease outbreak [12]. Once a common source is identified, the response by the food industry should be immediate.

The initial response would be to immediately remove all of the food processed in the establishment from commerce, essentially following the practices of a recall. Some of

the more specific guidelines for food recalls have been published by the Canadian Food Inspection Agency [13]. The food would then be categorized into specific production lots or code dates to determine which code dates were contaminated. The public health investigation should be helpful in identifying whether there were multiple code dates involved, either by recovering intact packages from the homes of the consumer or by investigating the geographical distribution of the disease in relation to the distribution of the food product. This presumes that the food product in question had sufficient lot coding in place to segregate the product. Lot coding becomes more problematic with bulk or commodity items. Extensive microbiological testing would be required to assure that product code dates that are not directly associated with human illnesses were in fact free of the intentional contamination.

The deliberately contaminated product must be disposed of in such a way as to assure that it will not pose any additional health or environmental effects. Unlike naturally contaminated product, intentionally contaminated product will likely contain high populations of the pathogen, or high levels of the toxin. Depending on the nature of the contaminant, the food may not be able to be disposed of through the usual methods of rendering, thermal processing, or burying in a land fill. Additional methods may need to be employed to assure that the food poses no further hazard to human health. Commercial irradiation, commonly used to sterilize pharmaceutical products and medical devices, may need to be employed to eliminate the contaminant from the food before final disposal. In the case of biological toxins, chemical methods such as those used to destroy animal carcasses infected with bovine spongiform encephalopathy, may have to be employed to ensure the destruction of the toxin. The safety of the workers handling and disposing of the infected products must be considered in the overall plan for disposal.

Once the immediate public health crises has subsided, the food industry as a whole should evaluate what happened so that similar incidences may be prevented in the future. Previous historical events have shown that "copycat" events may follow an initial event, and the industry should evaluate the processing systems to prevent a similar incidence from occurring. Naturally occurring contamination events have often identified shortcomings in the current processing systems, especially in lot tracing and logistical control of the food product. An intentional contamination event would identify any weaknesses within a given processing system, and an evaluation of the overall event would help to make the industry better prepared for future events.

## 4 RESEARCH AND FUNDING DATA

The type of research needed to address the concerns of deliberate food contamination is similar in many respects to that needed to address naturally occurring contamination. Consequently, the common sources of funding for food safety research are also likely to fund research on intentional contamination, simply because the outcome of the research will be applicable to many situations. The primary government source of research funding for food safety endeavors is the US Department of Agriculture (USDA) Cooperative State Research, Education and Extension Service (CSREES). Major funding programs include the National Research Initiative and the Integrated Research, Education, and Extension Competitive Grants Program. For the updated current request for proposals for these programs, see http://www.csrees.usda.gov/foodsafetybiosecurity.cfm. In addition to the government funding, many of the trade associations offer competitive grants programs in the area of food safety. Although these awards from these grant programs tend to be smaller than those from the federal programs, they are still a useful source of funding for this type of research.

## 5 CRITICAL NEEDS ANALYSIS

The potential for a deliberate act of contamination to occur is well documented. Historically such events have taken place, although usually perpetrated by an individual intent of financial gain or by a disgruntled employee [14]. The potential disruption that could be caused by an organized group, for example for contaminating multiple foods in various locations with different agents, is great. Protecting the food supply from a deliberate contamination event is one of the priorities of the US Department of Homeland, as well as the other agencies that are responsible for the safety of the food supply (USDA Food Safety and Inspection Service (FSIS), Food and Drug Administration (FDA), Environmental Protection Agency (EPA), etc.). The food industry is global in its operations, with food being one of the main commodities traded internationally. A deliberate act of contamination in a specific food could have far reaching impacts not only on human health but also on international trade. A recent incident involving naturally occurring *Salmonellae* contamination of cantaloupe illustrates this point [15]. One of the key components in research is that the outcome of virtually all of the programs will have applications not only for deliberate events but also for contamination that occurs as part of the overall food process.

## 6 RESEARCH DIRECTIONS

Future research needed to address the needs of both regulatory and public health officials in the event of a deliberate event falls into several categories, but can be broadly classified as scientific or technical, logistical, and societal. These are the same research needs for naturally occurring contamination events, so previous, current, and future research programs serve both purposes.

The scientific or technical issues relate to sampling and detection methods. Improvements need to be made in sampling techniques, as well as the statistical sampling plans needed to determine the extent of contamination. One of the weaknesses of the current detection methods is the lack of an adequate understanding of sampling, with the end result being no better than the quality of the sample collected. Additional resources also need to be applied to detection methodologies. Although significant advances have been made in the area of detection, most notably with the commercialization of polymerase chain reaction (PCR) technology, many of the methods still require an overnight incubation of the sample to increase the number of target cells. In the event of a deliberate contamination event, timing will be essential, and an ideal method would be one that could be performed on-site without a prolonged incubation. Methods that meet these criteria are under development, but have not been entirely successful.

The logistical issues that should be addressed include the ability to locate and recover all of the affected food. Recent events, especially with produce and meat [16], have shown how difficult it is to locate and retrieve all food involved. Further research is needed to improve the ability of food processors and federal agencies to track and identify food products to assist in the ability to identify and recall intentionally contaminated food.

Once contaminated food has been recovered, there is an issue of disposal. Depending on the nature of the contaminant, the food may require special processing to render it safe for disposal. In addition, the safety of the workers handling the contaminated food must be considered. As an example, food contaminated with a high population of pathogenic bacteria may require methods of disposal beyond rendering or burying in a land fill.

Although it is relatively simple to dispose of small amounts of contaminated food, scale of a potential disposal operation must be considered. The recent actions by USDA in recalling more than 140 million pounds of product [16] illustrate this point. There is a need to study the logistical and technical issues involved in rendering large quantities of food products safe for subsequent disposal.

A final research topic would be the effects of an intentional contamination event on society and consumers. An intentional event would raise questions not only about the specific food or foods affected but also about the food supply in general. It would be reasonable and prudent to determine what methods could be used to restore consumer confidence in the general food supply, as well as with a specific commodity. Consumer research could be conducted to determine the most effective means of communicating with consumers after an intentional contamination event, and what messages would be most effective in conveying that the emergency has passed. Presumably, this type of research has been conducted for other natural and intentional catastrophes, and this information could be applied to a food contamination event.

## REFERENCES


1. Branigan, W., Allen, M., and Mintz, J. (2004). *Tommy Thompson Resigns From HHS*. Washington Post.com Dec 3 2004. www.washingtonpost.com/wp-dyn/articles/A31377-2004Dec3.html (accessed 12 September 2006).
2. Torok, T. J., Tauxe, R. V., and Wise, R. P. (1997). A large community outbreak of salmonellosis caused by intentional contamination of restaurant salad bars. *JAMA*. **278**, 389–395.
3. Kolavic, S. A., Kimura, A., Simons, S. L., Slutsker, L., Barth, S., and Haley, C. E. (1997). An outbreak of *Shigella dysenteriae* type 2 among laboratory workers due to intentional food contamination. *JAMA*. **278**(5), 396–398.
4. *Morb. Mortal. Wkly. Rep*. (1991). Epidemiologic notes and reports: Cyanide poisonings associated with over-the-counter medication—Washington State, 1991. **40**(10), 161, 167–168
5. Wolnik, K. A., Fricke, F. L., Bonnin, E., Gaston, C. M., and Satzger, R. D. (1984). The Tylenol tampering incident—tracing the source. *Anal. Chem*. **56**, 466A–468A, 470A, 474A.
6. Lee, R. V., Harbison, R. D., and Draughon, F. A. (2003). Food as a weapon. *Food Prot. Trends*. **23**(8), 664–674.
7. Levine, W. C., Bennett, R. W., Choi, Y., Henning, K. J., Rager, J. R., Hendricks, K. A., Hopkins, D. P., Gunn, R. A., and Griffin, P. M. (1996). Staphylococcal food poisoning caused by imported canned mushrooms. *J. Infect. Dis*. **173**(5), 1263–1267.
8. NACMCF (1998). Hazard analysis and critical control point principles and application guidelines. *J. Food Prot*. **61**, 1246–1259.
9. ISO (2005). *ISO 22000:2005, Food Safety Management Systems - Requirements for Any Organization in the Food Chain*. International Organization for Standardization .www.iso.org/iso/home.htm
10. *Morb. Mortal. Wkly. Rep*. (2007). Preliminary foodnet data on the incidence of infection with pathogens transmitted commonly through food—10 States, 2006. **56**(14), 336–339.
11. *Morb. Mortal. Wkly. Rep*. (2006). Ongoing multistate outbreak of *Escherichia coli* serotype O157:H7 infections associated with consumption of fresh spinach—United States, September 2006. **55**(38), 1045–1046.
12. Buehler, J. W., Berkelman, R. L., Hartley, D. M., and Peters, C. J. (2003). Syndromic surveillance and bioterrorism-related epidemics. *Emerging Infect. Dis*. **9**, 1197–1204.

13. CFIA (2007). *Food Recalls: Make a Plan and Action It! Manufacturers' Guide. Updated April 19, 2007*. www.inspection.gc.ca/english/fssa/recarapp/rap/mgguide.shtml (accessed 9 January 2008).
14. Tucker, J. B. (1999). Historical trends related to bioterrorism: an empirical analysis. *Emerging Infect. Dis*. **5**, 498–504.
15. Department of Animal Science (2008). *Voluntary Nationwide Recall of Honduran Cantaloupes grown by Agropecuaria Montelibano, San Lorenzo Valle, Honduras, 24 March 2008*. http://www.fda.gov/oc/po/firmrecalls/centralamerican03_08.html (accessed 7 May 2008)
16. USDA-FSIS (2008). *California Firm Recalls Beef Products Derived From Non-Ambulatory Cattle Without the Benefit of Proper Inspection*. http://www.fsis.usda.gov/PDF/Recall_005-2008_Release.pdf (accessed 10 May 2008).

## FURTHER READING

(a) AIB (2005). *The AIB Guide to Food Security*. AIB, Manhattan, KS; (b) National Food Processors Association (2005). *Food Security Manual*. GMA-NFPA, Washington DC.

US Department of Agriculture—Food Safety and Inspection Service. (2008). *Food Defense and Emergency Response*. http://www.fsis.usda.gov/Food_Defense_&_Emergency_Response/index.asp

US Food and Drug Administration. *Food Defense and Terrorism*. (2008). http://www.cfsan.fda.gov/~dms/defterr.html

# MICROBIAL FORENSICS AND PLANT PATHOGENS: ATTRIBUTION OF AGRICULTURAL CRIME

JACQUELINE FLETCHER AND ULRICH MELCHER
*Oklahoma State University, Stillwater, Oklahoma*

DOUGLAS G. LUSTER
*USDA ARS, Fort Detrick, Maryland*

JOHN L. SHERWOOD
*University of Georgia, Athens, Georgia*

## 1 INTRODUCTION

The US food system is among the safest and most secure, worldwide. Yet, because plant-based systems are essential components of the nation's farm-to-table food supply

system, they may be potential targets for the deliberate introduction of pathogens or pests by those intending harm [1–6]. In addition, plants comprise our fiber, forests, and rangelands—and may play an increasingly important strategic role as a source of biofuels. Possible impacts of intentional tampering include loss of product quality or availability, economic hardship for farm and market sectors and rural communities, and distrust of US produce and value-added products. National biosecurity capabilities must include scientific knowledge, technologies, and procedures to effectively trace the origin, timing, and site of introduction of a plant pathogen or pest, and the collection of evidence that ultimately will allow successful criminal prosecution of those responsible [7–10]. The general application of science to legal practices is termed *forensic science*, and if the activity focuses on pathogenic agents, it is called *forensic microbiology*. We will discuss the application of microbial forensic principles and activities to plant-based agricultural systems, and introduce the emerging subdiscipline of forensic plant pathology.

## 2 SCIENTIFIC OVERVIEW

### 2.1 Agriculture as a Target

The vulnerability of agricultural production systems to natural or intentional threats has long been recognized ([1]; *see also Stack, this volume*). Plant-based agriculture in the United States includes 382 million acres in crop production, 737 million acres in forests, and 525 million rangeland acres for grazing [11]. Complete security for such a vast area is not feasible. Biowarfare programs against plants and livestock were sponsored by governments of several countries during a period encompassing and following World Wars I and II, and deployment of animal pathogens including the agents of glanders and tularemia has been documented [12]. The purposeful introduction of plant pathogens to negatively affect crop production has not been confirmed, but some government-sponsored programs included plant pathogens in their bioweapons development programs [12]. Although most such programs were terminated after the 1972 Biological Weapons Convention, signed by 142 countries, the potential for application of agricultural pathogens for harmful purposes remains. The US security community has called for focused consideration of our capabilities to attribute a purposeful event that could threaten US agriculture, including our critical plant-based resources.

### 2.2 Impacts on Various Sectors

Millions of dollars are lost as a result of plant diseases each year, including loss of the commodity itself as well as downstream impacts and the costs of preventative measures. Loss estimates for new or emerging diseases can vary widely. For example, possible losses due to soybean rust, calculated before its arrival into the United States, were estimated at $240 million–$2 billion [13]. Fortunately, actual losses to date from the establishment of this pathogen have been at the low end of this range.

Introduction of foreign crop pathogens inevitably impacts domestic commodity markets and futures. In some cases such impacts may turn out to be positive for producers, as anticipated supply shortages can result in higher prices. However, impacts on export markets are often negative, possibly including temporary halts in exports of produce or commodities or imposition of costly phytosanitary inspections. Negative impacts may also reach the consumer, with adverse public reaction to diseased commodities and concomitant drops in food product sales. Such events tend to promote tighter information management policies during future episodes.

### 2.3 Resolution and Recovery

Recovery from a new introduction of a foreign crop pathogen is generally time consuming and costly. Site recovery may include quarantine regulations to limit spread of the new pathogen to nearby regions and states, implemented by state authorities or by the United States Department of Agriculture (USDA), although many pathogens have proved impossible to contain once introduced. Actual decontamination of agricultural biocrime sites is feasible only in a limited number of scenarios, such as storage or transportation facilities. Actual field sites may remain infested or contaminated for long periods of time, depending upon the climate and biological cycle of the microbe.

The USDA has invested much effort into the development of National Plant Disease Recovery System (NPDRS) plans for high-threat pathogens (http://www.ars.usda.gov/research/docs.htm?docid=14271). Each plan includes methods, practices, and recommendations for short- and long-term management of a specific disease. Many of the NPDRS plans identify critical gaps in knowledge that must be filled before recovery would be likely to be successful, recognizing that true recovery often requires years of research toward the development of customized disease management and control practices, with the eventual deployment of genetic host resistance, where feasible.

### 2.4 Detection of a Deliberate Event

The first question facing law enforcement personnel investigating a potentially suspicious plant disease outbreak is whether a crime actually has occurred. Responsibility lies with the USDA Animal and Plant Health Inspection Service (APHIS) and the Federal Bureau of Investigation (FBI) to decide quickly whether to sequester the site and surrounding evidence as a crime scene. If an outbreak has been threatened or announced, the question becomes whether the situation is real or a hoax. Hoaxes may have impacts as serious as those of a verified disease. While obvious physical evidence, such as microbiological or laboratory materials, may be present at an agricultural scene, early clues to discriminate between an intentional plant disease introduction and one that is natural or accidental often come from spatial or epidemiological patterns or signatures. Because the recognition of anomalous patterns requires baseline data on temporal and spatial patterns of disease incidence for all diseases, research on rapid recognition of deliberate events will require a prioritization of pathogens for targeted study and a focused, large-scale research effort to map worldwide disease outbreaks and determine "normal" baseline patterns for high-priority diseases [14, 15].

### 2.5 Responses to First Detection

Immediate challenges would ensue as a result of declaring an agricultural field or storage site as a crime scene. The extent or scope of the delineation must be estimated rapidly, and sampling strategies developed to cover the affected areas. Genetic background information on relevant pathogens must be gathered or accessed, and a careful plan developed for preservation of evidence. Microbial sampling may be driven to larger scale by factors of pathogen epidemiology and population dynamics, but limited by practical forensic sample preservation capacities. Critical factors and limitations in sampling schemes devised for agricultural settings include the advantages of maintaining live samples, the requirement for stringent chain of custody, and the limitations of sampling time frames. Research to improve statistical pathogen sampling with applications in natural,

accidental, and deliberate outbreak scenarios has been conducted and disease parameters modeled based upon modes of dissemination (soil-borne, wind, rain, insect vectors, etc.) [16, 17], environmental factors, cropping practices (spacing, canopy parameters), and genetic susceptibility of the host. However, more research is needed, with an emphasis on high-threat plant pathogens and on specific applications for forensic investigation.

The USDA-APHIS, the FBI, and the Department of Homeland Security (DHS) will share responsibility for providing and implementing incident command at an agricultural crime scene, although it is not clear whether an incident command structure has been fully optimized and coordinated among the three federal agencies. Clearly, all agencies would benefit from field simulation exercises focusing on deliberate introductions. Crop disease outbreak simulation exercises have been, and continue to be planned and overseen by the National Plant Diagnostic Network (NPDN) Exercises Committee ([18]; personal communication, Carla Thomas, Western Plant Diagnostic Network). Crop disease scenarios have been carried out with or by the NPDN in 49 states, involving county, state, and federal agricultural and law enforcement officials, including tabletop and field exercises, simulating a deliberate event, it is time to focus on issues and problems related to conducting a criminal investigation in an agricultural setting. Major issues for such an exercise include information management, media briefings and access, and decisions on levels of access and knowledge. Decisions on "right to know" are relevant to local, state, and national interests, such as county and state agricultural extension specialists and commercial crop consultants (who may be the first detectors), State Plant Health Responsible Officials (SPRO), State Plant Health Directors (SPHD), and diagnosticians at NPDN laboratories, who may see similar or associated diseased plant samples for diagnosis during the crisis. The site may be subjected to quarantine or regulation by APHIS plant protection and quarantine (PPQ) and/or state officials, introducing a second level of issues related to site accessibility and information management.

### 2.6 The Emerging Discipline of Forensic Plant Pathology

How does forensic plant pathology differ from what plant pathologists do every day? The science of plant pathology is the study of plant diseases and their causal agents, which include fungi, oomycetes, bacteria, viruses and viroids, nematodes, and a few protozoa and parasitic plants. Most plant pathology research is directed at understanding the relationships between pathogens and their plant hosts and, if involved, their insect vectors, with the goal of identifying potential disease management strategies as well as points in the disease cycle at which such strategies are likely to be most effective. Among the most important components of any plant disease management program is early diagnosis, because of its potential to limit the spread and impact of a disease. However, due to the vast and widely distributed nature of US agricultural production, plant diseases may not be noticed for days or weeks. Early diagnosis often is unlikely and when a disease is finally noticed, it may be difficult to identify the site and the means of initial pathogen introduction. Fortunately, the plant disease diagnostician focuses primarily on pathogen identification, and a selection of the best control strategy does not usually require complete knowledge of the disease event or fine discrimination among plant pathogen strains.

In contrast, a forensic scientist investigating a potential crime involving a plant pathogen in a natural or field setting will need to understand as much as possible about the crop or landscape history and management, pathogen introduction and establishment, disease development and spread, and pathogen identification [19]. Although much

knowledge, technology and expertise in plant pathogens already exist and can be accessed in a forensic investigation, special features characterize their application in a forensics setting. As a criminal case is likely to be tried in a court of law, where testimony is subject to vigorous cross-examination, all evidence and information must be collected using highly standardized and validated procedures. The standardization of procedures presents a daunting challenge due to the variety of environments and infrastructures at agricultural sites, and the absolute requirement to preserve microbiological characteristics and molecules required for downstream sample analysis. Development of strict standard operating procedures (SOPs) for such settings could actually hinder sample collection, preservation, and analysis [20]. It may be more appropriate to develop a set of generalized "best practices" for certain agricultural settings (e.g. for fields, postharvest storage facilities, transportation vehicles and containers, etc.), which could be applied and refined on site with experts on scene. More defined SOPs could be developed for extraction and analytical phases, depending upon the type of molecule to be analyzed, from specific procedures that have been published in the plant pathology diagnostics literature.

## 3 ELEMENTS OF A STRONG MICROBIAL FORENSICS CAPABILITY

### 3.1 Sampling and Evidence Handling

Although many features of sampling for investigation of microbial incidents will be similar among incidents involving humans, livestock, or plants, details will differ [19]. After initial infection and before symptoms are evident, sick people and animals are likely to move (or be moved) and interact with one another, and once symptomatic, encounter health professionals. Plant production systems are immobile (although factors that impact them, such as insects and other animals, humans, wind, and water are not) and involve huge acreages and very large numbers of individual plants. Significant time may pass during pathogen establishment and spread before a plant health care professional is involved. Crime investigators, who may have little training in, or understanding of, agricultural systems, must be prepared to sample large land areas and know what constitutes a useful sample and how such samples should be collected, packaged, transported, and stored. Sampling techniques must be reliable, standardized, and validated, and their limits known. Stringent chain-of-custody records are necessary to document sample handling and movement from the field to the laboratory to the courtroom. The precise identity of the pathogen and its relationship to all known microbial relatives becomes critically important. Careful preservation of the evidence, including molecular signatures, and its suitability for downstream reexamination are all required. Yet, very little research has been done to establish optimal sampling strategies in agricultural settings. For example, current diseased plant sampling techniques may involve collection of various plant organs (leaves, stems, roots, fruits, etc.) and organs of various ages (young to old). Samples might be placed into bags of plastic or paper, and might be stored on ice or maintained at ambient temperature. Depending upon circumstances and the experience of the collector, relevant samples may be taken from field soil and from nearby water sources (streams, farm ponds, or irrigation sources). If an insect vector may be involved in the disease, the field may be swept with insect collection nets, or yellow sticky traps or vacuum traps may be deployed; depending upon the insect and its behavior. Needed are specific data on optimal field sampling patterns, sampling tools, such as swabs, knives, bags or containers, storage temperatures and humidity, and other parameters of sampling.

### 3.2 The Role of Plant Disease Epidemiology

The processes and time course of progression and spread of diseases are diverse and complex [14, 16]. Pathogen generational cycling, dispersal, transport, deposition on the host, and disease initiation and progression are unique to each pathogen–host pathosystem. Fungal, oomycete, virus, bacterial, and nematode pathogens occupy unique niches within the agroecosystem, so disease initiation and spread may be influenced by completely unique combinations of macro- and microclimatic factors (air, soil and/or leaf moisture, temperature, solar radiation), arthropod vectors, and/or cropping and cultural practices. The genetic structure and ecology of pathogen populations in their crop hosts and weedy relatives play an important role in the epidemiology of each associated disease.

Modern plant pathogen epidemiology focuses on the development of models that describe and predict diseases on the basis of measurements of the above mentioned factors. To identify anomalous patterns in the introduction and spread of plant pathogens, baseline data on pertinent epidemiological factors and fully developed disease models will be necessary for each high-priority pathosystem in each major climatic region of the United States. Additionally, the development of statistically sound sampling strategies for forensic analysis will require detailed knowledge of epidemiological factors, particularly disease dispersal, and subsequent predictive models to identify the potential scale of an agricultural crime scene [14–16]. Application of baseline epidemiological data to a suspicious event could, for example, recognize that multiple widespread simultaneous disease foci for a pathogen normally spread naturally by wind represent an anomalous pattern, indicative of suspicious origins.

### 3.3 Current Microbial Forensic Identification and Typing Methods Applied to Plant Pathogens

Although evaluations of the event site and disease epidemiology are critical, identifying the pathogen and discriminating among very similar strains are generally among the most important components of a forensic investigation. Analysis beyond visual or microscopic inspection will likely result in the destruction of at least a part of the sample for analysis of its component macromolecules, primarily nucleic acids or proteins. If the sample is very small, choice of analysis for one macromolecule may preclude the ability to analyze the sample for another macromolecule. For example, RNA, the infectious molecule of many plant viruses, is more labile in plant samples than DNA and requires conversion to DNA before PCR can be utilized. Test validation is necessary to assure repeatability, efficacy, and reliability. Validation criteria and procedures for plant pathogens are in a state of development, presently led by USDA-APHIS with multiple agencies developing the National Plant Protection Laboratory Accreditation Program (NPPLAP), which is developing standards and criteria for accreditation and validation to be applied at the NPDN diagnostic laboratories. Criteria and procedures will largely follow those developed in methods validation for animal disease diagnostics [21–23]. To date, such standards for plant pathogen diagnostics have generally been determined individually by the developer of the test or reagent, and “affirmed” by the procedure being published in a peer reviewed journal. Only recently have steps been taken to certify labs or individuals for specific tools and procedures.

### 3.4 Genome Dynamics, Phylogeny, and Systematics

Ideally, an SOP for identifying and typing plant pathogens would be applicable to any microbe. Unfortunately, because microbes vary greatly in gene content, in the mechanisms by which genes change sequence, and in rates of sequence change, it is impossible to choose a single small set of genes shared among all microbes as targets for forensic analysis. Insertion and deletion of large or small DNA fragments and nucleotide substitutions occur at different rates in different organisms and under different conditions. In addition, a variety of DNA rearrangements leading to duplication of genes, deletion of genes or gene segments, inversion of chromosome sections, and translocation or transposition of large pieces of DNA can occur within a cell or its descendants. These changes are mediated by homologous recombination, site-specific recombination, and illegitimate recombination. Overlaid on the genomic changes that can occur in any cell and its progeny are events in which additional DNA is added. Such events include fertilization, heterokaryon formation, (with subsequence homologous recombination), conjugation, natural transformation, and phage or virus infection. Similarly, for diploid cells or nuclei, meiotic processes halve the complexity of DNA such that gamete chromosomes are chimeras of parental chromosomes. Thus, while substitutions may be better indicators in some organisms, in others, examination of the sizes of genomic regions may yield more reliable information.

Microbial forensics research and technology have focused on identifying suspect pathogens to strain level, to establish with reasonable certainty that the pathogen that caused an outbreak came from pathogens in the hands of the suspect. Often this is done by examining one or a limited number of genetic loci. However, the recent demonstration that the entire genome of an organism can be replaced with that of another [24] removes one barrier to creating designer pathogens by fusing genome parts of several different organisms, possibly with some totally synthetic DNA. As a result, the forensic microbiology investigator must be able to survey the causative agent's entire genome to identify the sources of each of its parts. Considering the diversity of microbes, SOPs must be devised for multiple narrow groupings of microbes and/or pathogenicity components, and they must address multiple genomic regions.

If cost is no object, complete genome sequencing will be most useful in pinning down the construction of a genetically engineered pathogen. Complete genome sequencing of several *Bacillus anthracis* strains was part of the anthrax investigation. Recent developments in nucleotide sequencing [25], such as emulsion PCR and the application of pyrosequencing to glass fiber bundles, have already lowered the cost and are making the sequencing of multiple isolates of bacterial species routine and facilitating complete genome analysis of multiple fungal species. Additional high throughput methods including the use of cleavable terminators and ligation-mediated sequencing are under commercial development.

Currently preferred methods of testing matches between DNA from a crime scene and that in a suspect's hands are based upon nucleotide sequences. Whether they can demonstrate absolute identity between two samples depends on the rate at which that DNA changes. As the rates of change are typically high for viruses, due to the error-prone nature of replicative enzymes and the rapid replication of many viral genomes, achieving absolute virus identity is not practical. For bacteria, as demonstrated by research in the anthrax incident [26], the rate of strain divergence is much lower. However, detailed investigations of genomic changes over time are available only for a handful of organisms, and it is likely that many bacterial species undergo mutation at rates higher than those

seen for anthrax. Changes in genomes during laboratory propagation also have been reported [27]. Better understanding of the rates of change and the mechanisms that generate them (substitutions, insertions, and deletions) is needed to judge which changes might be expected in short time frames and which are highly unlikely [28].

Multiple locus approaches to microbial typing include complete genome sequencing, multiple locus sequence typing (MLST), multiple locus variable number of tandem repeats analysis (MLVA), random amplification of polymorphic DNA (RAPD), amplified fragment length polymorphism (AFLP), PCR approaches targeting repeated sequences, DNA–DNA quantitative hybridization and microarray methods involving Single nucleotide polymorphisms (SNPs), whole genome chips, and pathochips. MLST involves determining the nucleotide sequence of a few genes conserved within the taxon being tested [29]. Absence of an expected gene in a sequencing attempt may reveal man-made recombination events. A disadvantage of this approach is that different gene sets appear to be ideal for different species. In MLVA (for example, [30]), the genome sequence of one strain is searched for simple sequence tandem repeats and primers designed to amplify across the region of repeats are then tested on a panel of strains to reveal which loci naturally exhibit polymorphism. If enough such polymorphic loci can be identified, they will likely be distributed over the whole genome and can thus also be identifiers for recombination events. The disadvantage is that the development of such typing systems takes time and would need to be developed for every potential problem microbe. RAPD and AFLP methods [31], though useful in individual laboratories, are difficult to standardize for routine validated use in multiple laboratories. Rep-PCR methods, which amplify repeated sequences in bacteria, are limited to certain species. SNPs, detectable by DNA synthesis methods from small primers such as SNaPshot [32] are useful when dealing with genomes with known fixed polymorphisms, particularly for rapidly evolving viruses having small genomes. DNA–DNA hybridization will readily reveal large replacements (insertions and deletions) in genomes. Microarray applications [33–35] include those in which whole or pathogenically important regions of select agents' genomes are arrayed on slides. Arrays useful for detecting and characterizing synthetic genomes also can be developed. SNPs can also be surveyed by microarray methods [36].

### 3.5 Gene Expression and Protein Modification—Plant Pathogen and Plant Host

An organism's genome provides insight into the potential transcripts that can be produced for subsequent translation, but the final complement of transcriptional and translational products in a pathogen or host can be significantly influenced by the interaction of organisms and the environment. The field of proteomics is rapidly expanding our ability to assess the impact of such regulation. In addition, as the cost of DNA sequencing declines and more sequences become available, their analysis can inform the characterization of genome transcription, providing information about environmentally influenced gene expression. High throughput microarrays can yield transcriptional signatures for both host and pathogen. Antibody microarrays and application of mass spectrometry to small samples have permitted significant advances. Thus, obtaining a "pathoprint" of a specific disease, i.e. all the biomolecules in a specific host–pathogen interaction, may be possible, providing greater precision in attributing or excluding a specific pathogen isolate as the cause of the disease.

### 3.6 Informatics and Data Analysis

Informatics plays a large role in forensic microbiological investigation, and agricultural crimes are no exception. At the level of genomes and genome sequences, although many useful comparative tools and databases have been developed, further refinement may be required. Major developments are needed at the organismal and ecosystem levels to interrelate information about pathogen distribution, vector distribution, and weather patterns into easily accessible models that allow comparison of natural versus man-made outbreaks.

## 4 CURRENT CONTRIBUTIONS OF THE FIELD TO HOMELAND SECURITY AND CRITICAL NEEDS ANALYSIS

### 4.1 Recent and Current Federal Initiatives

The US bioforensics capacity has been substantially enhanced in recent years. A significant new component is the DHS' () National Bioforensics Analysis Center (NBFAC), established at Fort Detrick, MD as part of the National Biodefense Analysis and Countermeasures Center (NBACC). The NBFAC mission is to be the lead federal agency in conducting forensic analysis on materials recovered following a biological attack, and to provide data from analyses to law enforcement agencies for prosecution of biocrimes. The creation of NBFAC presents an opportunity to develop a cooperative federal program addressing forensics gaps for high-priority microbial plant pathogens.

The Laboratory Division of the FBI has played a central role in the development of the emerging discipline of microbial forensics [7, 8]. FBI scientists organized and led a productive Scientific Working Group on Microbial Genomics and Forensics (SWGMGF), which has brought together individuals from various federal agencies involved in national security, the National Laboratories, academia, and industry. The SWGMGF identified research and training needs, set priorities, and provided information to agency administrators and funding units.

The USDA also has created new infrastructure in response to concerns about the security of US plant production systems. In 2002 the USDA Cooperative State Research, Education and Extension Service (CSREES) established the NPDN, a collective network of Land Grant University plant disease and pest diagnostic facilities located in each state [18], enhancing national agricultural security by facilitating rapid detection of introduced pests and pathogens. CSREES' National Research Initiative, a competitive grants program, created a small new, targeted program in Plant Biosecurity that supports integrated projects to facilitate research, extension, and education projects directed at assuring a safe, high-quality, affordable food and fiber for consumers in the United States and its international trade partners.

APHIS' PPQ program safeguards US agriculture and natural resources from the introduction, establishment, and spread of plant pests and noxious weeds (http://www.aphis.usda.gov/plant_health/plant_pest_info/biosecurity/index.shtml). APHIS emergency response is outlined in a National Response Plan, released in 2004 as directed in Homeland Security Presidential Directive (HSPD)-5. APHIS responsibilities, as outlined in the plan, include: "(i) Implement an integrated national-level response to an outbreak of an economically devastating or highly contagious animal/zoonotic exotic plant disease, or plant pest infestation, and (ii) In response to a biohazardous event, the decontamination and/or destruction of animals and plants as well as associated facilities

(e.g. barns, processing equipment, soil, and feeding and growing areas) may be required." As of 2007, a National Response Framework is under development to replace the National Response Plan.

Finally, in addition to conducting its own research relevant to plant biosecurity, the USDA's Agricultural Research Service (ARS) is responsible for implementing the new NPDRS, which was mandated under HSPD -9 (Agricultural Biosecurity). Plant Disease Recovery Plans are being developed for plant pathogen "select agents" listed under 7 CFR part 331 (seven plans developed to date) and for other high-priority threat agents. These plans have been developed by teams of plant pathology experts in government, academic, and private companies, under the direction of the USDA Office of Pest Management Policy. NPDRS resources are also directed at research gaps on new and emerging pathogens by the ARS National Program Staff.

### 4.2 Recent and Current Academic Efforts

Plant pathologists in several of the USDA-supported system of Land Grant Universities, as well as researchers in other academic institutions, have contributed significant research relevant to the emerging field of forensic plant pathology, addressing issues of plant disease epidemiology, diagnostics and pathogen strain discrimination, pathogen evolution and microbial background, and basic pathogen and vector biology. Such efforts are generally independent and focused within the investigator's specific area of expertise. The National Institute for Microbial Forensics and Food and Agricultural Biosecurity (NIMFFAB), established recently at Oklahoma State University to be a component of an overall national effort to safeguard plant and food resources, will provide a synergistic focal point to conduct interactive research, address policy issues, provide cross-disciplinary education and training, and participate in outreach activities, in plant pathology and forensic sciences. Rapid progress by either independent investigators or collaborative ventures has been constrained by the extremely limited amount of targeted funding, both federal and local, for plant biosecurity and agricultural bioforensics initiatives.

### 4.3 The Role of Professional Societies

The American Phytopathological Society (APS), a 5000-member international professional organization dedicated to plant health, has been a significant resource and scientific voice in US plant pathology research, education, outreach, and policy making. APS utilizes its strong publication house and press, interactions with related scientific societies and coalitions, and value-rich annual meetings that serve to bring plant pathology professionals together for scientific exchange. Since 2002, the APS Plant Pathogen Forensics Interest Group, composed of members from various Federal agencies, academic institutions, industry, and others, has met annually in conjunction with the APS Annual Meeting to review and plan US and global initiatives related to forensic plant pathology [19].

## 5 FUTURE RESEARCH–BUILDING CAPACITY AND SCIENCE

### 5.1 Gaps Assessment and Recommendations

*Prioritization of plant pathogens and threats.* With dozens of potential high-value crop targets capable of hosting thousands of pathogens [37] the amount of

information required to develop a comprehensive forensics information baseline in plant pathology vastly exceeds the capacity of the federal agricultural research funding base. Highest priority pathogens must be identified and prioritized. Criteria for plant pathogen prioritization have been developed using external funding [38], and refined in workshops sponsored by USDA and hosted by the American Phytopathological Society, under the NPDRS. Future prioritization efforts will focus on pathogens most likely to be applied in a biocrime, requiring a unique subset of criteria and focusing on deliberate introduction scenarios. The resulting list of highest priority plant pathogens should be forwarded to agricultural and biosecurity research program leaders for their use in developing and applying research priorities for forensics applications.

*Training and education.* Education and training are critical to a strong capability in the emerging discipline of forensic plant pathology [19]. Extant graduate plant pathology curricula are strong in molecular technology and basic sciences, both of which are necessary components of forensic science, but many have moved away from the field-based and applied plant pathology that must underpin targeted forensic investigations. A new paradigm of education, blending the disparate disciplines of plant pathology and forensic sciences, is needed to prepare a new cadre of plant pathologists having the range of expertise necessary for attribution of agricultural crime. Such a program will require close collaborations among educators, and must incorporate epidemiology, botany, biochemistry, microbial ecology, and phylogeny, and other relevant disciplines. Training cannot stop with graduate student education. Extension educators and staff, crop consultants, master gardeners, and others who may be called first in the case of a new and threatening agricultural emergency, also must learn key indicators of intentional pathogen release and appropriate reporting steps. Law enforcement personnel need to know how to recognize an agricultural crime and respond appropriately. These education needs pose challenges at a time when the Land Grant University system, primarily responsible for education in agriculture-relevant disciplines, are suffering from financial cutbacks, reduced faculty numbers, and falling research budgets.

*Forensic tools and procedures.* Better background knowledge of key plant pathogens is essential. Knowing whether a pathogen was present in the vicinity of the outbreak before the outbreak occurred is important when deciding whether a disease occurrence was natural or man-incited. For that reason it is important to consolidate scattered worldwide information on the occurrence of pathogens and potential pathogens in a structured, easily searchable database. Further surveys of what potential pathogens exist in natural and managed ecosystems is also needed to obtain a complete picture of the background against which outbreaks occur.

*The decision tree.* Deciding whether a crop disease is natural or man-made may be very challenging for law enforcement personnel. A series of criteria for making such a decision, or "decision tree," could facilitate this crucial early step, as happened during the investigation of a tularemia outbreak among residents of Kossovo, a nation in strife from 1999 to 2000 [39]. To assess allegations that the outbreak was the result of biowarfare, a series of 12 nonconclusive questions was devised. Answers were rated to reflect characteristics, such as "uncertain and indistinct" "peculiarities or suspicions"; "obvious peculiarities or indications"; "considerable peculiarities or deviations", or "no data available." Formulas converted the data to conclusions having a specified degree of confidence. A current NIMFFAB initiative

is to develop a similar decision tree for use in plant disease outbreaks, and to test the tree using, as a model, a common, endemic plant disease for which a direct comparison can be made between a natural outbreak and an intentional, man-made event (such as those commonly created for assessment of disease-resistance or pesticide efficacy among crop cultivars). Criteria by which an outbreak would be considered potentially intentional could include, but are not limited to, factors such as (i) disease occurrence in a new geographical location; (ii) pattern of disease in the field unexpected based on normal pathogen dissemination methods; (iii) if an insect vector is required for dissemination, disease present without evidence of vector; (iv) disease appears at an unusual time of year, or under normally unsupportive climatological conditions; (v) pathogen is unusual in some way; (vi) pathogen has unusual features; or (vii) evidence of unauthorized human presence is found.

### 5.2 Targeted Funding for Research and Education/Training

Unlike diseases of humans and production animals, those of plants are usually managed within large host populations. Since eradication of infected host plants is generally unsuccessful, most of the limited funding for plant biosecurity-related research and education has targeted the development of new approaches for pathogen detection, understanding plant pathogen epidemiology, or identification of disease resistant plant material. That a plant disease could result from a criminal act has been a new perspective within the plant pathology community. The plant pathology and US security communities now recognize and support the emergence of a new discipline of plant pathogen forensics, but the lack of targeted funding for research and education efforts directly related to forensics for plant diseases has constrained progress. The focused adaptation and extension of our national plant pathology capabilities to meet the needs of microbial forensic investigation will require the attention of Federal funding agency decision-makers and the creation of targeted funding opportunities for development of technologies and resources to enhance national capability to identify, trace, and attribute criminal assaults on plant-based resources.

### 5.3 Cross Communication Among Plant, Veterinary, and Human Systems

Although specific case details and appropriate responses will differ, the needs of the plant pathologist–forensic scientist will be very similar to those of forensic investigators in public health and veterinary sciences with respect to disease epidemiology, molecular biology and detection technologies, sample collection and handling, and other forensic tools, as both seek to determine the origin and source of an outbreak [19]. Close communication among microbial forensics investigators in all three areas will promote synergy and optimization in the use of limited resources. Encouragement of collaborative research, especially by the creation of targeted funding programs, the development of blended and forensics-focused scientific meetings, and other cross-disciplinary activities will facilitate effective communications.

## REFERENCES

1. American Phytopathological Society Public Policy Board. (2002). The American Phytopathological Society, first line of defense.~APSnet. http://www.apsnet.org [online].

2. Casagrande, R. (2000). Biological terrorism targeted at agriculture: the threat to U.S. national security. *Nonprolif. Rev.* Fall-Winter, 92–105. http://cns.miis.edu/pubs/npr/vol07/73/73casa.pdf. [Online.]
3. Madden, L., and Wheelis, M. (2003). The threat of plant pathogens as weapons against U.S. crops. *Annu. Rev. Phytopathol.* **41**, 155–176.
4. Wheelis, M., Casagrande, R., and Madden, L. V. (2002). Biological attack on agriculture: low-tech, high impact bioterrorism. *Bioscience* **52**, 569–576.
5. Whitby, S. M. (2001). The potential use of plant pathogens against crops. *Microbes Infect.* **3**, 73–80.
6. Whitby, S. M. (2002). *Biological warfare against crops*, Palgrave, Basingstoke, U.K., pp. 271.
7. Budowle, B., (2003). Defining a new forensic discipline: Microbial Forensics. Profiles in DNA **6**: 7–10. [Online.] http://www.promega.com/profiles/601/ProfilesInDNA_601_07.pdf.
8. Budowle, B., Burans, J., Breeze, R. G., Wilson, M. R., Chakraborty, R.. (2005a). Microbial forensics. In *Microbial Forensics*, R. G. Breeze, B. Budowle, and S. E. Schutzer, Eds. Elsevier Academic Press, Burlington, MA, pp. 1–26
9. Budowle, B., Johnson, M. D., Fraser, C. M., Leighton, T. J., Murch, R. S., and Chakraborty, R. (2005b). Genetic analysis and attribution of microbial forensics evidence. *Crit. Rev. Biotechnol.* **31**, 233–254.
10. Budowle, B., Murch, R. S., and Chakraborty, R. (2005c). Microbial forensics: the next forensic challenge. *Int. J. Legal Med.* **119**, 317–330.
11. Murch, R. S. (2003). Microbial forensics: building a national capacity to investigate bioterrorism. *Biosecur. Bioterror. Biodef. Strat. Pract. Sci.* **1**, 117–122.
12. United States Environmental Protection Agency Ag 101. (2008) http://www.epa.gov/agriculture/ag101/index.html
13. Sutton, V., and Bromley, D. L. (2005). Understanding technologies of terror. *Technol. Soc.* **27**, 263–285.
14. Livingston, M., Johansson, R., Daberkow, S., Roberts, M., Ash, M., and Breneman, V. (2004). *Economic and Policy Implications of Wind-borne Entry of Asian Soybean Rust into the United States*, Electronic Outlook Report OCS-04D-02, USDA Economic Research Service.
15. Nutter, F. W. Jr. (2004). Post-introduction mapping of new and emerging agricultural pathogens in real-time using GPS and GIS technologies. (Abstr.). *Phytopathology* **94**, S130.
16. Nutter, F. W. Jr., and Madden, L. V. (2002). Plant diseases as a possible consequence of biological attack. In *Biodefense: Principles and Pathogens*, M. S. Bronze, and R. A. Greenfield, Eds. Horizon Bioscience, Norwich, pp. 793–818.
17. Madden, L. V., and Hughes, G. (1999). Sampling for plant disease incidence. *Phytopathology* **89**, 1088–1103.
18. Hughes, G., Madden, L., and Gottwald, T. R. (2004). Strategies of sampling for detection. *Phytopathology* **94**, S137.
19. Stack, J., Cardwell, K., Hammerschmidt, R., Byrne, J., Loria, R., Snover-Clift, K., Baldwin, W., Wisler, G., Beck, H., Bostock, R., Thomas, C., and Luke, E. (2006). The national plant diagnostic network. *Plant Dis.* **90**, 128–136.
20. Fletcher J., Bender C. L., Budowle B., Cobb W. T., Gold S. E., Ishimaru C. E., Luster D. G., Melcher U. K., Murch R. L., Scherm H., Seem R. C., Sherwood J. L., Sobral B., and Tolin S. A. (2006). Plant pathogen forensics: capabilities, needs and recommendations. *Microbiol. Mol. Biol. Rev.* **70**, 450–471.
21. Budowle, B., Schutzer, S. E., Burans, J. P., Beecher, D. J., Cebula, T. A., Chakraborty, R., Cobb, W. T., Fletcher, J., Hale, M. L., Harris, R. B., Heitkamp, M. A., Keller, F. P., Kuske, C., LeClerc, J. E., Marrone, B. L., McKenna, T. S., Morse, S. A., Rodriguez, L. L., Valentine, N. B., and Yadev, J. (2006). Quality sample collection, handling, and preservation for an effective microbial forensics program. *Appl. Environ. Microbiol.* **72**, 6431–6438.

22. Jacobson, R. H. (1998). Validation of serological assays for diagnosis of infectious diseases. *Rev. Sci. Tech.* **17**, 469–486.
23. Jacobson, R. H. (2000). Principles of validation of diagnostic assays for infectious diseases. In *OIE Manual of Standards for Diagnostic Tests and Vaccines*, 4th ed., Office International des Epizooties, Paris, France. pp. 10–17.
24. Wright, P., and Zhou, E.-M. (1999). Developments in international standardization. *Vet. Immunol. Immunopathol.* **72**, 243–248.
25. Lartigue, C., Glass, J. I., Alperovich, N., Pieper, R., Parmar, P. P., Hutchison, C. A. III, Smith, H. O., Venter, J. C. (2007). Genome transplantation in bacteria: changing one species to another. *Science* **317**, 632–638 DOI:10.1126/science.1144622.
26. Margulies, M., Egholm, M., Altman, W. E., Attiya, S., Bader, J. S., Bemben, L. A., Berka, J., Braverman, M. S., Chen, Y. J., Chen, Z. T., Dewell, S. B., Du, L., Fierro, J. M., Gomes, X. V., Godwin, B. C., He, W., Helgesen, S., Ho, C. H., Irzyk, G. P., Jando, S. C., Alenquer, M. L. I., Jarvie, T. P., Jirage, K. B., Kim, J. B., Knight, J. R., Lanza, J. R., Leamon, J. H., Lefkowitz, S. M., Lei, M., Li, J., Lohman, K. L., Lu, H., Makhijani, V. B., McDade, K. E., McKenna, M. P., Myers, E. W., Nickerson, E., Nobile, J. R., Plant, R., Puc, B. P., Ronan, M. T., Roth, G. T., Sarkis, G. J., Simons, J. F., Simpson, J. W., Srinivasan, M., Tartaro, K. R., Tomasz, A., Vogt, K. A., Volkmer, G. A., Wang, S. H., Wang, Y., Weiner, M. P., Yu, P. G., Begley, R. F., and Rothberg, J. M. (2005). Genome sequencing in microfabricated high-density picolitre reactors. *Nature* **437**, 376–380.
27. Read, T. D., Salzberg, S. L., Pop, M., Shumway, M., Umayam, L., Jiang, L., Holtzapple, E., Busch, J. D., Smith, K. L., Schupp, J. M., Solomon, D., Keim, P., and Fraser, C. M. (2002). Comparative genome sequencing for discovery of novel polymorphisms in *Bacillus anthracis*. *Science* **296**, 2028–2033.
28. Ye, F., Melcher, U., Rascoe, J. E., and Fletcher, J. (1996). Extensive chromsome aberrations in *Spiroplasma citri* strain BR3. *Biochem. Genet.* **34**, 269–286.
29. Jordan, I. K., Rogozin, I. B., Wolf, Y. I., and Koonin, E. V. (2002). Microevolutionary genomics of bacteria. *Theor. Popul. Biol.* **61**, 435–447.
30. Wassenaar, T. M. (2003). Molecular typing of pathogens. *Berl. Munch. Tierarztl. Wochenschr.* **116**, 447–453.
31. Monteil, M., Durand, B., Bouchouicha, R., Petit, E., Chomel, B., Arvand, M., Boulouis, H.-J., and Haddad, N. (2007). Development of discriminatory multiple-locus variable number tandem repeat analysis for *Bartonella henselae*. *Microbiology* **153**, 1141–1148.
32. Baransel, A., Dulger, H. E., and Tokdemir, M. (2004). DNA amplification fingerprinting using 10 x polymerase chain reaction buffer with ammonium sulfate for human identification. *Saudi Med. J.* **25**, 741–745.
33. Makridakis, N. M., and Reichardt, J. K. (2001). Multiplex automated primer extension analysis: simultaneous genotyping of several polymorphisms. *Biotechniques* **31**, 1374–1380.
34. Bodrossy, L., and Sessitsch, A. (2004). Oligonucleotide microarrays in microbial diagnostics. *Curr. Opin. Microbiol.* **7**, 245–254.
35. Kingsley, M. T., Straub, T. M., Call, D. R., Daly, D. S., Wunschel, S. C., and Chandler, D. P. (2002). Fingerprinting closely related *Xanthomonas* pathovars with random nonamer oligonucleotide microarrays. *Appl. Environ. Microbiol.* **68**, 6361–6370.
36. Willse, A., Straub, T. M., Wunschel, S. C., Small, J. A., Call, D. R., Daly, D. S., and Chandler, D. P. (2004). Quantitative oligonucleotide microarray fingerprinting of *Salmonella enterica* isolates. *Nucleic Acids Res.* **32**, 1848–1856.
37. Xiao, P. F., Cheng, L., Wan, Y., Sun, B. L., Chen, Z. Z., Zhang, S. Y., Zhang, C. Z., Zhou, G. H., and Lu, Z. H. (2006). An improved gel-based DNA microarray method for detecting single nucleotide mismatch. *Electrophoresis* **27**, 3904–3915.

38. Madden, L. V. (2001). *What are the Nonindigenous Plant Pathogens that Threaten U.S. Crops and Forests?* APSnet Feature Article. www.apsnet.org/online/feature/exotic/.

39. Schaad, N. W., Abrams, J., Madden, L. V., Frederick, R. D., Luster, D. G., Damsteegt, V. D., and Vidaver, A. K. (2006). An assessment model for rating high-threat crop pathogens. *Phytopathology* **96**, 616–621.

40. Grunow, R., and Finke, E.-J. (2002). A procedure for differentiating between the intentional release of biological warfare agents and natural outbreaks of disease: its use in analyzing the tularemia outbreak in Kosovo in 1999 and 2000. *Clin. Microbiol. Infect.* **8**, 510–521.

## FUTHER READING

National Research Council, Committee on Biological Threats to Agricultural Plants and Animals. (2003). *Countering Agricultural Bioterrorism*, National Academies Press, Washington, DC.

# POTENTIAL FOR HUMAN ILLNESS FROM ANIMAL TRANSMISSION OR FOOD-BORNE PATHOGENS

DAVID M. HARTLEY

*Department of Radiology, Georgetown University School of Medicine, Washington, DC*

## 1 INTRODUCTION

Humans become infected with pathogens via aerosol, oral, and percutaneous pathways. Infection may produce a spectrum of outcomes, ranging from asymptomatic and self-limited disease, to long-term sequelae, to death. During the Cold War, several nations exploited these facts to develop biological weapons for use against humans. Designed to achieve specific strategic or tactical military objectives efficiently, weapons were based on a limited number of agents and designed to be delivered primarily as small particle aerosols [1, 2]. In contrast, bioterrorists may employ a multiplicity of microbial agents, delivered via diverse pathways, against civilian populations. The diversity of entryway and a spectrum of outcomes makes bioterrorism a difficult problem to characterize and defend against.

In this article we focus on diseases of humans associated with animals or food and foodstuffs, which have demonstrated potential to disrupt populations and societies. Human illness could result from a bioterrorist infecting animal species (e.g. livestock,

wildlife, and insect vectors) or food and foodstuffs with biological agents aimed at human populations, or as "collateral damage" in a biological attack aimed at domestic livestock. Volumes have been written on zoonotic and food-borne illnesses; this is a brief resume. However broad, three underlying themes are evident: (i) the threat spectrum is very broad; (ii) options for disease control are diverse and often problematic; and (iii) there is a need for creative approaches to both threat analysis and control and prevention.

## 2 SCIENTIFIC OVERVIEW

This is a brief overview of zoonotic and food-borne threats. Details regarding individual agents and diseases can be found in the References and Further Reading sections.

### 2.1 Zoonotic Threats

***2.1.1 Scope of the Problem.*** Diseases of humans acquired from animal sources or reservoirs—zoonoses—have figured prominently in human health historically. For example, *Yersinia pestis*, the causative agent of plague, is carried by different rodents, lagomorphs, and feline species and vectored to humans by fleas. In the fourteenth century an epidemic of bubonic and pneumonic plague caused the death of an estimated one-third of the population of Europe [3]. Reverberations from this event lasted for centuries; even today the word plague carries the connotation of a disastrous affliction.

***2.1.2 Agents.*** The United States Department of Health and Human Services (DHHS) has published a list of agents important for biodefense (Table 1), many of which are zoonotic. The United States Department of Agriculture (USDA) has an analogous list of agents relevant to livestock health, the majority of which do not cause human disease. The intersection of these describes some 20 zoonotic pathogens of public health importance. The threat to human health, however, is much broader. A standard reference describes approximately 150 zoonoses and communicable diseases common to man and animals, and new and novel zoonoses continue to be recognized [4–8]. Table 2 contains additional threat agents that do not appear on the HHS and USDA lists, but nonetheless command respect.

***2.1.3 Transmission.*** Many zoonotic agents infect humans via multiple pathways. *Y. pestis*, for example, can be transmitted from rodents to humans via biting fleas, droplets, and aerosols. Rift Valley fever (RVF) virus is transmitted to humans from ungulate species via mosquitoes, via aerosolized blood or body fluids from a viremic animal or abortus, and possibly through contact with infected meat. *Bacillus anthracis*, which often spreads from animals to humans via direct contact, can also infect humans via contaminated food and inhalation. *Francisella tularensis* can infect humans via biting arthropods, aerosols, or by handling and consuming infected meat and water. Severity of illness can depend upon the route of infection. In the case of *B. anthracis*, for example, cutaneous anthrax has a much lower case fatality rate (CFR; ~20%) than inhalation anthrax (~90%) [10]. Similar remarks apply to bubonic versus pneumonic plague and vector-borne versus pneumonic tularemia.

**TABLE 1 HHS Select Agents and Toxins**

| Non-Overlap Agents and Toxins (HHS list only) | Overlap Agents and Toxins (common to HHS and USDA lists) |
|---|---|
| **Bacteria, Fungi, and Rickettsia** | |
| Coccidioides posadasii | *Bacillus anthracis*[a] |
| *Rickettsia prowazekii*[a] | *Botulinum neurotoxin producing species of Clostridium* |
| *Rickettsia rickettsii*[a] | *Brucella abortus*[a] |
| *Yersinia pestis*[a] | *Brucella melitensis*[a] |
| | *Brucella suis*[a] |
| | *Burkholderia mallei* (formerly *Pseudomonas mallei*)[a] |
| | *Burkholderia pseudomallei* (formerly *Pseudomonas pseudomallei*)[a] |
| | *Coccidioides immitis*[a] |
| | *Coxiella burnetii*[a] |
| | *Francisella tularensis*[a] |
| **Toxins** | |
| Abrin toxin | Botulinum neurotoxins |
| Conotoxins | *Clostridium perfringens* epsilon toxin |
| Diacetoxyscirpenol | Shigatoxin |
| Ricin | Staphylococcal enterotoxins |
| Saxitoxin | T-2 toxin |
| Shiga-like ribosome inactivating proteins | |
| Tetrodotoxin | |
| **Viruses** | |
| Cercopithecine herpesvirus (Herpes B virus) | Eastern Equine Encephalitis virus[a] |
| Crimean-Congo hemorrhagic fever virus[a] | Hendra virus[a] |
| Ebola Virus[a] | Nipah Virus[a] |
| Lassa fever virus[a] | Rift Valley fever virus[a] |
| Marburg virus[a] | Venezuelan Equine Encephalitis virus[a] |
| Monkeypox virus[a] | |
| Reconstructed replication competent forms of the 1918 pandemic influenza virus containing any portion of the coding regions of all eight gene segments (Reconstructed 1918 Influenza virus) | |
| South American hemorrhagic fever viruses (Flexal, Guanarito, Junin, Machupo, Sabia)[a] | |
| Tick-borne encephalitis complex (flavi) viruses (Central European tick-borne encephalitis, Far Eastern tick-borne encephalitis, Kyasanur forest disease, Omsk hemorrhagic fever, Russian spring and summer encephalitis)[a] | |
| Variola major virus (Smallpox virus) | |
| Variola minor virus (Alastrim) [9] | |

[a]Zoonotic agents

**TABLE 2 Selected Additional Zoonotic Agents Posing Threats to Human Health**

| |
|---|
| *Borrelia burgdorferi* |
| *Campylobacter jejuni* |
| *Leptospira interrogans* |
| *Staphylococcus aureus* |
| **Viruses** |
| Rabies |
| Mosquito-borne flaviviruses (West Nile, Japanese Encephalitis) |
| Sin nombre |
| Yellow fever |
| Emerging and yet-to-emerge influenza |
| SARS coronavirus |
| **Prion** |
| vCJD prion |
| **Parasite** |
| *Trypanosoma cruzi* |

***2.1.4 Disease Ecology.*** Many zoonoses are transmitted in distinct areas suited to their transmission and persistence. If such agents are translocated to new geographic areas, they may be successful if ecologic conditions are suitable. Many factors contribute to suitability, including *inter alia* land use, host population abundance, climate, presence and density of reservoir species, and vector capacity among indigenous arthropods. For example, in the 1999 North American introduction of West Nile virus (WNV), the agent found a diverse set of wildlife hosts and competent mosquito vectors, facilitating effective local and long-range spread (and thereby increasing human morbidity). Other examples of the translocation of pathogens to immunologically naïve regions include *Y*. pestis, which entered the Western United States in the late nineteenth century, finding wildlife and domestic hosts, and persists to the present; and RVF virus, which entered the Arabian Peninsula in 2000, and continues to circulate [11]. In general, the interactions between, and the relative importance and significance of, specific ecologic factors will differ from agent to agent.

A zoonosis introduced into an immunologically naïve population may behave differently, epidemiologically, than it does in endemic regions [12]. In the case of WNV in North America, for example, disease in both humans and wildlife species was more severe than recent observations in Europe and the Middle East would have suggested [13]. Transmission and disease severity are complex functions of environment, host resistance, and immunity, and properties of the agents themselves (all of which are dynamic).

***2.1.5 Disease Diversity.*** As a whole, zoonotic agents cause a spectrum of disease. Toward the less virulent end of the spectrum is WNV, in which the proportion of asymptomatic infections may be as high as 80%; neuroinvasive disease occurs in a small minority of cases. More virulent RVF is rarely asymptomatic, typically resulting in self-limited febrile illness; a minority of cases results in severe complications including

**TABLE 3 Human Vaccines for Zoonotic Threat Agents**

| Agent | Vaccine Type | Status |
|---|---|---|
| Eastern equine encephalitis virus | Inactivated | IND[a], but no longer produced |
| Japanese Encephalitis virus | Inactivated | US licensed vaccine |
| Junin virus | Live attenuated | Not US licensed. Meets requirements for IND application |
| Kyasanur virus | Inactivated | Not US licensed. Shown to be effective in field trials in India |
| Monkeypox virus | Live attenuated | Same as smallpox virus vaccine (and thus part of the US Strategic National Stockpile) |
| Rabies virus | Inactivated | US licensed vaccine |
| Rift Valley fever virus | Inactivated | IND |
| | Live attenuated | Under IND |
| Tick-borne encephalitis virus | Inactivated | Not US licensed. Available in Europe |
| Yellow fever virus | Live attenuated | US licensed |
| Venezuelan equine encephalitis virus | Live attenuated | IND, but no longer produced |
| | Inactivated | IND, but no longer produced |
| *Bacillus anthracis* | Inactivated cell-free | US licensed vaccine. Part of the US Strategic National Stockpile |
| *Coxiella burnetii* | Inactivated | IND, but no longer produced |
| *Francisella tularensis* | Live attenuated | Not currently available in the US |
| *Yersinia pestis* | Inactivated | Effective against bubonic but not pulmonary plague. No longer produced |

[a]IND is required in the United States before a product undergoes human testing. [See 22 - Refs 3, 10, 14–16, Chapter 3]

hepatitis, retinal hemorrhage, and hemorrhagic fever. At the most virulent end of the spectrum are Marburg virus and Ebola virus, fatal in as much as 90% of all cases.

***2.1.6 Therapy and Prevention.*** Antimicrobial and vaccine prophylaxis is available for a subset of the agents shown in Tables 1, 2. Antibiotic resistance is observed in some pathogens. Multidrug-resistant *Y. pestis* has been observed in outbreaks in Madagascar [17]. Vaccines exist for a small subset of the zoonoses (Table 3); many possess poor epidemiologic properties (e.g. low protective efficacy, short period of protection) and undesirable side effects (e.g. teratogenisis, severe local tissue reaction). Personal protective measures including barrier precautions, breathing apparatus, and vector repellent can have good protective efficacy; which are appropriate are agent- and scenario-dependent.

At the population level, public health measures including vector and reservoir species control can be effective. However, such measures can have unintended consequences and should be considered with respect to the scenario. Theoretically, for example, indiscriminant rodent culling in plague-endemic areas could result in a shortage of natural hosts for vectors carrying *Y. pestis* [18]. Fleas abandoning dead rodents could instead infest human habitations, spawning transmission of bubonic plague. In other cases it may be possible to protect humans by controlling disease in intermediate hosts. For example, in

the case of RVF it is theorized that the most effective approach for human protection is to vaccinate domestic livestock populations.

## 2.2 Food-Borne Threats

***2.2.1 Scope of the Problem.*** Modern food production and storage technology has caused massive declines in food-borne illness. Nonetheless, outbreaks continue to occur, facilitated by, *inter alia*, centralized food production and supply systems; the growing frequency of imported food and foodstuffs from nations with less-developed agricultural and production procedures and practices; and lapses in good preparation and serving practices in dining establishments and homes. These and related avenues represent potential targets of bioterrorism [19].

***2.2.2 Agents.*** Foods ready to eat as well as their ingredients can carry a large number of pathogens and toxins. There is no analog of the DHHS select agent list for food-borne pathogens; Table 4 contains a representative collection. Generally, pathogens must pass the gastric barrier successfully and colonize the gut to produce disease. Disease can (but need not) be toxin-mediated, meaning that toxins are produced as a by-product of microbial growth in the gut. Foods contaminated with toxins at the time of consumption can produce disease regardless of microbial growth in the gut (food-borne intoxication).

***2.2.3 Transmission.*** Poor food sanitation and handling practices are important causes of disease. Secondary transmission via fecal—oral routes is possible for many viral and bacterial pathogens, due to a combination of high levels of pathogen shedding, viability and persistence of the agents in the environment and the low infectious dose. For example, depending on the age and condition of host, the infective dose for *Shigella* species may be as low as 10–100 cells. The $ID_{50}$ (dose sufficient to infect 50% of exposed persons) infectious dose of *Vibrio cholerae* may be as high as $10^3$ organisms, but recent observations imply a "hyperinfectious" state of the organism in which this is reduced by 1–2 orders of magnitude for a short time after the pathogen is shed by the host [20]. Whether hyperinfectious states exist for other enteric pathogens of humans remains unknown. Generally, the $ID_{50}$ of food-borne organisms are incompletely known and variable, depending, *inter alia*, upon the food matrix within which they are consumed and the acidity of the gastric environment. Toxins can be extremely potent; botulinum toxin A (a protein neurotoxin), for example, possesses a mean lethal dose $<0.001\,\mu g/kg$ and has been called *the most lethal substance known to humans* [21].

***2.2.4 Disease Ecology.*** Many enteric pathogens are ubiquitous in the natural environment. *Clostridium botulinum*, for example, is found commonly in soil and can contaminate food or foodstuffs anytime between harvest and preparation. *C. botulinum* spores can germinate and grow, producing toxins, in anaerobic environments. Home and occasionally commercially canned products have been implicated in botulism cases; other foods associated with botulism include herb-infused oils, bottled garlic, and baked potatoes in aluminum foil that have been held warm for extended periods of time. *C. botulinum* subtypes may produce one or more of seven types of toxin that readily cross the gastric acidic barrier. *Vibrio* species (including *V. cholerae*, *Vibrio parahaemolyticus* and *Vibrio vulnificus*) are common in estuarine and marine environments, frequently contaminating water and shellfish. *V. cholerae* is also a major cause of disease in areas lacking effective water treatment and sanitation systems.

***2.2.5 Disease Diversity.*** Food-borne agents cause a broad spectrum of disease. Toward the less virulent end of the spectrum are the Norwalk-like viruses and enterotoxigenic (ETEC) strains of *Escherichia coli* (CFRs in nonpediatric and nongeriatric populations near 1%). More virulent are the enterohemorrhagic *Escherichia coli* (EHEC) and other shigatoxin-producing *Escherichia coli* (STEC), often associated with hemolytic uremic syndrome (HUS), kidney failure, and death. Toward the most virulent end of the spectrum are *Shigella dysenteriae* and *E. coli* O157:H7, associated HUS; *Campylobacter jejuni*, associated with Guillain—Barre syndrome; and variant Creutzfeldt—Jakob disease (vCJD) prion ($PrP^{Sc}$), which may be latent for years but conveys near 100% mortality.

***2.2.6 Therapy and Prevention.*** Antibiotics may be indicated for some bacterial infections (e.g. *Listeria monocytogenes, Brucella* spp., *B. anthracis*) but are contraindicated for many others (e.g. EHEC). Many agents are developing antibiotic resistance. For viral diseases and nonviral diseases if antibiotics are contraindicated, therapy is limited to supportive measures. Vaccines exist for very few agents as seen in Table 4. A rotovirus vaccine was approved for infants in the United States in 1998 but was removed in 1999 when it was found to be associated with intussusception. Currently, available cholera vaccine provides weak (~50%) protection 3–6 months after administration; new vaccines are under development [22]. Investigational vaccines exist for ETEC and *Shigella* strains. Investigational antitoxins exist for botulinum toxin, but must be given early in the course of the disease.

Given the limited chemoprophylactic and chemotherapeutic options, preventive measures are central to avoiding food-borne illnesses. Food inspection and good practice in food sanitation and hygiene may be the first line of defense in preventing an introduced food-borne illness, especially secondary cases of infection. With few exceptions, proper food manufacturing, storage, and preparation practices can prevent illness. Exceptions include *Staphylococcus aureus* and some *Bacillus* species, which produce heat-stable toxins. At the population level, the "hazard analysis and critical control point" (HACCP) approach has proven effective in reducing the microbial load of foods and foodstuffs, and thus the incidence of disease.

As the comments of this section suggest, a bioterrorist attack on livestock could result in human illness via multiple pathways, including vector-borne transmission (e.g. RVF, eastern equine encephalitic (EEE)), aerosols (e.g. RVF), infected meat or milk (e.g. brucellosis), and direct contact (e.g. anthrax, glanders). People at primary risk would include agricultural and abattoir workers and those associated with handling animals and raw foodstuffs. Introduction of multiple agents into wildlife species could similarly result in human disease in anyone exposed to wildlife or wildlife-feeding vectors. Regarding food-borne attacks, proper production, preservation, and preparation practices can safeguard against contamination (but may not render heat-stable toxins inert). Post-production contamination, or contamination of foods that are traditionally not cooked or are eaten raw (e.g. lunch meat, fruits, and vegetables), may have a high probability of producing human disease.

## 3 CURRENT RESEARCH

In this section we highlight research directly related to detection, control, and prevention of human illness events (i.e. sporadic cases or outbreaks).

**TABLE 4 Selected Food- and Water-borne Agents Posing Threats to Human Health**

| |
|---|
| **Bacteria** |
| *Bacillus anthracis, B. cereus* |
| *Brucella* species |
| *Campylobacter jejuni* |
| *Clostridium botulinum, C. perfringens* |
| Enterovirulent *Escherichia coli* (including EHEC, ETEC, EPEC, and EIEC strains) |
| *Listeria monocytogenes* |
| *Salmonella typhi* |
| *Shigella* species |
| *Staphylococcus aureus* |
| *Streptococcus pyogens* |
| *Vibrio cholerae, V. parahaemolyticus, V. vulnificus* |
| *Yersinia enterocolitica* |
| **Viruses** |
| Calciviruses |
| Hepatitis A virus |
| Rotovirus |
| Astroviruses |
| Adenoviruses |
| Parvoviruses |
| **Parasites** |
| *Cryptosporidium parvum* |
| *Cyclospora cayetanensis* |
| *Giardia lamblia* |
| *Toxoplasma gondii* |
| **Toxins** |
| Anatoxin A |
| Botulinum toxin |
| Ciguatera toxin |
| Epsilon toxin of *C. perfringens* |
| Staphylococcal enterotoxins |
| Saxitoxin |
| T-2 mycotoxin |
| Tetrodotoxin |
| Ref. [21] |

### 3.1 Detection

Early outbreak detection can reduce human illness. There are two essential approaches to event detection: detection by health care providers and detection via the exploitation of surveillance data. In the first category, the incidence of disease in individual health care facilities is detected by clinical laboratory tests. For most organisms of interest, sensitive, and specific microbiologic tests provide results within minutes to days of specimen collection. Higher performance tests are under development (discussed elsewhere in this *Handbook*). Typically, infections are noted by periodic manual chart review or computer

data mining and reported, as appropriate, to public health agencies. In the United States, "notifiable diseases" vary between states; if a particular disease is not notifiable, cases may be reported weeks or months later, and possibly not at all.

Surveillance is the "ongoing, systematic collection, analysis, and interpretation of outcome-specific health data, coupled with the timely dissemination of these data and their analyses" to medical, public health, and homeland security stakeholders [23]. Surveillance can entail the active or passive collection of data such as laboratory-confirmed cases (the most common), incidence of disease syndromes, human behavior thought to be associated with outbreaks, or environmental specimens. In the United States, public health surveillance data regarding many of the agents discussed in this article are reported to different Centers for Disease Control and Prevention (CDC) national surveillance systems (e.g. the National Notifiable Diseases Surveillance System [NNDSS] and the Food-borne Disease Active Surveillance Network [FoodNet]). No single surveillance system in the United States conducts surveillance for all bioterrorism-related agents or conditions [24]. A recent study, for example, identified more than 20 US-based networks for food-borne diseases alone [25]. Syndromic surveillance and human behavior/social disruption surveillance are under active development at present [26, 27].

Surveillance of air samples is carried out in various US cities. Specimens from collectors are removed periodically and analyzed for the presence of certain agents [28]. Details regarding this system, known as *BioWatch*, are scarce. However, the system has produced a number of alerts in different cities, all focused on the zoonotic agent *F. tularensis*. Domestic or wild animals can serve as sentinels of infection (e.g. avian influenza virus [29] and arboviruses [30]). A recent analysis [31] reviewed the potential of animals as sentinels of bioterrorism agents, concluding that "for certain bioterrorism agents, pets, wildlife, or livestock could provide early warning" of an attack.

Event detection from surveillance data is a complex function of measured observables and analytic methodology. The main objective is to identify a signal corresponding to a biological event of interest in a noisy and often ill-defined background. Mathematical and statistical approaches to analyzing such data at present include: spatial, temporal, and spatio—temporal clustering analyses; data mining; multivariable monitoring; and data fusion. Some approaches can be automated and/or executed in real- or near real-time. A review the statistical issues and challenges associated with timely integration of multiple data sources for purposes of detecting epidemiologic events can be found in reference [32, 33]

### 3.2 Control and Intervention

Control and intervention research focuses on discovering new chemoprophylactic and chemotherapeutic agents and identifying public health measures. Gaps revealed in Table 3 are the reason for current emphasis on developing new and improved vaccines. Such efforts, however, are not as vigorous as they could be due to the economic situation facing pharmaceutical companies. Lang and Wood [34] note that "costs from research to licensure, the risks inherent in vaccine development (e.g. technological constraints, regulatory approval), and the short- and long-term market financial evaluations (e.g. net present value, return on investment) are key factors in the decision to develop a vaccine" for rare diseases. Despite efforts to offset these risks (e.g. the Orphan Drug Act of 1982, the BioShield Act of 2004), discovery and development of new vaccines in the United States remains depressed. Similar comments apply to antibiotics.

To spur research and development in drug and other biodefense technology development, the US National Institutes of Health (NIH) and Department of Homeland Security (DHS) sponsor academic "Centers of Excellence" in bioterrorism defense research. Each center is a consortium focused on either a specific topic (DHS centers) or serving specific geographical regions (NIH centers). (See URLs listed in Further Reading.) Among others, vaccines for tularemia, RVF, and brucellosis are being studied at these centers. Additional researches focus upon diagnostic technology and analytic methodologies.

Identifying effective (or finding new) public health measures involves a range of analytic activity. Traditional epidemiologic observational studies identifying infection risk factors are useful, particularly for newly recognized agents about which little is known. Mathematical modeling and simulation techniques have led to fundamental insights regarding contagion processes and the applied practice of public health [35, 36]. Mathematical models enable evaluation of control and intervention measures such as vaccination (e.g. impact of protective efficacy, time-to-protection, and rate of administration), vector control (e.g. impact of adulticides vs. larvicides, spraying frequency, spraying concentration), host culling (e.g. impact of the rate of culling, effects of incomplete culling), and reduction in exposure rates, without costly or difficult laboratory experiments.

Models are built upon knowledge of the epidemiology of specific diseases. If properly constructed and analyzed, they can provide information on the effects of different controls or other quantities of interest. Thus, models can guide further laboratory research as well as provide defense planners with valuable guidance. At present, the literature reveals a paucity of applications to zoonoses. Current work by modelers at the DHS National Center of Excellence for Foreign Animal and Zoonotic Disease Defense [37] is noteworthy because it involves experts in human and agricultural medicine, human and agricultural epidemiology, microbiology, mathematics, ecology, geography, and information technology. The effort is addressing aspects of spatio—temporal vulnerability to RVF introduction, the relative payoff of possible control and intervention measures, and the economic impacts of an introduction into the United States.

A related methodology is risk assessment (RA), which aims to identify what events can happen, their likelihood, and their consequences. RA grew out of methods developed for assessing health impacts from chemical exposure. Typically, there are four stages to RA: hazard identification, exposure assessment, dose-response assessment, and risk characterization. Qualitative RA is descriptive and indicates whether disease is likely under specified conditions of exposure, whereas quantitative RA provides numerical estimates of risk [38]. Both types are relevant for risk management and communication in biodefense. RA has been applied to several bioterrorism issues, including the risk of a RVF incursion and its persistence within the European Community [39]. However, methodological and data gaps exist that continue to limit researchers ability to complete comprehensive RAs for most biothreat agents.

Regarding food safety and microbial contamination, microbial risk assessment (MRA) is under active development at present. MRA recognizes the biologic nature of organisms and accounts for it in the analysis. Typical facets of MRA include (i) the dynamic concentration of biologic agents due to growth and death; (ii) the heterogeneous distribution of biologic agents on/in food and water media; (iii) the potential for secondary (e.g. person-to-person) transmission; and (iv) the role played by immunity [40]. MRA studies have been carried out on a relatively small number of food-borne pathogens; the extent to which the methods developed for food-borne diseases can be utilized in assessing homeland security risk remains undemonstrated. There are substantial uncertainties

regarding the use of animal models to inform human RAs; the viability and infectivity of pathogens in environmental media; and the use of potential sampling and detection methods for RA. To address these and related issues, the US DHS and the Environmental Protection Agency have recently founded the Center for Advancing MRA.

## 4 CRITICAL NEEDS

More is needed to assess the homeland security implications of the above discussion. Here, we consider three broad categories.

### 4.1 Data Needs

Robust, real-time surveillance systems capable of accurately and precisely estimating baseline values of human and veterinary disease incidence in both time and space are needed. In addition to looking "inward" at local, regional, and national disease activity, surveillance must look "outward" to identify the potential of threats being imported from distant regions. This requires up-to-date knowledge of disease transmission in foreign areas as well as data on the ecological conditions that might support the emergence and transmission of zoonoses. Analytic methods and effective concepts of operations to exploit early warnings of diseases effectively must be developed in conjunction with public health and homeland security stakeholders.

Mathematical modeling and RA methodologies require a range of data on different threat agents, such as distributions of latency and incubation periods; identification of the competent vectors of different agents in terms of temporal (e.g. seasonal) and spatial distributions; periods of disease, attack rates, and related epidemiological quantities, especially for exotic diseases; and dose-response functions. At present, such data are not often available. Both laboratory and field studies are needed. In the case of livestock diseases, up to date data on the location or probable location of livestock populations are needed, as are reliable data on livestock transportation between farms, feedlots, stockyards, and slaughter facilities.

### 4.2 Analytical Needs

While RA and mathematical modeling can both contribute to vulnerability analysis (e.g. identification of ecological areas, distribution nodes, or manufacturing systems that are particularly vulnerable to bioterrorism), only a small number of such analyses have appeared from the list of agents appearing in Tables 1–4. Analyses of the potential economic impact of these diseases must be elucidated. Only if such data are available that it will be possible to identify priorities and understand the need for vaccines and other public health prevention and control efforts. Comprehensive analyses involving more agents are needed; and it is vital that stakeholders and experts from all relevant technical fields participate.

Collaboration from related fields (e.g. ecology, microbiology, and psychology) is needed to resolve challenges facing mathematical epidemiologic modeling, including identifying methods to integrate data collected at different temporal and spatial scales into models; identifying of surrogates for data that do not exist; refining the multimodeling

approach (i.e. integration of models into larger models); and finding how best to communicate the results of models to decision makers, policy makers, planners, and public health operations personnel. Similarly, approaches to model validation must be developed for the rare and foreign diseases of highest interest, for which limited data is available.

### 4.3 Basic Science Needs

Questions regarding how a variety of zoonotic agents are maintained in natural populations; how they respond to changes in the environment; and what causes them to emerge and be transmitted remain unanswered. Lederberg and Shope [41] notes that "the precise ecological factors that lead to human infection . . . are murky, and textbook descriptions of the epidemiology of most zoonotic diseases are at best simplistic." In order to effectively counter threats from these diseases, we must understand the ecology of such agents better.

## 5 RESEARCH DIRECTIONS

In the short term, a central question is how to bring current and nascent capabilities to bear on public health preparedness so that effective interventions can be made in the event of a bioterror incident. Research into public health systems engineering should have a high priority. For example, how might current sensors be employed (e.g. in animal and food settings) in optimal spatial and temporal sampling strategies to detect threats at the earliest time possible? And given detection, what are the appropriate actions to initiate, given existing treatment and prophylactic options and logistic limitations on delivery and administration? It is unclear whether, for example, the BioWatch system has been designed according to such concerns, or whether surveillance systems that are under development aim to address such questions.

Such questions could be investigated with current analytic methods. A first step entails the refinement and validation of analytic tools. Mathematical approaches are, arguably, the only way to identify vulnerabilities, opportunities for prevention, and candidate control options in a systematic, unbiased way. However, models must be validated if they are to be credible. Validation is difficult for rare food-borne infections and zoonotic diseases that exist only in foreign nations. Prospective field studies in endemic areas must be undertaken in order to validate models of important threat agents.

In the longer term, effective vaccines, antibiotics, and antivirals must become available if we are to increase public health preparedness. Research to identify generalizable programmatic approaches to commercialization of new solutions would be of immense use. Research from the US Centers of Excellence, for example, must be transitioned and commercialized if new products are to become available at the clinical level. One way forward may be to focus on public—private partnerships for purposes of technology transfer and product transition. However, the economic disincentives facing pharmaceutical companies must be solved if these products are ever to be mass produced.

## ACKNOWLEDGMENTS

The author thanks Dr J. Glenn Morris and all the anonymous reviewers for suggestions strengthening this article.

## REFERENCES


1. Patrick, W. (2001). Biological warfare scenarios. In *Firepower in the Lab: Automation in the Fight Against Infectious Diseases and Bioterrorism*, S. P. Layne, T. J. Beugelsdijk, and C. K. N. Patel, Eds. Joseph Henry Press, Washington, DC, pp. 215–223.
2. Alibek, K. (1999). *Biohazard*, Random House, New York,
3. Inglesby, T. V., Dennis, D. T., Henderson, D. A., Bartlett, J. G., Ascher, M. S., Eitzen, E., Fine, A. D., Friedlander, A. M., Hauer, J., Koerner, J. F., Layton, M., McDade, J., Osterholm, M. T., O'Toole, T., Parker, G., Perl, T. M., Russell, P. K., Schoch-Spana, M., and Tonat, K. (2000). Plague as a biological weapon: medical and public health management. Working Group on Civilian Biodefense. *JAMA* **283**(17), 2281–2290.
4. Acha, P. N., and Szyfres, B. (2003). *Zoonoses and Communicable Diseases Common to Man and Animals*, *Bacterioses and Mycoses*, *Vol. I*, 3rd ed., Pan American Health Organization, Washington, DC.
5. Acha, P. N., and Szyfres, B. (2003). *Zoonoses and Communicable Diseases Common to Man and Animals*, *Chlamydioses, Rickettsioses, and Viroses, Vol. II*, 3rd ed., Pan American Health Organization, Washington, DC.
6. Acha, P. N., and Szyfres, B. (2003). *Zoonoses and Communicable Diseases Common to Man and Animals*, *Parasitoses, Vol. III*, 3rd ed., Pan American Health Organization, Washington, DC.
7. Lederberg, J., and Shope, R. E. (1992). *Emerging Infections: Microbial threats to Health in the United States*, National Academy Press, Washington, DC.
8. Smolinski, M. S., Hamburg, M. A., and Lederberg J., Eds. (2003). *Microbial Threats to Health: Emergence, Detection, and Response*, National Academies Press, Washington, DC.
9. US Code of Federal Regulations 7 CFR Part 331; 9 CFR Part 121; 42 CFR Part 73, http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm.
10. Inglesby, T. V., O'Toole, T., Henderson, D. A., Bartlett, J. G., Ascher, M. S., Eitzen, E., Friedlander, A. M., Gerberding, J., Hauer, J., Hughes, J., McDade, J., Osterholm, M. T., Parker, G., Perl, T. M., Russell, P. K., Tonat, K., Working Group on Civilian Biodefense. (2002). Anthrax as a biological weapon, 2002: updated recommendations for management. *JAMA* **287**(17), 2236–2252.
11. CDC, (2000). Update: outbreak of rift valley fever - Saudi Arabia, August–November 2000. *MMWR Morb. Mortal. Wkly. Rep.* **49**(43), 982–985.
12. Cartwright, F. F., and Biddiss, M. (2004). *Disease and History*, Gloucestershire, Phoenix Mill.
13. Kilpatrick, A. M., Kramer, L. D., Jones, M. J., Marra, P. P., and Daszak, P. (2006). West Nile virus epidemics in North America are driven by shifts in mosquito feeding behavior. *PLoS Biol.* **4**(4), e82, Epub 2006 Feb 28.
14. Borio, L., Inglesby, T., Peters, C. J., Schmaljohn, A. L., Hughes, J. M., Jahrling, P. B., Ksiazek, T., Johnson, K. M., Meyerhoff, A., O'Toole, T., Ascher, M. S., Bartlett, J., Breman, J. G., Eitzen, E. M. Jr., Hamburg, M., Hauer, J., Henderson, D. A., Johnson, R. T., Kwik, G., Layton, M., Lillibridge, S., Nabel, G. J., Osterholm, M. T., Perl, T. M., Russell, P., Tonat, K., Working Group on Civilian Biodefense. (2002). Hemorrhagic fever viruses as biological weapons: medical and public health management. *JAMA* **287**(18), 2391–2405.
15. Peters, C. J. (2002). The role of antivirals in responding to biological threats. In Knobler, S. L., Mahmoud, A. A. F. and Pray, L. A. Eds. *Biological Threats and Terrorism: Assessing the Science and Response Capabilities*, National Academy Press, Washington, DC.

16. Lemon, S., Thaul, S., Fisseha, S., and O'Maonaigh, H., Eds. (2002). *Protecting Our Forces: Improving Vaccine Acquisition and Availability in the U.S. Military*, National Academy Press, Washington, DC.
17. Chanteau, S., Ratsifasoamanana, L., Rasoamanana, B., Rahalison, L., Randriambelosoa, J., Roux, J., and Rabeson, D. (1998). Plague, a reemerging disease in Madagascar. *Emerg. Infect. Dis.* **4**(1), 101–104.
18. Keeling, M. J., and Gilligan, C. A. (2000). Metapopulation dynamics of bubonic plague. *Nature* **407**(6806), 903–906.
19. Wein, L. M., and Liu, Y. (2005). Analyzing a bioterror attack on the food supply: the case of botulinum toxin in milk. *Proc. Natl. Acad. Sci. U.S.A.* **102**(28), 9984–9989.
20. Merrell, D. S., Butler, S. M., Qadri, F., Dolganov, N. A., Alam, A., Cohen, M. B., Calderwood, S. B., Schoolnik, G. K., and Camilli, A. (2002). Host-induced epidemic spread of the cholera bacterium. *Nature* **417**(6889), 642–645.
21. Khan, A. S., Swerdlow, D. L., and Juranek, D. D. (2001). Precautions against biological and chemical terrorism directed at food and water supplies. *Public Health Rep.* **116**(1), 3–14.
22. Dennehy, P. H. (2001). Active immunization in the United States: developments over the past decade. *Clin. Microbiol. Rev.* **14**(4), 872–908.
23. Thacker, S. B., and Berkelman, R. L. (1992). History of public health surveillance. In *Public Health Surveillance*, W. Halperin, E. L. Baker, and R. R. Monson, Eds. Van Nostrand Reinhold, New York, pp. 1–15.
24. Chang, M., Glynn, M. K., Groseclose, S. L. (2003). Endemic, notifiable bioterrorism-related diseases United States, 1992–1999. *Emerg. Infect. Dis.* [serial online] 2003 May. Available from: URL: http://www.cdc.gov/ncidod/EID/vol9no5/02-0477.htm. Last accessed 6 November 2006.
25. Besser, J. M. (2006). Systems to detect microbial contamination of the food supply. In *Addressing Foodborne Threats to Health: Policies, Practices, and Global Coordination. IoM Board on Global Health*, National Academy Press, Washington, DC, p. 179.
26. Yih, W. K., Caldwell, B., Harmon, R., Kleinman, K., Lazarus, R., Nelson, A., Nordin, J., Rehm, B., Richter, B., Ritzwoller, D., Sherwood, E., and Platt, R. (2004). Centers for disease control and prevention (CDC). National bioterrorism syndromic surveillance demonstration program. *MMWR Morb. Mortal. Wkly. Rep.* **53**(Suppl.), 43–49.
27. Wilson, J. M., Polyak, M. G., Blake, J. W., Collmann, J. (2008). A heuristic indication and warning staging model for detection and assessment of biological events. *JAMA.* **15**(2), 158–171.
28. Lim, D. V., Simpson, J. M., Kearns, E. A., and Kramer, M. F. (2005). Current and developing technologies for monitoring agents of bioterrorism and biowarfare. *Clin. Microbiol. Rev.* **18**(4), 583–607.
29. Boltz, D. A., Douangngeun, B., Sinthasak, S., Phommachanh, P., Rolston, S., Chen, H., et al. (2005). H5N1 influenza viruses in Lao People's democratic republic. *Emerg. Infect. Dis.* **12**(10), 1593–1595.
30. Buckley, A., Dawson, A., and Gould, E. A. (2006). Detection of seroconversion to West Nile virus, Usutu virus and Sindbis virus in UK sentinel chickens. *Virol. J.* **3**, 71.
31. Rabinowitz, P., Gordon, Z., Chudnov, D., Wilcox, M., Odofin, L., Liu, A., and Dein, J. (2006). Animals as sentinels of bioterrorism agents. *Emerg. Infect. Dis.* **12**(4), 647–652.
32. Fienberg, S. E., and Shmueli, G. (2005). Statistical issues and challenges associated with rapid detection of bio-terrorist attacks. *Stat. Med.* **24**(4), 513–529.

33. Bravata, D. M., McDonald, K. M., Smith, W. M., Rydzak, C., et al. (2004). Systematic review: surveillance systems for early detection of bioterrorism-related diseases. *Ann. Intern. Med.* **140**(11), 910–922.

34. Lang, J., and Wood, S. C. (1999). Development of orphan vaccines: an industry perspective. *Emerg. Infect. Dis.* **5**(6), 749–756.

35. Hethcote, H. W. (2000). The mathematics of infectious diseases. *SIAM Rev.* **42**, 599–653.

36. McKenzie, F. E. (2000). Why model malaria? *Parasitol. Today* **16**, 511–516.

37. Gaff, H. D., Hartley, D. M., and Leahy, N. P. (2007). An epidemiological model of Rift Valley fever virus. *Elect. J. Diff. Equat.* **115**, 1–12.

38. Committee on Standards and Policies for Decontaminating Public Facilities Affected by Exposure to Harmful Biological Agents: How Clean is Safe? (2005). *Reopening Public Facilities after a Biological Attack: A Decision-Making Framework*, National Research Council, The National Academies Press, Washington, DC.

39. Pfeiffer, D., Pépin, M., Wooldridge, M., Schudel, A., Pensaert, M., Collins, D., Baldet, T., Davies, G., Kemp, A., Martin, V., Paweska, J., Swanepoel, R., and Thiongane, Y. (2005). The risk of a Rift Valley fever incursion and its persistence within the community. *EFSA J.* **238**, 1–128.

40. *Revised Framework for Microbial Risk Assessment: An ILSI Risk Science Institute Workshop Report*, International Life Sciences Institute, Washington, DC, 2000.

41. Lederberg, J. (2002). Summary and assessment. In *The Emergence of Zoonotic Diseases: Understanding the Impact on Animal and Human Health*, T. Burroughs, S. Knobler, and J. Lederberg, Eds. National Academy Press, Washington, DC, p. 115.

## FURTHER READING

Additional information on these approaches to infectious disease surveillance can be found at the International Society for Disease Surveillance Web site, http://www.syndromic.org/, 2008.

Projects under investigation at the DHS National Center of Excellence in Foreign Animal and Zoonotic Disease Defense (at Texas A&M University) are described at http://fazd.tamu.edu, 2008.

Projects under investigation at the DHS National Center of Excellence for Food Protection and Defense (at the University of Minnesota) are described at http://www.ncfpd.umn.edu/, 2008.

Information on the 10 National Institutes of Health Regional Centers of Excellence can be accessed via URL http://www3.niaid.nih.gov/research/resources/rce/, 2008.

Projects under investigation at the DHS-EPA Center for Advancing Microbial Risk Assessment (at Michigan State University) are described at http://camra.msu.edu/, 2008.

Banks, H. T., and Castillo-Chevez, C, Eds. (2003). Applications of a range of different mathematical modeling techniques are described. In *Bioterrorism*, SIAM, Philadelphia, PA.

General information on the ecology and clinical symptoms of many of these diseases can be accessed at the WHO site http://www.who.int/mediacentre/factsheets/en/, 2008.

Evans, A. S., and Brachman P. S., Eds. (1998). Detailed information on the ecology and clinical symptoms of many of these diseases appears. In *Bacterial Infections of Humans*, Plenum, New York.

Evans, A. S., and Kaslow, R. A. (1997). *Viral Infections of Humans*, Plenum, New York, Though a bit dated, these are encyclopedic references.

American Medical Association, American Nurses Association, American Nurses Foundation, Centers for Disease Control and Prevention, Center for Food Safety and Applied Nutrition, U.S. Food and Drug Administration, Food Safety and Inspection Service, U.S. Department of Agriculture. (2004). Diagnosis and management of foodborne illnesses: a primer for physicians and other health care professionals. *MMWR Recomm. Rep.* **53**(RR-4), 1–33.

# LIVESTOCK AGROTERRORISM AND THE POTENTIAL PUBLIC HEALTH RISK

WILLIAM D. HUESTON

*Center for Animal Health and Food Safety and National Center for Food Protection and Defense, University of Minnesota, St. Paul, Minnesota*

STEPHAN SINGLETON

*Center for Animal Health and Food Safety, University of Minnesota, St. Paul, Minnesota*

## 1 INTRODUCTION

"Agroterrorism" evokes images of sick and dying animals, forlorn farmers, and burning cow carcasses. The public health risks associated with agroterrorism are typically described as the spillover human illness associated with agroterrorism agents that are zoonoses (diseases shared by domestic animals or wildlife and humans), such as anthrax or cattle brucellosis, the human form of which is undulant fever. However, public health is more than simply the illness and death directly caused by infectious diseases. The World Health Organization (WHO) defines health as "a state of complete physical, mental, and social well being and not merely the absence of disease or infirmity" [1]. The potential public health risks of livestock agroterrorism must be evaluated in this broader context.

Agroterrorism is the intentional use of chemical, biological, radiological, nuclear, or explosive weapon or device against the nation's agricultural industries with the goal of generating fear, causing economic losses, and/or undermining social stability [2]. Livestock agriculture presents a comparatively easy target for intentional disease introduction. The widespread distribution of farms and ranches across the country, relatively easy access to fields and buildings, high density husbandry, concentrated feed production and distribution, livestock and poultry marketing and transportation channels, imperfect traceability of farm inputs and livestock, and inadequate biosecurity represent significant vulnerabilities. Consequently, the threat of agroterrorism is real and the potential public health consequences must be considered.

## 2 AGROTERRORISM DIFFERS FROM NATURAL DISASTERS

No nation has suffered a major agroterrorism incident in recent times and the refereed scientific literature is lacking in scientific studies of the public health implications of natural, accidental, or intentional animal health catastrophes. The impact of agroterrorism is informed by examining other types of catastrophic events such as natural disasters and government reports on major animal disease outbreaks and their control. Natural disasters and agroterrorism differ in a number of ways (Table 1).

**TABLE 1 Similarities and Differences of Natural Disasters and Agroterrorism (Adapted from Hall, 2003)**

| Dimension | Natural Disaster | Agroterrorism |
|---|---|---|
| Threat/risk | Local | Local or widespread |
| Knowledge of responders/physicians | High | Low |
| Knowledge of veterinarians | High | Moderate |
| Public health preparedness | Moderate | Low |
| Impact phase | Sudden | Variable |
| Duration | Acute | Variable |
| Hoaxes/copycats | No | Yes |
| Altered perception of safety | Local | Widespread |
| Potential for altered trust in officials | Moderate | High |

### 2.1 The Characteristics of Natural Disasters

Floods, fires, droughts, earthquakes, tornados, typhoons, hurricanes, volcanic eruptions, and tsunamis are natural disasters with which we all are familiar. Natural disasters have a known *beginning* and *end*, that is, hurricanes and tornados strike and then move on or floods and fires begin and then subside or are managed. The patterns of natural disaster have been widely studied, so that the geographic areas prone to these events can be mapped. Southern California is prone to wildfires and mud-slides, Florida and the Gulf Coast to hurricanes, and Bangladesh to typhoons. These natural disasters usually have a sudden impact on a circumscribed geographic area. Although potentially devastating for those involved, the public health risks are well characterized, with a whole emergency responder network and preparedness protocols in place. Even though the magnitude of the disaster may initially overwhelm responders, the mechanics of response are universally understood so that reinforcements can be solicited from other localities, states, and even countries. Natural disasters are so much a part of everyday life that the public response is a collective resolve to aid those affected and speed recovery, to get life "back to normal".

### 2.2 The Characteristics of Agroterrorism

Agroterrorism is not commonplace. Given the motivations of the perpetrators, the beginning and/or end of the event may never be known. Intentional acts can take place anywhere. The intent may be harm to animals, people, the economy, the public sense of security, or all of the above. The terrorist's target can be local, like an individual community or farm, or widespread, with multiple sites attacked across a wide geographic area. Not only can these events be devastating, but we are also largely unprepared for handling agroterrorism events because of the large number of uncertainties described above and because these events cut across multiple jurisdictional lines, including animal health, public health, and law enforcement. Traditional approaches to investigating a crime such as roping off an area and leaving it undisturbed to facilitate evidence collection may be exactly the wrong response to an infectious disease or chemical attack where rapid action including cleaning and disinfection may be critical to contain the potential damage. Unlike natural disasters, intentional acts are often followed by copycat actions including threats and hoaxes, which themselves have potential consequences in terms of mental health. Furthermore, the opportunity costs of responding to the livestock agroterrorism event,

copycat action, threat, or hoax may be significant, redirecting scarce public health dollars away from programs with a greater public health impact. Finally, intentional acts of agroterrorism have the potential to dramatically alter our collective perception of safety. The uncertainties surrounding the event likely will exceed the certainties, further altering the trust people have in the ability of government to respond effectively. While the danger of the event is real, the multiple uncertainties and the intentional nature of the event will stimulate a wide array of emotional reactions including anger, frustration, dread, and anxiety. In the language of risk communication, the public "outrage" will be huge.

## 3 AGROTERRORISM AND THE PUBLIC'S PERCEPTION OF RISKS

Given that terrorism by definition is an act intended to create "terror", the public's response to the agroterrorism event is critical. Risk communication experts know that our personal perception or interpretation of risk involves not only the available scientific data concerning the likelihood and consequences of something bad happening, but also our personal value system and the degree to which we feel that the risk is important, a subjective assessment variously called *dread* or *outrage*. Although scientists tend to focus on what is known about the likelihood and consequence of something going wrong, humans are influenced, often disproportionately, by their feelings.

A whole range of outrage factors have been catalogued [3]. Germane to this discussion of agroterrorism are factors such as the degree of personal control (uncontrollable risks are perceived to be more important), intentionality (intentional acts of terrorism stimulate more dread than a similar event caused by an accident), and the newness of the risk (new risks evoke more outrage). Acts of agroterrorism will ignite public outrage and foster elevated perceptions of risk.

## 4 THE IMPACTS OF AGROTERRORISM

The direct impacts of agroterrorism reach far beyond the animal health impacts (i.e. illness and death of affected animals). Affected producers bear some or all of the costs of treatment and response. The standard response to outbreaks caused by many of the agroterrorism agents such as foot-and-mouth disease (FMD) and highly pathogenic avian influenza (HPAI) is "stamping out", the systematic depopulation of affected herds and flocks. Although the government may offer indemnity for all unaffected animals destroyed and the costs of cleaning and disinfection, these represent only a fraction of the overall costs of the incident. No compensation is usually provided for dead and diseased animals or for the loss of anticipated income. Losing animals means a loss of investment and potential loss of valuable genetics in the case of purebred or breeding animals. Producers may also have a significant emotional attachment to the animals. Additional costs of recovery may include the forced "resting" of the facilities to assure the death of any remaining pathogens before they can be restocked (down time).

### 4.1 Impacts Extend Beyond the Producers Experiencing the Disease

The producers experiencing the disease are not the only ones affected. In cases of exotic disease introduction, those farms with potential exposure (epidemiologic links) and geographic proximity are quarantined and the herds and flocks are then often destroyed to

prevent spread. Movement of animals and animal products are restricted and additional health requirements may be put in place. These additional control efforts will increase the cost of production for livestock, reducing the producer's net income and adding to the logistical challenges of production, harvesting, and processing. Evaluating the public health risks must include those who are not experiencing the disease but whose livelihoods and sense of security also are affected.

### 4.2 International Implications for Trade

On the global scale, livestock agroterrorism can affect international trade. Introduction of a new livestock disease changes the disease status of a country as it can no longer claim disease freedom. A change in disease status of the country can cause major disruption in the export of animals and animal products. Trade issues are rarely quickly resolved. Once established, trade bans often take months to years to resolve such that reestablishment of historical levels of export is achieved.

Even the control strategy chosen to address the introduced disease can have trade implications. For example, a country that chooses to use vaccination as a strategy for dealing with FMD can only achieve a classification of "free with vaccination", which still has negative trade implications.

The economic impacts of trade disruptions can be huge. Agriculture remains one of only a handful of sectors in which the United States and many other nations maintain a positive trade balance, due, in part, to international trade in animals and animal products. The ripple effects of trade bans secondary to livestock agroterrorism may extend throughout the nation.

## 5 EVALUATING POTENTIAL PUBLIC HEALTH RISKS OF LIVESTOCK AGROTERRORISM

Based on current knowledge of natural disasters and natural or accidental animal disease outbreaks, livestock agroterrorism will have both direct and indirect impacts on public health. Victims can be described on many levels from those directly involved with the event to concerned and caring people outside of the affected area [4]. These risks include human illness and death from zoonoses, individual mental health impacts, and societal impacts including social well being and the secondary impacts of economic disruption on rural communities and the stability of agricultural industries.

### 5.1 Direct Public Health Impacts of Livestock Agroterrorism

The direct public health impacts of agroterrorism are those where the intentional act of terrorism itself, whether introduction of the chemical, biological, radiological, nuclear, or explosive agent, affects livestock and their producers. The direct public health impacts of livestock agroterrorism also extends to first responders including the animal health professionals and law enforcement agents who would visit the scene of the incident(s), handle the diseased animals, and investigate the criminal act. The direct public health impacts can also extend to others along the food chain, such as abbatoir workers who harvest the animals.

***5.1.1 Physical Health Impacts.*** The agent used by the terrorist can have direct impacts on farm workers and those present at the time of attack plus first responders. Five of the six Category A bioterrorist agents are zoonoses (i.e. diseases that affect both humans and domestic animals). Many zoonotic agents can serve as potential agents of agroterrorism. For example, natural exposure to Nipah virus has a high case mortality rate in humans working with affected pigs. Although Nipah has not been shown to transmit from human-to-human, this agent can be easily produced in large quantities in cell culture and does not have effective treatment. Other agents that could cause illness and death from zoonoses include tularemia, plague, brucellosis, and Q fever.

Some agroterrorism agents themselves can cause neurologic disease such as encephalitis. Neuropsychiatric syndromes or symptoms are associated with anthrax, brucellosis, Q fever, botulinum toxin, and viral encephalitides [5]. Neuropsychiatric sequellae also have been noted in people infected with Nipah virus [6].

***5.1.2 Mental Health Impacts.*** The mental health impacts of an agroterrorism attack likely will exceed the physical health impacts, perhaps by several orders of magnitude. Mental health issues may increase the case load and diagnostic challenges on healthcare providers as well as redirect resources that may be important for prevention and control actions related to the incident.

Disasters are stressful situations and individuals respond differently to these traumatic events. Increased depression is one of the psychological and psychiatric impacts of natural disasters that has been studied [7]. The stress of the agroterrorism event may be even greater due to the newness of the threat and its unique characteristics [4]. Man-made disasters, especially intentional ones like bioterrorism, cause more psychological and psychiatric problems than natural disasters. Since no country has modern experience dealing with a livestock agroterrorism event, it would generate unique stressors. Social isolation also may contribute to this stress as quarantines and movement restrictions may preclude normal community interactions, with some agricultural workers under virtual house arrest.

Most people suffering stress recover without any long-term psychiatric sequellae. Nevertheless, long-term psychiatric illness can also be expected, like depression, post-traumatic stress disorder, substance abuse, anxiety, and somatization, where psychological stress is expressed as physical problems [4].

## 5.2 Indirect Public Health Impacts of Livestock Agroterrorism

The indirect public health impacts of livestock bioterrorism include the secondary public health impacts precipitated by the illness and/or death of livestock and/or producers, the economic losses suffered by individuals and the community, and the societal disruption. Indirect public health impacts may also result as unintended consequences of the animal health, law enforcement, and public health response to the agroterrorism event [4].

***5.2.1 Indirect Physical Health Impacts.*** While humans are the dead end host for many zoonoses, others have significant potential to spread from human-to-human. These secondary cases could include healthcare workers and the extended family, neighbors, or community members who provide support for the affected farm workers and/or first responders. Theorists also speculate that sophisticated terrorists might genetically engineer an agroterrorism agent to enhance its potential to spread from human-to-human.

Fomites may play a role in secondary spread of zoonoses or other chemical or radiological agent. Contaminated equipment leaving the affected premise could expose others. Contaminated clothing of farm workers or first responders could expose other livestock populations or "foul the nest", taking the agent home to expose family members. Biological vectors such as insects may also play a role.

Although less likely in developed countries with robust food systems, an agroterrorism event could lead to significantly increased costs of protein from animal sources (meat, milk, poultry, and eggs). These cost increases may precipitate substitution of other protein sources or reduction in dietary protein altogether which can contribute to malnutrition. The 1983 HPAI outbreak in Pennsylvania, while not agroterrorism, caused an increase in poultry prices, costing consumers an additional $548 million in food expenditures [8].

***5.2.2 Indirect Mental Health Impacts.*** Disasters, regardless of their cause, evoke an outpouring of care and concern not only in the affected communities but also among those far removed from the event. Some people far distant from the event will experience the disaster vicariously with such intensity that it creates psychological health problems for them. Still others will develop mental health problems due to the ripple effects of the disaster on the agricultural community and economics.

In the case of agroterrorism, the first discussion topic is usually economics. The economic impacts not only have direct effects on the farmer's mental health but they also affect individuals and businesses along the entire food chain including input suppliers, food processors, transportation, retailer, and food service providers [2].

Producers who lose animals or suffer direct or indirect economic damage may in turn have less money to spend on healthcare and other related costs. In some cases producers never recover from the loss of their animals or income and may lose their livelihood and have to turn to other types of employment. The social disruptions secondary to agroterrorism events or large-scale animal disease outbreaks have not been documented.

The economic impacts of agroterrorism extend far beyond the farming community itself. Agriculture provides the primary employer and largest source of economic activity for many rural areas. Decreased agricultural revenue has a trickle down effect on goods and services. Local community businesses may suffer sufficiently to have to lay off employees, adding to unemployment. Tourism, too, can be affected if the response to the disease outbreak limits access to the area or negative publicity from the event discourages visits. The tax revenue generated by an agriculture-based economy fuels public services and community improvements. Economic instability also decreases local philanthropy, negatively affecting charities that pick up where government services stop. Taken together, the economic impacts of agroterrorism have the potential to adversely affect the public health infrastructure of rural communities.

An agroterrorism attack with widespread impact may disrupt the food system and/or cause an increase in food prices that may affect discretionary income and diets. For animal products that are often produced, processed, and consumed in a defined geographic area like dairy products and eggs, an agroterrorism attack may disrupt local supplies. Consumers confronting empty food shelves in the local grocery will have a heightened sense of the impact of the event, which in turn may lead to anxiety and other psychological manifestations.

More difficult to estimate are the psychological impacts that may follow from the increased sense of vulnerability of the food supply and the loss of trust that the food supply is safe. An agroterrorism event could seriously disturb the community's sense

of optimism. The event may shake public confidence with political ramifications for the party in power at the local, regional, or national level.

## 6 CRITICAL NEEDS ANALYSIS AND RESEARCH DIRECTIONS

Preparedness in the context of the public health impacts of agroterrorism is hampered by the paucity of scientific literature. Even studies of public health impact of natural or accidental livestock disease outbreaks are limited. An agroterrorist event would have a higher impact than an unintentional outbreak because a terrorist would make an attempt to create maximum damage. Recognition of this difference highlights the need for additional research exploring the adaptability and flexibility of public health to address these types of situations including provision of broad-scale psychological and psychiatric support in situations where the healthcare providers themselves are also experiencing unprecedented collective stress due to the intentional nature of the event and its impact on the core need we humans have for food [9]. Furthermore, given the global nature of our food supply, consideration must be broadly given to addressing the needs of consumers as well as the affected producers and their communities. Methods for effective risk communication and the use of transdisciplinary approaches need to be explored.

## REFERENCES

1. Awofeso, N. (2005). Re-defining 'Health' Article. *Üstün Jakob.* **83**, 802.
2. Monke, J. (2006). *Library of Congress, Congressional Research Service. Agroterrorism: Threats and preparedness*. Congressional Research Service, Library of Congress, Washington, DC, http://www.policyarchive.org/bitstream/handle/10207/2168/RL32521_20070122.pdf.
3. Covello, V., and Sandman, P. (2001). *Risk Communication: Evolution and Revolution. Solutions to an Environment in Peril*. John Hopkins University Press, Baltimore, MD, pp. 164–178.
4. Kron, S., and Mendlovic, S. (2002). Mental health consequences of bioterrorism. *Isr. Med. Assoc. J.* **4**(7), 524–527.
5. Benedek, D. M., Holloway, H. C., and Becker, S. M. (2002). Emergency mental health management in bioterrorism events. *Emerg. Med. Clin. North. Am.* **20**(2), 393–407.
6. Ng, B. Y., Lim, C. C., Yeoh, A., and Lee, W. L. (2004). Neuropsychiatric sequelae of nipah virus encephalitis. *J. Neuropsych. Clin. Neurosci.* **16**(4), 500–504.
7. Ginexi, E. M., Weihs, K., Simmens, S. J., and Hoyt, D. R. (2000). Natural disaster and depression: a prospective investigation of reactions to the 1993 midwest floods. *Am. J. Commun. Psychol.* **28**(4), 495–518.
8. Ashlock M. A., Leising J. G., Cartmell D. D. (2007). *Agroterrorism: Implications for Effective Crisis Management in Agricultural Communications*. http://aee.cas.psu.edu/NAERC/sessions/SessionD/AgroterrorismPaperAshlockLeisingCartmell.pdf. Accessed 2007, October 15.
9. Hall, M. J., Norwood, A. E., Ursano, R. J., and Fullerton, C. S. (2003). The psychological impacts of bioterrorism. Biosecurity and bioterrorism: biodefense strategy. *Pract. Sci.* **1**(2), 139–144.

## FURTHER READING

Bender, J. B., Hueston, W., and Osterholm, M. (2006). Recent animal disease outbreaks and their impact on human populations. *J. Agromed.* **11**(1), 5–15.

Casagrande, R. (2000). Biological terrorism targeted at agriculture: the threat to US national security. *Nonproliferat. Rev.* **7**, 98–99.

Chalk, P. (2004). *Hitting America's Soft Underbelly: The Potential Threat of Deliberate Biological Attacks Against the US Agricultural and Food Industry*. Rand Corporation, Santa Monica, CA.

Pearson, G. S. (2006). Public perception and risk communication in regard to bioterrorism against animals and plants. *Rev. Sci. Tech.* **25**(1), 71–82.

Seebeck, L. (2007). Responding to systemic crisis: the case of agroterrorism. *Stud. Conf. Terrorism* **30**(8), 691–721.

# THE ROLE OF FOOD SAFETY IN FOOD SECURITY

JUSTIN J. KASTNER, ABBEY L. NUTSCH, AND CURTIS L. KASTNER
*Kansas State University, Manhattan, Kansas*

## 1 INTRODUCTION

Today's agricultural security and food safety and security discussions are, admittedly, burdened by confusion of terminology. Therefore, this article necessarily begins by addressing the terms "security" and "defense" in the context of the agricultural and food industry. Some definitions that have been used by food regulators include the following:

- *Food security.* Activities associated with ensuring the adequacy of the food supply.
- *Food defense.* Activities associated with protecting food from intentional contamination.

The term "food security" has been contested in recent years. In the post-9/11 era, new understandings of security have influenced the interpretation of both "homeland security" and "food security" [1, 2]. Indeed, the adoption, by such regulatory agencies as the US Food and Drug Administration, of the term "food defense" stems from confusion surrounding the term "food security" [3].

While some contend that "food security" ought to be strictly the domain of international-aid and economic-development policy communities, others have used the term "food security" to encompass international food defense issues as well as unintentional incidents that impact the adequacy of the food supply. Rather than letting semantics unduly complicate more important issues, leaders should support—or, at least, tolerate—the use of either "food security" or "food defense" in discussions devoted to

how to protect the food supply and ensure food safety as well as food-supply sufficiency. Quite simply, knowledge of and practices regarding food safety are applicable regardless of one's understanding of food security or food defense. The purpose of this article is not to debate the correct terminology but to show how food safety knowledge serves the broad objectives of food security/defense. Whether or not a food industry professional is concerned about bioterrorism, quality assurance, sanitation, physical site security, border security, supply chain management, or international trade, he/she will find that food safety capabilities and strategies are almost, if not always, applicable.

The historical development of preventive, process-oriented food control systems notably includes the Hazard Analysis and Critical Control Point (HACCP) system; in the next section, the advent of HACCP and its application to food safety/defense is discussed. In order to paint a picture of the relevance of food safety principles, practices, and research to food security/defense, a situation- and commodity-specific example is offered in the next section. Finally, food safety education and its application to food security/defense is highlighted.

## 2 FOOD SAFETY PREVENTION, HACCP, AND FOOD SECURITY/DEFENSE

Food safety and control systems have developed in concert with better understanding of foodborne hazards [4]. Prior to the mid-nineteenth century, for example, a lack of epidemiological knowledge about microbiological pathogens left public health officials wondering what was the cause of diseases, including those brought on by the ingestion of particular foods. However, during the second half of the nineteenth century—and, indeed, up to the mid-twentieth century—particular foodborne illness cases were tied to particular agents (e.g. between 1850 and 1880, trichinosis and other diseases' link to parasites was confirmed; between 1880 and 1950, specific bacterial diseases were tied to specific meat-borne pathogens). Between 1950 and 1985, food safety researchers continued to identify new microbiological (and chemical) hazards in food, and they became intrigued with the idea of intervening in food processing to *reduce* the likelihood (i.e. risk) of such hazards occurring [4].

By the mid-1980s, more deliberate process-oriented (as opposed to merely inspection-oriented) systems came into being [4]. One program—HACCP—had been developed previously to ensure food safety in the US Space Program; during the 1980s and 1990s, food companies and federal regulators began to insist on the seven principles of HACCP as a way to systematically control hazards (whether biological, chemical, or physical) in the food supply. The principles include the following:

1. Conduct a hazard analysis (identification of biological, chemical, and physical hazards that may cause food to be unsafe).
2. Identify critical control points, that is, steps or procedures in which a hazard can be prevented, eliminated, or reduced.
3. Establish critical limits for each critical control point (e.g. specific temperature or processing parameters that ensure reduction of risk to an acceptable level).
4. Establish critical control point monitoring requirements.
5. Establish corrective actions in the event monitoring to indicate a violation of a critical limit.

6. Establish record keeping systems.
7. Establish validation procedures to demonstrate the HACCP system is in fact working.

HACCP is notably different from inspection-oriented food safety systems. HACCP's introduction into the food industry has helped foster a prevention-oriented mindset amongst food professionals. Prevention-oriented food safety systems like HACCP are an invaluable asset in larger food security/defense efforts. Food safety systems can, in a sense, provide a kind of proverbial "downpayment" on ensuring that a food plant is culturally open to systematically considering, reducing, monitoring, and documenting risks of all kinds.

## 3 CARVER + SHOCK AND THE EXAMPLE OF THE KANSAS MEAT INDUSTRY

Examples are illustrative of wider concepts, and this section considers how food safety efforts can help address food-security vulnerability concerns. In 2006, Kansas State University (K-State) conducted a vulnerability assessment of the meat processing industry in Kansas. The assessment revealed several instances in which food safety focused initiatives could be adapted to address food security/defense issues. Similarly, the assessment underscored how university-based food safety research could contribute to larger objectives of food security and food defense. This section explains the relevance of food safety efforts—including research efforts to broader activities designed to ensure a more secure food supply.

CARVER + Shock is one of several tools and resources available through the US Food and Drug Administration [5]. CARVER is an acronym for six factors used to evaluate the attractiveness of a target for attack: Criticality (assesses the public health and economic impacts), Accessibility (the ability to physically access and egress from a target), Recuperability (ability of a system to recover from an attack), Vulnerability (ability to accomplish a successful attack), Effect (amount of direct loss from an attack as measures by loss of production), and Recognizability (ease of identifying a target). "Shock" assesses the combined health, economic, and psychological impacts of an attack within the food industry.

Food safety systems (including HACCP) and food safety educational efforts (discussed at the end of this article) minimize food safety hazards and help provide an initial obstacle to achieving any significant consequences through intentional contamination. With regard to Criticality, the size of the meat processing industry in Kansas is consistently ranked among the top 3 in the nation. Indeed, the processing plants operated in Kansas by the world's largest processors account for the bulk of that ranking; however, medium, small, and very small processors also contribute significantly to the high national ranking. Regardless of the relative contributions (i.e. whether production stems from large or small plants), Kansas is a major contributor to the totality of the United States and global meat industry. What happens in Kansas—whether in a large or small plant—impacts not only the state but also the entire domestic and international meat industry. Therefore, the safety of meat products processed in Kansas has far reaching implications that can impact both public health and economic stability. Regarding the safety and security of the meat supply, the US meat industry recognizes that all of its members could be "painted with the

same brush" if meat safety were compromised. When considering meat processing along with allied livestock production, the total system is the number one revenue generator in Kansas. The value of livestock, poultry, and their products in 2002 was $6.3 billion in Kansas alone [6].

The second element of CARVER + Shock—namely, Accessibility—also falls within the domain of traditional food safety efforts. Food safety officials are concerned about hazards and how they might be introduced into a food production system. The concept of food defense more purposefully addresses the issue of intentional actors who might introduce a hazard into the food supply. Terrorism, whether instigated by a transnational terrorist organization, a disgruntled employee, or a hired perpetrator, can result in similarly chaotic, catastrophic consequences for the food industry. Classically motivated terrorists prefer to destroy life as well as economic stability with an emphasis on taking as many lives as possible. Though the emphasis on protecting public health is a primary concern, an attack on the economy alone could, indeed, be devastating in and of itself.

Because of the meat processing protocols being similar for beef, pork, lamb, and poultry, the following scenario was viewed as generically applicable to all species in the Kansas meat industry. Animals are normally held and rested for a period of time at the slaughter facility before being processed. A hazard could be introduced at that point and carried into processing. An externally administered hazard would be removed or at least diluted during dehiding, dehairing, pelting, or defeathering. Internalized hazards would be largely removed during evisceration. Therefore, to have the greatest impact, introduction of these later in processing was assessed as being more likely.

Intact carcasses would be the next opportunity for cross contamination during slaughter or initial intentional contamination. However, this would primarily be limited to the surface of the carcass and subsequent food safety interventions (e.g. trimming, washing, and decontamination) would reduce or eliminate the hazard.

It is the further processing of lean trim and particularly in comminuted systems (i.e. ground beef and wieners) that offers the greatest opportunity for introducing a hazard that would be uniformly incorporated into a large quantity of meat. Formulation ingredients (i.e. water and spices) would also widely distribute a hazard if contaminated. Further processing operations are readily accessible to workers and introduction of a hazard during mixing and blending would be relatively easy and effective. Smaller, isolated-yet-devastating episodes could be perpetrated at, for example, retail stores where grinding and mixing occurs [7].

With regard to the issue of Recuperability, food safety systems and food safety education place an emphasis on how to institute "corrective measures" in the event of a food safety violation. Traceability, mediated through attention-to-detail management and appropriate lot and date coding, would allow for product recall while the product is in storage or transit. All companies should have this capability to address food safety issues. However, if the hazard persisted undetected for a period of time, much of the product would be consumed prior to the recall. Even though it may not always be possible, consumers could use coding information to avoid consumption. Directions for disposal would also be required. Effective, appropriately crafted communications would be imperative to ensure an orderly and effective response.

With regard to Vulnerability, those studying the Kansas meat industry concluded that a hazard introduction, while feasible, was likely to be less attractive than other segments of the food industry. (Indeed, if a widespread impact on public health was the terrorists' goal, the beverage industry would be a better choice and terrorists have indicated their

awareness of that.) Nevertheless, the impact of the livestock and meat industry on the economy could be dramatic. In fact, it was proposed that the following scenario would be feasible and have an impact on the economy. A hazard that both (a) has notable "shock value" and (b) is considered an adulterant (i.e. *Escherichia coli* O157:H7) in ground beef would, in the eyes of a terrorist, be a hazard of choice. The vulnerability assessors assumed that *E. coli* O157:H7 was evenly mixed by terrorists into a defined lot of ground beef. Finished packages of that ground beef containing the lot identification would be taken by the terrorist(s). One week from that time a sample package would be submitted to the authorities. The product lot that is now on the retail shelves would then be verified as containing the hazard. Even though the hazard is diluted, and possibly of little or no public health consequence, consumer confidence in the US meat supply could be dramatically impacted. Indeed, the mere presence of *E. coli* O157:H7, regardless of the concentration, would initiate a recall of *all the product* in that lot and would impact the *consumer demand for beef in general*. The infective dose of *E. coli* O157:H7 is very low, and if the product was not cooked properly, it could cause foodborne illness. This scenario has been chronicled by the US Department of Homeland Security [8].

Additionally, terrorists might *falsely claim* that they had randomly contaminated more than the one lot and product type; under such a scenario, the economic impacts would be even further widespread. Large-scale meat recalls experienced by the US meat industry further illustrate the costs of such a scenario.

In such scenarios, traditional food safety programs devoted to microbiological pathogens will be critical to minimizing vulnerability.

Focusing on Effect, the vulnerability assessors discovered that if a meat product (processed by even a small meat processor in Kansas) could be verified as contaminated and is in the distribution chain, the effects would be dramatic. Even in the absence of a public health impact, the economic effects could be devastating. Here, food safety risk communication would be especially relevant.

The vulnerability assessment did not address Recognizability in the sense of CARVER + Shock; officially, Recognizability relates to whether or not a perpetrator can identify the point for contamination. In addition, but in a different and sense of "recognizability," the vulnerability assessors concluded that those interested in intentionally contaminating the food supply recognize the economic as well as potential public health impact. An in-line, real-time surveillance/detection device that could sense any level of any abnormal ingredient (i.e. the hazard) would be an ideal counter measure. Even though that does not currently exist, progress is being made in development of this capability. Prevention is preferred, but imperfectly effective in the real world.

Therefore, a short-term strategy would be to train the work force to be aware of physical site security vulnerabilities, unusual behavior of co-workers, and security around processing areas of highest risk (e.g. mixing and blending operations). The assessors concluded that awareness, though not the ultimate answer for prevention, could help achieve that goal. To assist in this effort, a series of food safety and security modules on a variety of topics such as physical site security, threat recognition, response, and so on were made available in 2006 for Internet delivery from Kansas State University's Division of Continuing Education.

At this point, education to heighten awareness to recognize potential threats is an excellent first step. Dr. David Franz, an internationally recognized expert on bioterrorism,

noted that education was the number one strategy based on effectiveness, including cost effectiveness [9].

With regard to the final element (Shock), the vulnerability assessors noted that an attack on the food supply could wreak economic, public health, and sociological havoc. The economy that the United States presently enjoys is implicitly reliant on a plentiful, affordable food supply. The magnitude of US discretionary spending is a result of an inexpensive food supply. Disruption of that food supply and its affordability would result in a chaotic situation that would rival any parallel loss of life [10]. For such sectors as the Kansas meat industry, responsive food safety systems could, potentially, help minimize economic, public health, and mental health consequences.

### 3.1 Food Safety Research and Food Defense

Local-area, university-based food safety research can help meet food defense/security concerns identified in the above CARVER + Shock vulnerability assessment.

Shortly after the *E. coli* O157:H7 outbreak in the Northwest United States in 1993, K-State researchers set to work with an engineering firm and a major meat processor to help prevent such future safety outbreaks. In response to this food safety issue, steam pasteurization of beef carcasses was developed, validated, and widely employed in the meat processing industry for food safety purposes. Though directed at an incidental food safety event, the strategy of steam pasteurization of carcasses would also eliminate intentionally added hazards if they were susceptible to steam pasteurization. Assuming that an added hazard was eliminated by steam pasteurization, added hazards up to carcasses fabrication would be eliminated. Stated alternatively, a food safety solution developed by K-State researchers could help address food security/defense issues. To be sure, the opportunity exists for incidental as well as intentional contamination beyond other intervention strategies; in these cases, steam pasteurization of meat trimmings before grinding could prove valuable.

By "hardening" (through the steam pasteurization of all beef carcasses and beef trim) a target, both food safety and food security/defense could be improved. This is but one example in which research to address food safety has come to address food security/defense concerns. Significantly, resources and practices serve a dual purpose and will make the food supply safer even if a terroristic event never occurs.

K-State is but one of many universities across the United States where food safety programs are being used to address food security/defense issues. K-State is part of the Food Safety Consortium, a program that has been funded by the US Department of Agriculture since 1988 to address the safety of beef and beef products (at K-State), pork (at Iowa State University), and poultry (at the University of Arkansas). While the original Congressional mandate to the Consortium was to develop and validate methods and technologies to isolate, identify, and eliminate microbial and chemical hazards, those important areas have been enhanced through the addition of new research programs regarding the food safety challenges associated with food security/defense. Meanwhile, a joint K-State-New Mexico State University *Frontier* program for the historical studies of border security, food security, and trade policy (http://frontier.k-state.edu) seeks to inject interdisciplinary and social-science perspectives into traditional food safety and food security research.

The National Center for Food Protection and Defense, based at the University of Minnesota, provides leadership in the overall food defense research and educational effort in the United States.

## 4 FOOD SAFETY EDUCATION IN FOOD SECURITY/DEFENSE

Traditional food safety related courses, such as food microbiology, food chemistry, epidemiology, toxicology, and so on are integral to food security/defense strategies and are part of most food science—related curricula. Food security/defense curricula can be easily augmented with these existing courses. Examples of this augmentation include a Food Safety and Defense Masters Certificate offered by K-State, the University of Nebraska at Lincoln, Iowa State University, and the University of Missouri. A similar initiative with Purdue University and the University of Indiana will lead to a graduate curriculum in Food Safety and Defense. These initial initiatives are being replicated and integrated with the educational efforts of the Department of Homeland Security Centers such as the University of Minnesota based National Center for Food Protection and Defense.

## REFERENCES

1. Beresford, A. D. (2004). Homeland security as an American ideology: implications for U.S. policy and action. *J. Homeland Secur. Emerg. Manag*. **1**(3), 301.
2. Kastner, J. and Ackleson, J. (2006). Chapter 6: global trade and food security: perspectives for the twenty-first century. In *Homeland Security: Protecting America's Targets*, J. J. F. Forest, Ed. Praeger Security International, Westport, CT and London, pp. 98–116.
3. FDA (2006). *Food Defense Awareness: FDA Satellite Broadcast*.
4. Koolmees, P. (2000). Chapter 4: Veterinary inspection and food hygiene in the twentieth century. In *Food, Science, Policy and Regulation in the Twentieth Century*, F. S. David and J. Phillips, Eds. Routledge, New York, pp. 53–68.
5. U.S. Food and Drug Administration (2007). *Food Defense and Terrorism*, 10 December [cited 28 January 2008]. Available from: http://www.cfsan.fda.gov/~dms/defterr.html
6. United States Department of Agriculture (2002). *Kansas State and Country Data*, Vol. **1**. *Geographic Area Series Part 15*, National Agricultural Statistic Service.
7. Hui, Y. H., Hip, W.-K., Rogers, R. W., and Young, A., Eds. *Meat Science and Applications*, Marcel Dekker, Inc., New York, 2001.
8. U.S. Department of Homeland Security Risk Management Division Office of Infrastructure Protection (2005). *Characteristics and Common Vulnerabilities, Infrastructure Category, Beef Processing*.
9. Franz, D. (2006). A multidisciplinary overview of food safety and security. *Biological Security: An International Perspective* (presentation of 18 May 2006, Kansas State University).
10. Jaax, J. (2006) A multidisciplinary overview of food safety and security. *The Agricultural Bioterrorism Threat* (presentation of 16 May 2006, Kansas State University).

## FURTHER READING

Frazier, T. W. and Richardson, D. C., Eds. (1999). *Food and Agricultural Security: Guarding Against Natural Threats and Terrorist Attacks Affecting Health, National Food Supplies, and Agricultural Economies*, New York Academy of Sciences, New York.

# CARVER + SHOCK: FOOD DEFENSE SOFTWARE DECISION SUPPORT TOOL

PHILLIP POHL, ERIC LINDGREN, CECELIA WILLIAMS, JEFFREY DANNEELS, ROBERT BROWITT, LEE EUBANKS, MADISON LINK, AND REGINA HUNTER

*Sandia National Laboratories, Albuquerque, New Mexico*

DON KAUTTER, JON WOODY, AND CORY BRYANT

*Food and Drug Administration, Silver Spring, Maryland*

## 1 CARVER BACKGROUND

The US Food and Drug Administration (FDA) is tasked with protecting the nation's food supply [1]. The acronym CARVER represents the steps in a threat analysis exercise: Criticality, Accessibility, Recognizability, Vulnerability, Effect, and Recuperability. The CARVER+Shock methodology was employed by the FDA and the US Department of Agriculture (USDA) to assist in defending food production systems from malevolent acts. Shock is added to incorporate the intangible focus of a terrorist in frightening a targeted group. The method was recently incorporated into stand-alone software by Sandia National Laboratories, which is user-friendly and is designed to remove the biases that can occur by group execution of the CARVER+Shock methodology. The algorithms that give rise to scores for two of these properties are described below, followed by a case study. The group execution of the CARVER+Shock methodology, a part of the Strategic Partnership Program Agroterrorism (SPPA), typically takes 2 to 3 days work by 15 to 30 experts [2].

Use of the software does not require expertise in risk assessment, chemical processing, or computer science. Rather, the goal of the software is to allow food production personnel to execute the CARVER+Shock method in a few hours. With the software, a user can modify production design specifications as needed and can evaluate various options as a function of security.

## 2 ALGORITHMS

A CARVER+Shock user session starts by gathering information about the process, facility security, and safety of the product being dealt with. The three steps in the session are building a process flow diagram, answering questions regarding the process nodes, and evaluating the results. The major challenge in designing the software is to ensure that the questions, subsequent answers, and reported scores adequately reflect the results of the SPPAs, of which over 20 have been done to date. To do this, algorithms were developed to depict the information flow from the user answers to preliminary calculated variables,

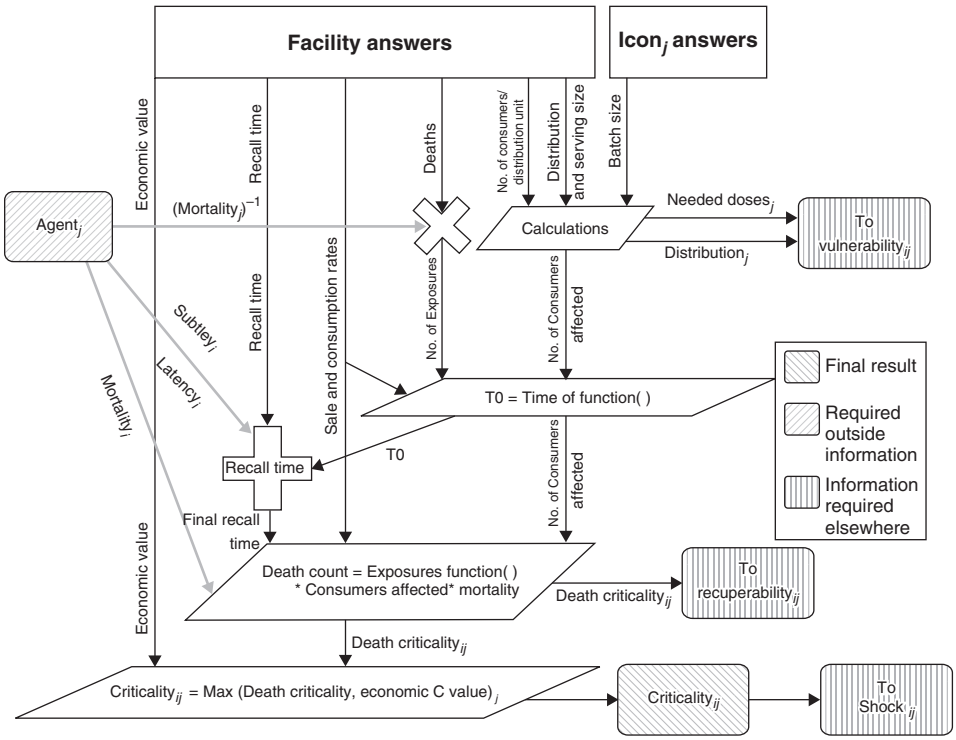



**FIGURE 1** Algorithm for criticality.

and finally to a score for each node in a process flow diagram. Figures 1 and 2 show the algorithms for Criticality and Accessibility. The complexity of each gives the reader an idea of how many questions may be required to determine the score for each property. Note that scores from one property may be used in other scoring algorithms.

## 3 TEST PROCESSES

These case studies consider two idealized processes: apple packing and yogurt production. Apple packing was chosen because of its simplicity and lack of food processing steps or ingredient additions. Yogurt production was chosen because it includes steps for simple food processing and ingredient addition. Each process is examined on three levels, a small scale representing a local provider, a medium scale representing a regional provider, and a large scale representing a national provider. The batch size for each increment of scale increases by a factor of 10. Each process was also examined under the assumptions of best case and worst case security practices. The CARVER+Shock score was calculated using CARVER+Shock Version 1.0.

The process flow diagram for apple packing is shown in Figure 3. The process is very simple, with no added ingredients. The fruit is sorted for size and quality, packed, and placed in storage until delivery to the retailer. The local supplier is assumed to have no refrigerated storage; therefore, packed apples are moved directly to the truck for delivery.

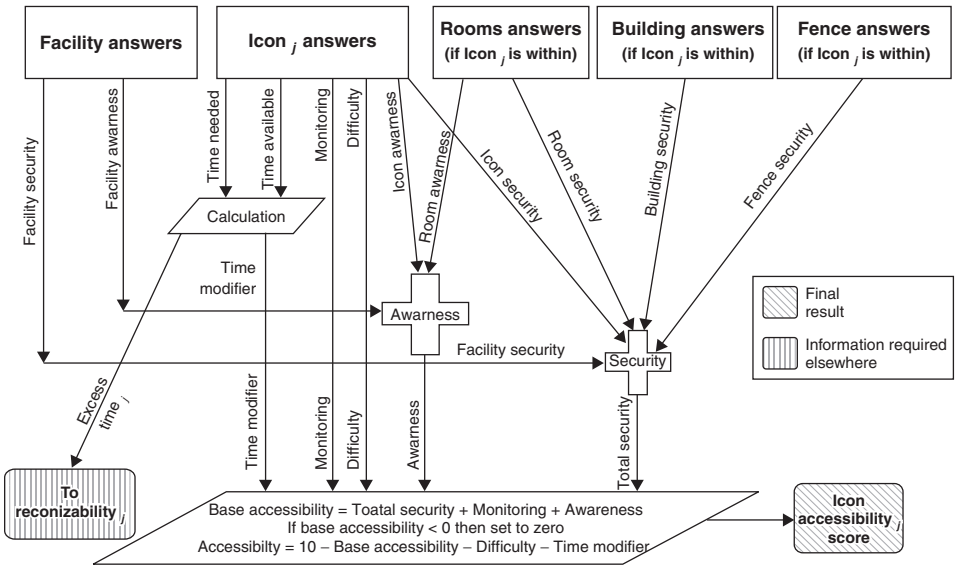



**FIGURE 2** Algorithm for accessibility.

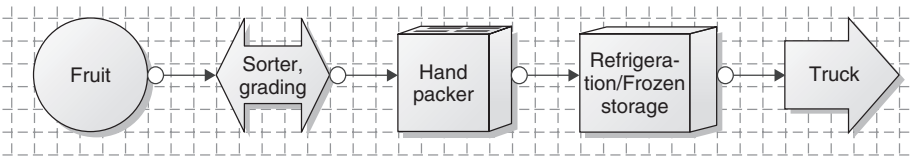



**FIGURE 3** Apple packing process.

Contamination would not easily taint an entire batch of apples; so, it is assumed that a contamination attempt would affect only 1 to 10% of the batch.

The process flow diagram for simplified yogurt production is shown in Figure 4. Raw milk is filtered, chilled, and then pasteurized, which raises the temperature to 85°C for 30 min. This heat treatment is much more severe than regular milk pasteurization. The pasteurized milk is cooled and transferred to the culturing tank, where the yogurt culture is added, and the mixture is held at 43°C for three to four h. The yogurt is packaged directly from the culturing tank with the fruit being added directly to the containers at the time of packaging. The packaged yogurt is placed in refrigerated storage before distribution. Since yogurt is a fluid product, it is assumed that a contamination event prior to packaging would be uniformly distributed in the entire batch. A contamination event after packaging is assumed to affect only 1 to 10% of the batch based on the educated guess of the CARVER+Shock user.

### 3.1 Production Scale Attributes

Both apple packing and yogurt production were analyzed at three levels of production. Table 1 summarizes the general attributes of each production level. The smallest level

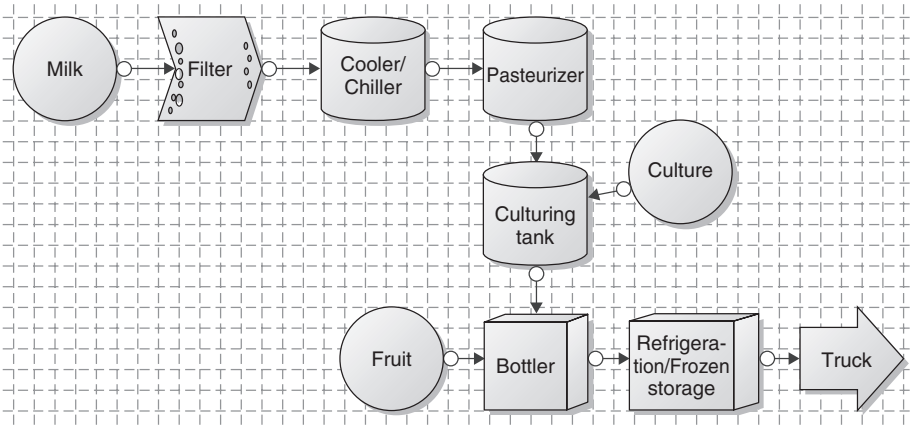



**FIGURE 4** Yogurt production process.

**TABLE 1 Production Attributes of the Three Production Scales Considered**

| | | Production Scale | | |
|---|---|---|---|---|
| Production Attribute | | Local | Regional | National |
| No. of cities supplied | | 1 | 4 | 15 |
| No. of outlets/batches | | 2 | 10 | 50 |
| Market share | | <1% | 1–9% | 10–25% |
| Name recognition | | No | No | Yes |
| Percentage of production loss | | >75% | >75% | 15–24% |
| Batch size: | Apples (lb) | 500 | 5000 | 50,000 |
| | Yogurt (fluid oz.) | 1280 | 12,800 | 128,000 |

represents a local producer who sells to one or two stores in a single locale. This producer operates a single small production line and has negligible market share and name recognition. The local producer's batch size is assumed to be 500 lb of apples or 1280 fluid oz. (10 gal) of yogurt. The medium level represents a regional producer who sells to a few stores in four regionally located cities. This producer operates a single, large production line and has established a small market share, but has little name recognition. The regional producer's batch size is 5000 lb of apples or 12,800 fluid oz. (100 gal) of yogurt. The large-scale operation distributes to many cities nationally. This producer operates multiple, large production lines and has established name recognition and an appreciable market share. The batch size for a single production line is 50,000 lb of apples or 128,000 fluid oz. (1000 gal) of yogurt.

### 3.2 Contamination Agents

The properties of the five toxic agents considered in each scenario are summarized in Table 2. All agents, except Agent 1, survive the heat treatment conditions of the

**TABLE 2 Summary of Toxic Agent Properties**

| Toxic Agents | Maximum Temperature (°C) | Solubility | Relative Toxicity |
|---|---|---|---|
| Agent 1 | 80 | Water | High |
| Agent 2 | 100 | Water and Oil | Medium |
| Agent 3 | 100 | Oil | High |
| Agent 4 | All temperatures | Water | Low |
| Agent 5 | All temperatures | Water | Very high |

pasteurizer (85°C for 30 min). The relative toxicity provides a measure of the quantity of the agent required for acute poisoning. In particular, the relatively low toxicity of Agent 4 limits the batch size that can reasonably be contaminated.

### 3.3 Security Practice Scenarios

All of the production scenarios were analyzed for "best" and "worst" security practices. Table 3 summarizes the essence of the two security scenarios. The best security practice scenarios included security personnel and perimeter fences, although the sophistication of the security at the perimeter increased with the size of the operation (local producers had a basic 6-ft fence; regional producers included perimeter lighting; and national producers included security patrols). In the worst security practice scenarios neither perimeter fences nor security personnel were included. The best-case security practice included operation plans—such as plans for food defense, continuity of operation, product recall, and health department coordination plans—along with employee training and practice drills. They also had tight control on shipping and receiving. The best-case practice did not publish any information about the production process or plant location on the internet and did not allow visitors on site.

### 3.4 Production Scale and Security Practice Results

The results of the CARVER+Shock analyses for apple packing and yogurt production are shown in Figures 5 and 6, respectively. These plots show the maximum CARVER+Shock score as a function of batch size for the best and worst security practices. The maximum CARVER+Shock score is taken as the greatest CARVER+Shock score of all the process icons used and all the agents considered.

As expected, for both apple packing and yogurt production, the CARVER scores for the worst security practices are significantly higher than for the best security practices. The best security practices CARVER scores were all below 50, which is generally considered acceptable; however, the results indicate there is possible benefit with improved security practices. The benefit gained by improved security for the yogurt operation (18 points) was greater than the benefit gained for apple packing (13 points). The difference in the improvement may be attributed to the difference in the nature of contamination spreading in apples (15 to 10%) versus yogurt (100%). For both apple packing and yogurt production, the CARVER+Shock score increased with the scale of the production. This

**TABLE 3 Operation Summary of the Best-Case and Worst-Case Security Practice Scenarios**

| | Security Practice | |
|---|---|---|
| Operation Attribute | Best Case | Worst Case |
| Perimeter fence | Yes | No |
| Security personnel | Yes | No |
| Plans (defense, continuity of operation, product recall, health department) | Yes | No |
| Training/drills (security, defense, recall) | Yes | No |
| Product traceability | Good | Poor |
| Customer support line | Yes | No |
| Background and drug use checks | Yes | No |
| Uniforms required | Yes | No |
| Internet information published | No | Yes |
| Visitors allowed | No | Yes |
| Shipping schedule enforced | Yes | No |
| GPS tracking of shipments | Yes | No |
| Tamper resistant seals used | Yes | No |
| Driver ID required | Yes | No |
| Acceptance testing performed | Yes | No |

GPS, global positioning system.

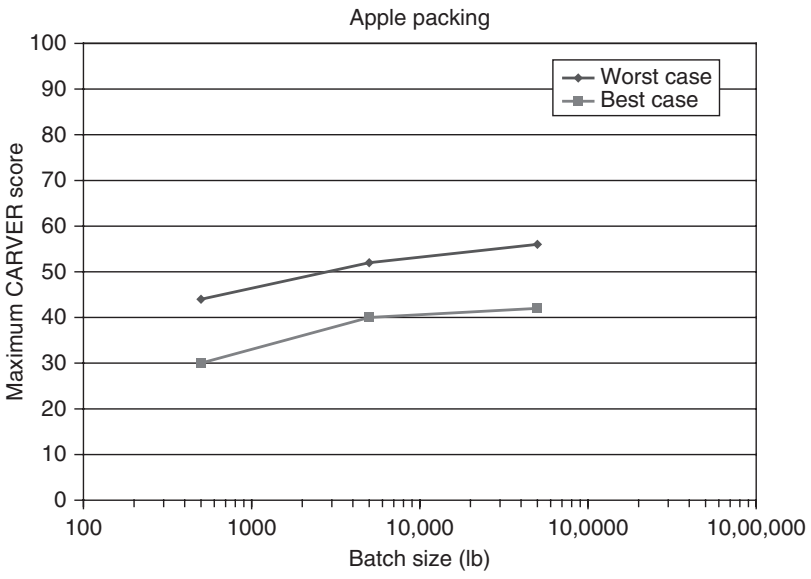



**FIGURE 5** Batch size dependence of total score for best/worst security practice.

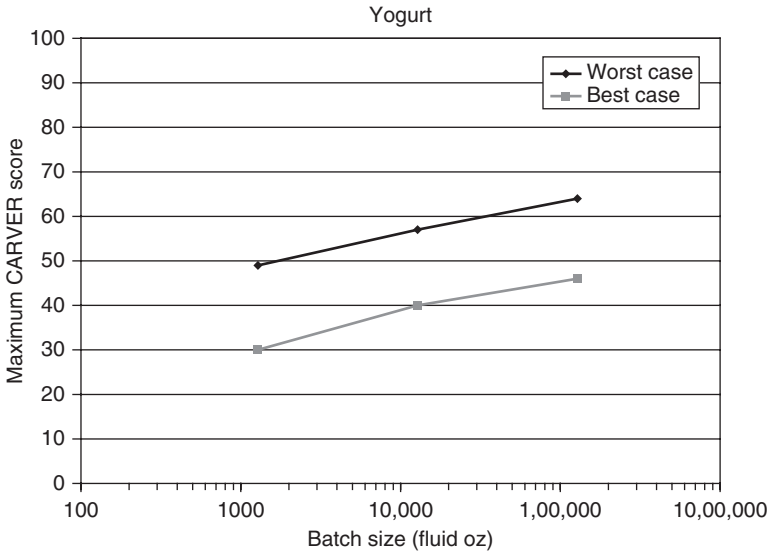



**FIGURE 6** Batch size dependence of total score for yogurt production security.

trend is expected, because the number of affected individuals scales with the size of the contaminated volume.

### 3.5 Toxic Agent Effects

The effects of the different properties of the various toxic agents considered are best illustrated in the yogurt production process. Table 4 shows scoring details for the best case scenario of the three levels of production of yogurt for toxic Agents 1, 2, and 4. As shown previously in Table 3, Agent 1 is the most temperature-sensitive and would be destroyed in the pasteurizer. Agent 4 is the least toxic and is subject to dilution by large batch sizes. Agent 2 is not destroyed in the pasteurizer and is toxic enough to be effective in the batch sizes considered. The scoring trends of Agents 3 and 5 were similar to Agent 2.

The differences in the toxic agent properties are best seen in the vulnerability scores for the process icons. The effect of temperature susceptibility can be seen by comparing the vulnerability scores for Agent 2 and Agent 1. The vulnerability scores for Agent 2 are high for the culturing tank and other process steps upstream. The vulnerability scores for Agent 1 are high only for the culturing tank, which is immediately downstream from the pasteurizer. The algorithms used in CARVER+Shock look downstream for higher-temperature processing steps and adjust scores accordingly, based on the properties of the toxic agent. Since the pasteurizer will destroy Agent 1, only process steps downstream from the pasteurizer have high scores.

Dilution effects are illustrated by the vulnerability scores for Agent 4. The maximum vulnerability score is 6 at the local scale, drops to a score of 4 at the regional scale, and reaches 1 at the national scale.

**TABLE 4 Scoring Details for Best Case Yogurt Production**

| | Agent 1 | | | | | | | | Agent 2 | | | | | | | | Agent 4 | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Local Best | C | A | R | V | E | R | S | Tot | C | A | R | V | E | R | S | Tot | C | A | R | V | E | R | S | Tot |
| Milk | 5 | 4 | 2 | 1 | 2 | 5 | 5 | 24 | 5 | 4 | 2 | 1 | 2 | 6 | 5 | 25 | 5 | 4 | 2 | 1 | 2 | 4 | 5 | 23 |
| Filter | 5 | 1 | 2 | 1 | 2 | 5 | 5 | 22 | 5 | 1 | 2 | 8 | 2 | 6 | 5 | 30 | 5 | 1 | 2 | 4 | 2 | 4 | 5 | 24 |
| Cooler/Chiller | 5 | 1 | 2 | 1 | 2 | 4 | 5 | 20 | 5 | 1 | 2 | 8 | 2 | 5 | 5 | 28 | 5 | 1 | 2 | 4 | 2 | 4 | 5 | 24 |
| Pasteurizer | 6 | 5 | 4 | 1 | 2 | 4 | 6 | 28 | 6 | 5 | 4 | 1 | 2 | 5 | 6 | 29 | 6 | 5 | 4 | 1 | 2 | 4 | 6 | 28 |
| Culture | 5 | 1 | 2 | 8 | 2 | 4 | 5 | 28 | 5 | 1 | 2 | 8 | 2 | 5 | 5 | 28 | 5 | 1 | 2 | 6 | 2 | 4 | 5 | 25 |
| Culturing Tank | 5 | 5 | 1 | 1 | 2 | 4 | 5 | 23 | 5 | 5 | 1 | 1 | 2 | 5 | 5 | 24 | 5 | 5 | 1 | 1 | 2 | 4 | 5 | 23 |
| Fruit | 5 | 1 | 2 | 3 | 2 | 4 | 5 | 22 | 5 | 1 | 2 | 3 | 2 | 5 | 5 | 24 | 5 | 1 | 2 | 1 | 2 | 4 | 5 | 20 |
| Bottler | 5 | 2 | 2 | 3 | 2 | 5 | 5 | 24 | 5 | 2 | 2 | 3 | 2 | 6 | 5 | 25 | 5 | 2 | 2 | 1 | 2 | 4 | 5 | 21 |
| Ref./FznStor. | 5 | 1 | 1 | 1 | 2 | 5 | 5 | 20 | 5 | 1 | 1 | 1 | 2 | 6 | 5 | 21 | 5 | 1 | 1 | 1 | 2 | 4 | 5 | 19 |
| Max Score | 6 | 5 | 4 | 8 | 2 | 5 | 6 | 28 | 6 | 5 | 4 | 8 | 2 | 6 | 6 | 30 | 6 | 5 | 4 | 6 | 2 | 4 | 6 | 28 |
| Regional Best | C | A | R | V | E | R | S | Tot | C | A | R | V | E | R | S | Tot | C | A | R | V | E | R | S | Tot |
| Milk | 7 | 2 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 2 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 2 | 2 | 1 | 3 | 10 | 7 | 32 |
| Filter | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 1 | 2 | 10 | 3 | 10 | 7 | 40 | 7 | 1 | 2 | 4 | 3 | 10 | 7 | 35 |
| Cooler/Chiller | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 1 | 2 | 10 | 3 | 10 | 7 | 40 | 7 | 1 | 2 | 4 | 3 | 10 | 7 | 35 |
| Pasteurizer | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 1 | 2 | 10 | 3 | 10 | 7 | 40 | 7 | 1 | 2 | 4 | 3 | 10 | 7 | 35 |
| Culture | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 |
| Culturing Tank | 7 | 1 | 2 | 10 | 3 | 10 | 7 | 40 | 7 | 1 | 2 | 10 | 3 | 10 | 7 | 40 | 7 | 1 | 2 | 4 | 3 | 10 | 7 | 35 |
| Fruit | 7 | 1 | 1 | 1 | 3 | 10 | 7 | 30 | 7 | 1 | 1 | 1 | 3 | 10 | 7 | 30 | 7 | 1 | 1 | 1 | 3 | 10 | 7 | 30 |
| Bottler | 7 | 1 | 2 | 3 | 3 | 10 | 7 | 34 | 7 | 1 | 2 | 3 | 3 | 10 | 7 | 34 | 7 | 1 | 2 | 3 | 3 | 10 | 7 | 34 |
| Ref./FznStor. | 7 | 1 | 2 | 3 | 3 | 10 | 7 | 34 | 7 | 1 | 2 | 3 | 3 | 10 | 7 | 34 | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 |
| Truck | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 | 7 | 1 | 2 | 1 | 3 | 10 | 7 | 32 |
| Max Score | 7 | 1 | 2 | 10 | 3 | 10 | 7 | 40 | 7 | 1 | 2 | 10 | 3 | 10 | 7 | 40 | 7 | 1 | 2 | 4 | 3 | 10 | 7 | 35 |
| National Best | C | A | R | V | E | R | S | Tot | C | A | R | V | E | R | S | Tot | C | A | R | V | E | R | S | Tot |
| Milk | 9 | 2 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 2 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 2 | 2 | 1 | 4 | 10 | 10 | 38 |
| Filter | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 1 | 2 | 10 | 4 | 10 | 10 | 46 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |
| Cooler/Chiller | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 1 | 2 | 10 | 4 | 10 | 10 | 46 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |
| Pasteurizer | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 1 | 2 | 10 | 4 | 10 | 10 | 46 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |
| Culture | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |
| Culturing Tank | 9 | 1 | 2 | 10 | 4 | 10 | 10 | 46 | 9 | 1 | 2 | 10 | 4 | 10 | 10 | 46 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |
| Fruit | 9 | 1 | 1 | 1 | 4 | 10 | 10 | 36 | 9 | 1 | 1 | 1 | 4 | 10 | 10 | 36 | 9 | 1 | 1 | 1 | 4 | 10 | 10 | 36 |
| Bottler | 9 | 1 | 2 | 3 | 4 | 10 | 10 | 40 | 9 | 1 | 2 | 3 | 4 | 10 | 10 | 40 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |
| Ref./FznStor. | 9 | 1 | 2 | 3 | 4 | 10 | 10 | 40 | 9 | 1 | 2 | 3 | 4 | 10 | 10 | 40 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |
| Truck | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |
| Max Score | 9 | 1 | 2 | 10 | 4 | 10 | 10 | 46 | 9 | 1 | 2 | 10 | 4 | 10 | 10 | 46 | 9 | 1 | 2 | 1 | 4 | 10 | 10 | 38 |

## 4 RESULTS OF CARVER + SHOCK ACTIVITY

In analyzing the effectiveness of the CARVER+Shock activity, we see that the software program allows users to identify the most critical, vulnerable, or accessible steps in the food processing systems. The variation of recuperability, effect, and shock scores is negligible amongst the nodes, as is found in many of the SPPA exercises. This lack of variation suggests that modifications of the methodology or possibly, the scoring mechanism should be considered.

Following identification of nodes with high scores, the program also gives mitigative information on how to reduce and even prevent potential threats (Fig. 7). The culturing tank had the highest score for the yogurt example and the individual attribute scores are listed along with the mitigation recommendations for reducing recognizability.

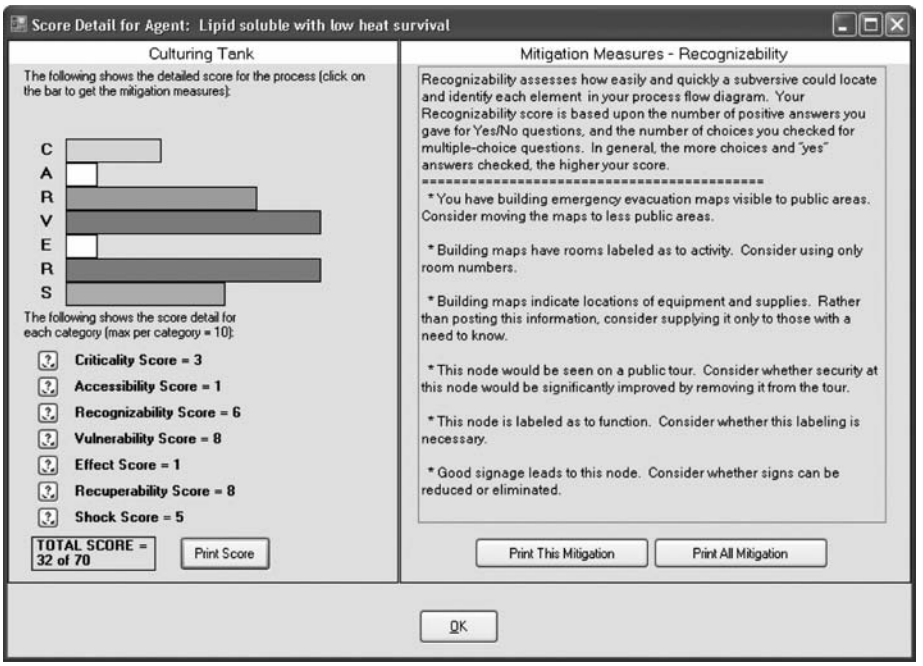



**FIGURE 7** Culturing tank score detail for yogurt production security.

## 5 DISCUSSION

The CARVER+Shock scores show variability among processes and among steps within processes with regard to the seven attributes analyzed by the SPPAs. Changing the batch size can affect Criticality. Increasing security can reduce Accessibility or Recognizability. Changing the nature of process steps, if feasible, can reduce Vulnerability or Effect. Modifications of the methodology or the scoring mechanism could increase the sensitivity of Recuperability, Effect, and Shock.

In future versions of the software, the output will be connected to a database of mitigation steps that can be further pursued. This database is near completion by the FDA and the scheduled release of version 2.0 of CARVER is early Spring 2009. This version of the software will also include preharvest (horticulture and anumal husbandry) as well as retail and restaurant modules [3].

## REFERENCES

1. Food defense at U.S. Food and Drug Administration, http://www.cfsan.fda.gov/~dms/defterr.html
2. Strategic Partnership Program Agroterrorism (SPPA) (2007). Initiative—First Year Status Report July, 2006, http://www.cfsan.fda.gov/~dms/agroter5.html, Second Year Status Report, Septemper 2007, http://www.cfsan.fda.gov/~dms/agroter6.html
3. Davis, S. F., McEntire, J. C., Acheson, D., Busta, F., Harlander, S., Acheson, D., Danneels, J., Ostfield, M., Pohl, P., Hoffman, C. J. T., Green, K., and Wankowski, D. (2007). International conference focuses on food Defense. *Food Technol.* **61**(9), 125–128.

# THE EDEN HOMELAND SECURITY PROJECT: EDUCATIONAL OPPORTUNITIES IN FOOD AND AGROSECURITY

STEVE CAIN

*Extension Disaster Education Network, Purdue University, West Lafayette, Indiana*

## 1 INTRODUCTION

The Extension Disaster Education Network (EDEN) Homeland Security Project (see logo in Fig. 1) provides research, materials, and educational courses to enhance Extension's abilities to deliver disaster and emergency management education. This article offers an overview of those efforts, provides insight into key issues, and information on the development of EDEN Homeland Security information and educational products.

EDEN reduces the impact of disasters through education. EDEN provides Extension, nationwide, with a network of specialists and a shared database of educational tools.

Extension has been involved in disaster education for decades, and in homeland security in a different form, since the civil defense days. Since 1993 EDEN, as a collaborative multistate effort, has improved the delivery of services to citizens affected by disasters. To learn more about United States Department of Agriculture (USDA)'s Cooperative State Research, Education and Extension Service (CSREES) visit: http://www.csrees.usda.gov/qlinks/extension.html.

EDEN primarily functions as a network of professionals with more than 75 subject-matter specialties, ranging from human development to crop and livestock development. Resources from the land grant, sea grant, and related institutions are shared through a national EDEN web site: www.EDEN.lsu.edu. This site provides Extension agents and educators access to resources for all phases of disaster management. EDEN also partners with USDA-CSREES.


**FIGURE 1** Logo of the EDEN homeland security project.

EDEN's mission is carried out through:

- interdisciplinary and multi-state research and education programs addressing disaster mitigation, prevention, preparation, response, and recovery;
- linkages with federal, state, and local agencies, and organizations;
- anticipation of future disaster education needs and actions;
- timely and prompt communications and delivery of information that meets audience needs; and
- credible and reliable information.

This article focuses on and highlights relevant EDEN homeland security efforts and findings. By design, EDEN is a multidiscipline, all-hazards network. Therefore, the varied topics covered here are homeland security-related.

## 2 CHILDREN AND TERRORISM

EDEN lunged into homeland security mode within moments of the 9/11 attacks. While hundreds of millions of people watched the horrific scenes of the destruction of the twin towers, thousands of first responders rushed to help. At the same time, EDEN responded by identifying pertinent educational information.

Public information officers (PIOs) for emergency management know that one of the primary needs of people in the event of a disaster is information. Mobilizing information helps people. It save lives, reduces the impact of the disaster, and helps with a quick recovery.

Within a few hours of the 9/11 attacks, EDEN made web resources available to help parents explain the disturbing events that were unfolding on television. Through the EDEN network and web page, day care centers and schools across the nation had access to handouts for parents on talking with their children about terrorism. By the end of the day, thousands of schools, day care centers, and news media had downloaded the vital information.

Studies have found that parents' levels of functioning, along with their relationships with each other, can be a buffer against the negative impact that disasters have on children. Thus, it was important after 9/11 that parenting partners pay attention to each other's needs, their own individual needs, and their children's needs. Because terrorism is still relatively new to the United States, many families do not necessarily have the skill sets to help children cope with terrorism. EDEN offers so many resources to help families cope, see Ref. 1.

## 3 AGROTERRORISM

Records captured in Afghanistan show that terrorists plotted to strike at the United States' agricultural system, not only to spread terror, but to hit the United States in this important economic sector. Within days of 9/11, EDEN's efforts produced a back-grounder for Extension educators to talk with farmers, ranchers, and producers about terrorism. This backgrounder, simply called *Agroterrorism*, www.ces.purdue.edu/eden/

disasters/agro/**Agroterrorism**.doc was used nationally and internationally by educators and the news media. It was developed from work done by the USDA and land grant universities to better understand and develop ways to cope with agroterrorism. It also helped unify use of the term *agroterrorism*, which was a newly evolving term. Other forms of the word included hyphenation and use of "agri" instead of "agro", which is helpful information for those doing research on the web.

The article explained that potential economic costs for an agroterrorism event could cost the United States more than $100 billion in short- and long-term losses in livestock and crop production and industries related to farming, such as transportation, processing, and retailing. Information is also given to help size up the possibility or probability of an agroterrorism event. The critical issue with agroterrorism is the low level of technical knowledge required to implement it. Any person with minimal understanding of microbiology can acquire the organisms and spread them, needing less technical know-how than what is required for other forms of bio-warfare, including that against humans.

When most people think of agroterrorism they probably think of extremist groups as being the major threat, when in reality agroterrorism, in many forms, has been around since people first began to till the soil, for example, burning or poisoning a rival's crops.

In Ref. 2, Anne Kohnen states that "Terrorists' motives vary widely . . . . The two most common today are the profit motive and the anti-GMO (genetically modified organism) motive." After the events of September 11, 2001, that list expanded to include international terrorists bent on harming the US economy and creating fear and mistrust toward governing agencies.

Today, the types of people who might instigate an agroterrorism attack fall into three categories:

- a criminal or activist with idealist motives;
- a criminal with economic motives;
- in international terrorist with motives against the United States.

### 3.1 Counterattack on Agroterrorism

Agricultural economists noted in Ref. 3:

> Given the potentially devastating impact, the best procedure is not only to increase our border defenses against Foot and Mouth Disease, but also plan and organize in advance to combat it effectively when it arrives.

Otto Doering, Purdue Extension agricultural economist, noted that the key determinants of the economic impact are:

- *Geography.* Where and over what area will the outbreak (contamination) occur?
- *Timing.* How quickly will outbreaks be detected and dealt with?
- *Strategy.* What strategy will be used to respond to the outbreak?

To prevent or reduce the impact of diseases, Kohnen listed four areas of USDA concentration:

1. the organism level, through animal or plant disease resistance;

2. the farm level, through facility management techniques designed to prevent disease introduction or transmission;
3. the agricultural sector level, through USDA disease detection and response procedures; and
4. the national level, through policies designed to minimize the social and economic costs of catastrophic disease outbreak.

For example, Kohnen recommended that to reduce the threat and costs of an attack at the organism level, the USDA should be ready with vaccines for the major forms of diseases affecting animals. Other mitigating actions would include training veterinarians, veterinary students, and plant pathologists on countering agroterrorism with emphasis on early diagnosis of potential diseases. At the farm level, the USDA should establish a biosecurity program to educate farmers on biosecurity best management practices.

In addition, Ken Foster, from the Department of Agricultural Economics at Purdue added, "It is important to place great emphasis on a detailed plan which clearly spells out the degree and mechanisms by which producers will be compensated for losses. The compensation plan has to clearly eliminate the private economic incentive to hide an outbreak that a producer faces. The cost of many contagious livestock diseases is so great that the rest of society can easily justify compensating individuals for early reporting."

At the national level, contingency budgets should be in place to fund disease eradication and compensation costs for producers who have a loss, and public affairs campaigns that bolster public confidence in the food production system. At the state level, laboratories should be given diagnostic capabilities and screening authorities to facilitate rapid diagnosis. At the local level, communities should identify a coalition of local officials, such as law enforcement, emergency managers, Extension, American Red Cross, and other leaders to address and respond to local disasters.

People concerned with potential agroterrorism should take steps to be informed. The USDA, the Department of Homeland Security (DHS) (and other federal departments), and land grant universities, including Extension, can be excellent sources of objective information. Also, concerned individuals may want to be involved at the local level to be sure that community disaster plans are addressed. There should be discussions with key people about their concerns and they should be encouraged to share their opinions with lawmakers.

Agricultural leaders, key stakeholders, and lawmakers must work together to make sure that the proper laws, procedures, and resources are in place to mobilize quickly and resolve any infestation or contamination. This includes rapid detection and containment to reduce the spread of infection and impact on the US economy. In addition, specific measures must be in place so that farmers, ranchers, and others in the agricultural sector have the proper education for detection and eradication. The information flow must convince farmers who are victims of an attack, that the proper eradication steps and economic reimbursements are in place. Once the proper steps have been taken, a consumer awareness and public education campaign must take place to restore domestic and international consumers' confidence in the food supply and the regulatory agencies.

## 4 EDEN HOMELAND SECURITY PROJECT

Immediately after 9/11, program leaders at the CSREES realized that EDEN could play an important role in homeland security education. The network applied for and received a $600,000, 2-year grant to examine homeland security educational needs and to begin building a bank of educational programs and courses to address those needs.

Since 2002, USDA-CSREES has supported the EDEN Homeland Security—Food and Agricultural Defense projects. The USDA-CSREES grant funded the development of several homeland security-related courses, research on interagency communication, basic EDEN communication support (at Purdue University), and web management support (at the Louisiana State University Agricultural Center). At the same time, EDEN established the EDEN Homeland Security Project Team.

### 4.1 EDEN Homeland Security Surveys

In 2002, EDEN conducted Homeland Security surveys of Extension educators, across the country, who represented the educational program areas of:

- Family and Consumer Sciences,
- Leadership and Community Development,
- 4-H and Youth Development, and
- Agriculture and Natural Resources.

The main goal of the surveys was to determine county-based educators' needs for educational materials regarding homeland security. Homeland security topics regarding how urgent they were to the educator's community were rated. The ratings (shown in Table 1) have guided the search for usable materials and the development of new materials.

At the same, time EDEN conducted a national survey of farmers, ranchers, and producers about their homeland security concerns (Table 2). The participants were asked if they had discovered a crop disease outbreak on their farm that was not recognizable and to whom they would turn to for advice. They were asked to check off the top

**TABLE 1 Results of Surveys to Determine Needs of County-Based Educators for Educational Materials Regarding Homeland Security**

| Security Topic | Urgent, 1–3 (%) | Not Urgent, 7–9 (%) |
|---|---|---|
| Drinking water | 78 | 4 |
| Food | 64 | 9 |
| Individual's role | 57 | 14 |
| Government's role | 55 | 14 |
| Animal biosecurity | 50 | 12 |
| Personal | 48 | 13 |
| Farm | 45 | 12 |
| Financial | 42 | 15 |
| Plant/crop biosecurity | 37 | 16 |

**TABLE 2 Result of a National Survey, Conducted by EDEN, of Farmers, Ranchers, and Producers about their Homeland Security Concerns**

| Agency/Person to Contact | Percentage |
|---|---|
| Cooperative Extension service | 79 |
| State department of agriculture | 42 |
| Another farmer/rancher | 32 |
| Pesticide dealer/representative | 31 |
| Consultant provided by dealer | 28 |
| Hired crop consultant | 10 |

three. Among many findings, the survey showed the majority of farmers would turn to Extension first, for a crop biosecurity concern that might be homeland security-related.

With the survey of urgent educational needs identified, EDEN began to address the issues. Instead of developing new, resources, the first goal was to find resources that matched the identified needs.

A publication from the Federal Emergency Management Agency (FEMA) [4] addressed many of the top priorities, including drinking water security, general information on the government's and the individuals' role in a world threatened by terrorism, and personal security. The DHS took steps to address food security needs by funding a DHS Academic Center of Excellence on Food Security at the University of Minnesota.

Having identified existing resources and making them available through the national EDEN web page www.EDEN.lsu.edu, the Homeland Security Project team began to allocate resources in the areas of most interest that were identified in the survey by farmers, ranchers, and producers.

## 5 INTERAGENCY RELATIONS IN ANIMAL DISASTER MANAGEMENT

One of the first efforts was to find more specific information on the government's role in an agricultural disaster. While FEMA's "Are You Ready" [4] had good information on general preparedness, more information was needed on the government's role in a terrorist attack on animal agriculture.

### 5.1 Defining the Issues

In 2003, Borron and Cain started a research project examining local, state, and federal regulations in the event of massive animal death. This work became part of a larger project for the USDA, which was lead by Kansas State University, Texas A&M University, and Purdue University [5].

Their goal was to identify all of the key agencies that might be involved in the response to massive animal die-off and examine the nature of the partnerships for such an event. For this project, the key people from those agencies were asked to spell out their roles and responsibilities in a fictional case of dead animal disease (DAD) that crossed species and occurred on several farms in Indiana. Those agencies submitted their

reports, which were shared with all the other agencies. Two weeks later, a roundtable discussion was conducted in which the agencies discussed how their role might change with consideration of what the other agencies said and as the scenario changed.

The results showed that there are significant tools to help agencies understand who plays what role, but not enough is being done to ensure that all agencies use those tools. Though not all potential problems can be anticipated and addressed in advance of a major biosecurity event, two overall actions might prevent a massive animal disaster from taking larger tolls. They are education and facilitation.

Factors related to education for better understanding include

- the Incident Command System (ICS) by agricultural industry leaders and participants;
- the ICS, standard operations procedures (SOPs), and agriculture by county governments and agricultural groups;
- agriculture by the emergency management and county government systems; and
- agricultural, disaster response by state, and local agencies (public health, legal, etc.).

A primary factor related to facilitation is encouragement of periodic (annual or semi-annual) meetings for all agencies at the state level to discuss specific operational, legal, and future research needs in the area of animal disaster management. These actions would also include exercising existing agreements.

In Indiana, two specific actions will enhance the response efforts during a major disaster.

- First, the necessary agencies need to know they are part of the Comprehensive Emergency Management Plan (CEMP) plan, and what role they play.
- Second, more people within agencies should have a comprehensive awareness and understanding of other agencies involvement, in addition to understanding their own agency's SOPs.

In 2003, US President George W. Bush issued directives that provided the Secretary of Homeland Security with the responsibility to manage major domestic incidents by establishing a single, comprehensive National Incident Management System (NIMS). The introduction of NIMS provides organizational muscle to the ICS, but still, not enough has been done to ensure NIMS and ICS, and subsequent agreements are well spelled out and exercised, especially at the county level, in response to major agricultural disasters.

An idealistic approach to a disaster would be to know, in detail, what needs to be done, what protocols need to be enacted, and who is going to take the lead. However, no real-life disaster plays out as a textbook example. General disaster plans are created with a number of annexes and SOPs attributed to specific situations. Regardless of the tragedy or the number of agencies involved, there are several areas that should be addressed to achieve a higher level of preparedness and response.

An interagency working group should be created that meets two times a year and consists of at least the state environmental, animal health, public health, contract service, emergency management, Extension service, transportation, and wildlife agencies.

An analysis should be conducted of the agencies' (county, state, and federal) awareness level of the functionality of the CEMP and its components related to agriculture, as well

as the overall functions of the ICS and NIMS. Questions that must be asked include the following:

- Have the correct agencies been included?
- Are there appropriate training opportunities for agency employees?
- Do the involved agencies have a well-established representation of their SOPs within the annexes of the CEMP?
- Are memorandums of agreement (MOAs) and other agreements tested through exercises.

A training program should be initiated that:

- requires ICS training for all agencies involved in the CEMP—state and country level;
- includes adequate representation from various agencies to ensure a widespread understanding of the ICS and various agencies roles;
- establishes programs at the county level to bridge the gap between the legal system and agricultural issues in a biosecurity event so that legal countermeasures to stop control efforts are made based on informed decisions.

Results of this roundtable discussion demonstrated that (i) more could be known about how critically involved agencies will react to a massive animal carcass disposal situation, and (ii) in an environment of short-staffing and high workloads, agency personnel will likely not place a high priority on planning for theoretical animal carcass disposal issues.

Therefore, to facilitate planning efforts and provide structure for interagency discussions and exercises, research into (and summarization of) the actual laws, regulations, guidelines, and SOPs of key agencies is warranted on a state-by-state basis.

This type of research is critical to the development of comprehensive plans for state and county governments to more easily identify their roles. These could be used in training programs for state and local agencies to develop pertinent SOPs and MOAs.

### 5.2 Agrosecurity Workshops for Interagency Relations

Extension professionals throughout the country recognized the need to better define their roles—and the roles of other agencies and organizations—before, during, and after an animal agrosecurity event. In addition, those roles vary from state to state, so there is a need to help agencies and organizations to fully understand the capacity to which Extension can serve in this arena.

With support from the Cooperative State Research, Education, and Extension Service, EDEN offered six regional conferences in 2007 and 2008, focusing on animal agrosecurity.

By the end of each conference, attendees are able to describe the roles of Extension and other agencies/organizations in an animal agrosecurity event within their region. Conference attendees can identify key roles and players in:

- emergency and disaster management in an animal agrosecurity event;
- education during all phases of emergency and disaster management;

- partnership development within and across states;
- crisis communication related to an animal agrosecurity event;
- state animal response team development;
- educational program and material development/delivery for an animal agrosecurity event.

For an analysis of outcomes of these events and a lisitng of conference hosts see Ref. 6.

## 6 EDEN COURSES

The following describes several courses developed by EDEN to help various audiences understand and prepare for natural disasters and homeland security events. All courses mentioned here are free of cost and are available on the EDEN web site at www.EDEN.lsu.edu/LearningOps.

### 6.1 Plant Biosecurity Course

In 2004, the EDEN Homeland Security Project released the EDEN *Plant Biosecurity Management Course*. EDEN focused on the plant course because Extension was identified as the preferred source of information if farmers or ranchers suspected an unrecognized crop disease outbreak on their farm.

A major attack or natural outbreak on US farms could cost the economy millions in control responses and billions in economic damages. Further, mismanaging a crop or plant biosecurity outbreak by not detecting it, or not communicating appropriate information, could increase damages.

The *Plant Biosecurity Management Course*, developed by a team at the University of Missouri, was designed to help Extension educators across the country better participate in all phases of a crop biosecurity disaster. Those phases included mitigation, preparedness, response, and recovery.

Anyone completing the on-line course will be better prepared to plan for and contribute to recovery efforts of a plant or crop biosecurity event.

The team's primary audience for the course was crop advisors, Extension professionals, and specialists who understand the urgency of plant protection and will have the opportunity to teach plant biosecurity management to those involved in the US plant sciences agricultural sector. This course enables Extension professionals to teach agricultural producers, workers, and others who are involved or have a vested interest in the US plant sciences agricultural sector on how to:

- prepare for a plant biosecurity event;
- appropriately respond and recover from a plant biosecurity event;
- reduce the effects of future plant biosecurity events.

The course was originally offered in 2004, but a new edition was released in 2006. Though the course aims to provide Extension educators and specialists with pertinent information, it is readily usable by agricultural and horticultural producers, emergency managers, and public health officials who have a vested interest in plant biosecurity.

Developed for EDEN by the University of Missouri Extension with support from the USDA, the 2006 edition provides updated and timely resources, as well as preventative activities, and current response efforts of the soybean rust monitoring and protection program. The course is free of charge and designed to be taken at a user's own pace. Completion time is approximately 8 h.

The six lessons focus on:

- the threat of both intentional and unintentional introduction of pests and pathogens to crops;
- how to mitigate plant biosecurity hazards and security risks to farm operations and agribusinesses;
- how to prepare for a rapid and appropriate response to a suspected plant biosecurity problem;
- what recovery activities to expect in the event a plant biosecurity problem is confirmed; and
- how to reduce the impact of a biosecurity event on humans, crops, property, and the environment.

### 6.2 Food Protection Course

The next EDEN course, *OnGuard: Protecting America's Food System* helps explain the protection of the United States' food production system and helps explain the consumer's role in food protection. Understanding how the US food system works and protecting the system against intentional attacks is the responsibility of all citizens.

This course is geared toward the general public through the facilitation of an Extension office in local, county-based meeting. The course focuses on:

- how specific food products are created and how they move through the food system;
- how our government protects against threats to the US food system;
- food-related actions a family can take to prepare for any type of disaster or emergency;
- what consumers and agricultural producers can do to protect against intentional threats to the food system; and
- lessons learned from actual cases of intentional attacks on our food systems.

This course was developed for EDEN at the University of Minnesota.

### 6.3 Business Preparedness

In 2005–2006, EDEN collaborated with the DHS to develop *Ready Business: Preparing a Disaster Business Plan*. The course helps businesses prepare for all-hazard disasters, including homeland security-related events. This course ties in closely with DHS's Ready campaign (www.ready.gov).

At one time or another, every community will be affected by an emergency or disaster. It is important for business owners and operators to understand how to prepare and manage their businesses through difficult times including disasters.

By preparing for emergencies and disasters in advance, businesses can save time and money in extreme situations. Therefore, EDEN developed the *Ready* Business course, enabling businesses to better understand this issue.

The course is geared toward small- and medium-sized business owners through the facilitation of a local Extension professional or volunteer group. Created to be taught in a classroom setting, this 3–4-h course helps participants walk away with the beginning of a disaster plan.

The course covers:

- developing a basic understanding of disaster preparedness and the importance of business planning;
- uncovering the significance of communicating regularly with employees before, during and after an incident;
- recognizing the need for evacuation and shelter-in-place plans; and
- taking steps to safeguard companies and secure physical assets.

This course was developed for EDEN by Purdue Extension, with support from the DHS and USDA and a team of experts from universities around the United States and CSREES.

### 6.4 Pandemic Preparedness for Businesses

At about the time that the Ready Business course was being developed, news of a potential pandemic surfaced. In fact, authorities continue to state that it is not a matter of "if" a pandemic strikes, but "when." Because DHS played a major role in supporting pandemic preparedness efforts, the EDEN Homeland Security Project team decided to take the *Ready Business* materials one step further and develop the *Pandemic Preparedness for Business Course*.

EDEN felt it was important for business owners and operators to understand how to prepare and manage Their business through a pandemic.

By preparing for a pandemic in advance, businesses can save time and money in extreme situations. The course is geared toward small- and medium-sized business owners through the facilitation of a local Extension professional. Created to be taught in a classroom setting, this 90-min course is available on-line and can be taught be any volunteer or professional with emergency management background.

The course focuses on:

- developing a basic understanding of pandemic preparedness and the importance of business planning;
- uncovering the significance of communicating regularly with employees before, during and after a pandemic; and
- understanding how businesses can help employees deal with a severe pandemic.

This course was developed for EDEN by Purdue Extension, with support from USDA and the same team that developed the Ready Business course.

### 6.5 USDA and the National Response Plan

Late in 2006, EDEN introduced a course titled USDA's Roles in the National Response Plan.

Because the National Response Plan is a comprehensive plan that establishes a single framework for the management of domestic incidents. it is imperative that Extension professionals understand their responsibility in the response efforts.

This plan relates how the federal government coordinates with state, local, and tribal governments and the private sector during incidents.

This course was developed for EDEN at North Dakota State University.

Through this course participants will:

- develop a basic understanding of the field of emergency management;
- increase awareness of the National Response Plan and NIMS;
- recognize the potential roles of Extension professionals in the National Response Plan, and disasters in their communities;
- discover potential resources for Extension staff members on hazard and disaster issues.

The materials provided in the course are intended for use at Extension workshops and/or staff development presentations with other local, state, and federal USDA agencies:

- Ready-to-use presentations with available audio
- Master documents for handouts

### 6.6 Pandemic Preparedness for Faith-Based Organizations

In 2007, enhancing the work previously done on pandemic preparedness, EDEN released a course targeting faith-based organizations (FBOs). The course is titled *Pandemic Influenza Preparedness for Faith-Based Organizations*.

This course was designed by EDEN, in collaboration with the Centers for Disease Control and Prevention, to enable congregations, synagogues, mosques and other places of worship to (i) protect the health of their staff and the communities in which they serve and (ii) fulfill their organizational mission during an influenza pandemic. The course is divided into two sections:

*Section 1.* Participants learn about pandemic influenza and infection control measures to use in their organization to protect themselves and their community before and during a pandemic.

*Section 2.* The course highlights organizational measures in which participantsl learn about the potential impact of pandemic influenza on their organization. They also learn to write a basic pandemic influenza preparedness and response plan to maintain the critical functions of the organization.

Extension educators, public health officials, and others with an interest in teaching FBOs to be better prepared for a pandemic can download all needed curriculum materials from the EDEN web site. FBO leaders, staff members, or volunteers charged with

pandemic influenza preparedness can also walk themselves through the on-line materials, rather than taking it in a classroom setting, if they prefer.

Through instructional design, course participants will be tested frequently on the material they are learning and encouraged to begin writing their pandemic influenza preparedness and response plan.

This course was developed by EDEN with help from the Centers for Disease Control and Prevention.

### 6.7 Animal Biosecurity and Emergency Management Course

The latest course to be developed is titled *Animal Biosecurity and Emergency Management Course*.

The ultimate goal of the course is to educate Cooperative Extension Service personnel and first responders so they may collaborate effectively during an animal agricultural emergency. In addition, producers acquire an awareness of their role in the phases of animal emergency management.

The course covers animal biosecurity and emergency management during natural and man-made disasters. Topics include interdisciplinary and interagency collaboration; prevention/mitigation, preparedness, response, and recovery measures; and biosecurity management. The course ends with several discussion-based scenarios depicting simulated animal emergencies, which allow students to apply course concepts.

Supplemental materials include:

- PowerPoint presentations and Instructor's Guides for use in face-to-face trainings;
- checklists including a facility vulnerability assessment, animal emergency action plan, off-farm risk assessment, and so on;
- fact sheets on animal diseases, animal handling, emergency fencing, and so on.

The course was developed at the University of Kentucky.

Technical support was provided by University of Kentucky Agricultural Communications Services and the Creative Applications for Learning Environments Laboratory.

The ultimate goal of the course is to educate Cooperative Extension Service personnel and first responders so they may collaborate effectively during an animal agricultural emergency. In addition, producers will acquire an awareness of their role in the phases of animal emergency management.

The lesson titles are as follows:

- Animal Emergency Management: Natural Disasters
- Animal Emergency Management: All Hazards
- Interdisciplinary Components of Animal Emergency Management
- Animal Management: Prevention/Mitigation and Preparedness
- Farm Management: Prevention/Mitigation and Preparedness
- Incident Management: Response and Recovery
- Off-Farm Biosecurity Management

The course was developed at the University of Kentucky.

**REFERENCES**

1. *Children's and Disasters*. EDEN, http://eden.lsu.edu/.
2. Kohnen, A. (2001). *Responding to the threat of agroterrorism: specific recommendations for the United States Department of Agriculture*, Discussion Paper 2000–29 October 2001.
3. Foot and Mouth Disease. (2001). *Purdue Agricultural Economics Report*, May 2001.
4. *Are You Ready?: An In-Depth Guide to Citizen Preparedness*, Federal Emergency Management Agency, http://www.fema.gov/areyouready/index.shtm.
5. Borron, A., and Cain, S. *Regulatory Issues & Cooperation*. University of Kansas, Available at http://fss.k-state.edu/index.php?option=com content&task=view&id=17&Itemid=37
6. *Regional Animal Agrosecurity Conferences*, EDEN, http://eden.lsu.edu/LearningOps/Workshops/AlAgroSecurity2007/OnePager.pdf.

# DECONTAMINATION AND DISPOSAL OF CONTAMINATED FOODS

M. Ellin Doyle, Seung Hak Lee, Craig H. Benson, and Michael W. Pariza
*University of Wisconsin, Madison, Wisconsin*

## 1 INTRODUCTION

Widespread contamination of the food supply with a hazardous agent would be an effective way for a terrorist to induce panic in the general population and cause great economic losses. Food processing and distribution have become more centralized, such that contamination in one plant may result in multistate and even international outbreaks of illness as occurred in 2006–2007 with spinach contaminated with *Escherichia coli* O157:H7, peanut butter containing *Salmonella*, and pet food with melamine. Food companies have developed procedures for recalling foods containing undeclared allergens, foreign material, or pathogenic bacteria but may not be equipped to handle large volumes of foods containing a terrorist agent. Such an event could present a substantial waste disposal problem for landfills and wastewater treatment plants (WWTPs) as well as for public health authorities. Representatives from disposal facilities, food companies, and government agencies participated in three meetings and voiced concern about a variety of issues that need to be addressed.

## 2 OVERVIEW

### 2.1 Agents

Disposal options for contaminated foods will be determined to some extent by the nature and concentration of the agent and its expected fate in landfills and wastewater treatment systems. Potential biological and chemical agents have been listed by Centers for Disease Control (http://www.bt.cdc.gov/agent/agentlistchem.asp, http://www.bt.cdc.gov/bioterrorism/) while toxic industrial chemicals that could pose a threat are listed by Occupational Safety and Health Administration (OSHA) (http://www.osha.gov/SLTC/emergencypreparedness/guides/chemical.html), and the most commonly encountered radionuclides are listed by Environmental Protection Agency (EPA) (Table 1). Some of these agents are inappropriate for poisoning food because their sensory characteristics would so alter the foods that they would not be consumed. Some microbes are not transmitted effectively through consumption of food and other agents are not soluble or stable in particular foods thereby precluding their use. There are also a number of other toxic chemicals and pathogens that terrorists may have access to, which are not on these lists. Accurate identification of the agent(s) used to contaminate food and their concentrations is necessary for making appropriate disposal decisions.

### 2.2 Food

A variety of foods could be contaminated by a terrorist and several factors, including the goal of the attack that will affect which food(s) might be chosen. If the goal is to cause widespread illness and death, then a highly infectious agent may be added to a commonly eaten, perishable food so that the agent will be widely dispersed and consumed before an alarm is raised. Massive economic losses and disruption of the food supply would be caused by contamination of animals in large rearing facilities or large areas of crop plants. Another goal may be to attack some American "icon" such as popular soft drinks, snacks, or fast foods. All of these possibilities should be considered in planning a response.

Target foods must be reasonably accessible. Although many processing plants have instituted strict in-house security practices, places where liquids or other foods are mixed in large tanks or vats may provide an opportunity to deposit some hazardous agent into food. Imported foods and food ingredients may be more easily contaminated in their country of origin or during transport from overseas locations. An imported contaminated spice, for example, may then be added to many different foods. One potential weak link in many food supply chains occurs during transport from farms to food processors. A mathematical model simulating contamination of milk with botulinum toxin demonstrated that a single addition of toxin, occurring at a holding tank on a dairy farm, in a truck transporting milk to a processing facility, or in a raw milk silo at a processing plant, could poison up to 142,000 gallons of milk [2].

Quantity of food requiring disposal as well as its nature (solid, liquid, acidic and fatty) will affect disposal decisions. Relatively small amounts of food containing very hazardous agents may be incinerated but usually solid foods would be sent to a landfill and liquids to a wastewater treatment plant. Recent recalls of "naturally contaminated" foods have involved millions of pounds of ground beef and millions of cases of canned products (http://www.fsis.usda.gov/Fsis_Recalls/index.asp) and a deliberate terrorist attack may contaminate even more food.

**TABLE 1 Radiological Agents: Potential sources, Disposal Limits in Wastewater, and Partitioning in Incinerators**

| Radionuclide | Chemical Formula | Source | Half-life | Concentration Permitted (Bq/ml)[a] | Estimated Partitioning (%)[b] | |
|---|---|---|---|---|---|---|
| | | | | | Combustion residues | Fly ash |
| Americium | $^{241}Am$ | Industrial/medical | 432.7 yr | 0.006 | 98 | 2 |
| Cesium | $^{137}Cs$ | Industrial/medical | 30 yr | 0.3 | 85 | 15 |
| Cobalt | $^{60}Co$ | Industrial/medical | 5.3 yr | 0.9 | 60 | 39 |
| Iodine | $^{129}I$ $^{131}I$ | Industrial/medical | $^{129}I$ ($15.7 \times 10^6$ yrs) | 0.06 | 2 | 68 |
| | | | $^{131}I$ (8 d) | 6.0 | | |
| Iridium | $^{192}Ir$ | Industrial/medical | 73.83 d | 3.0 | | |
| Plutonium | $^{238}Pu$ | Military/industrial | $^{238}Pu$ (87.7 yr) | 0.006 | 98 | 2 |
| | $^{239}Pu$ | | $^{239}Pu$ (24,100 yr) | 0.006 | | |
| | $^{240}Pu$ | | $^{240}Pu$ (6560 yr) | 0.006 | | |
| Polonium | $^{210}Po$ | Military | 138 d | 0.012 | | |
| Strontium | $^{90}Sr$ | Industrial/medical | 29.1 yr | 0.15 | 95 | 5 |
| Technetium | $^{99}Tc$ | Industrial/medical | 212,000 yr | 18.0 | 40 | 50 |
| Tritium | $^{3}H$ | Military/industrial Medical research | 12.3 yr | – | 0 | 0 |
| Thorium | $^{232}Th$ | Industrial | $1.4 \times 10^{10}$ yr | 0.009 | 98 | 2 |
| Uranium | $^{238}U$ | Military/industrial | $4.47 \times 10^9$ yr | 0.09 | 98 | 2 |

See http://www.epa.gov/radiation/radionuclides/index.html.

[a]Monthly average concentration limits for radionuclides disposed in sanitary sewers (10CFR20.2402).

[b]Predicted partitioning of radionuclides in an incinerator [1].

If contamination is discovered while the food is still within control of the food processor, it may be contained as a point source, secured and stored while disposal decisions are made. But if contaminated food were already distributed to retail stores and sold to the public, then the hazardous agent could be widely dispersed throughout the country. Consumers would be likely to throw the food in the trash or pour it down the drain unless a convenient, efficient collection system were organized to prevent indiscriminate disposal and further dissemination of the agent.

## 2.3 Decontamination

Neither municipal solid waste (MSW) landfills nor WWTPs would willingly accept foods with exotic terrorist agents if the fate of these agents during disposal were unknown. Effective decontamination or inactivation of agents may therefore be necessary before disposal. In a crisis situation, time constraints, cost, material limitations, and available diagnostic capabilities could limit decontamination options and it is not always clear what concentration of agent will be considered "clean enough" after decontamination [3].

Extensive information is available on destruction of many pathogens. However, some techniques are less effective when microbes are mixed with foods. EPA, the military, and some industries have had experience cleaning up chemical spills and deactivating chemical weapons and have developed decontamination procedures.

Biological agents are generally susceptible to heat, irradiation, and disinfectants. Vegetative bacteria are readily killed by thermal treatments although the actual time/temperature requirements for different species vary somewhat depending on the concentration of fats, sugars, and salts [4]. Vegetative bacteria are also readily inactivated by ionizing radiation and by chlorine (residual chlorine of $\sim$1.1 mg/l) if the organic load is low [5]. Viruses, protozoan parasites, and biological toxins are somewhat more heat stable in foods but, with the exception of some toxins, they are inactivated by cooking and thermal processing of foods. Chlorine bleach solutions inactivate botulinum toxin, viruses, and vegetative bacteria on surfaces and in water but do not destroy protozoan parasites, mycotoxins, or ricin [6, 7].

Bacterial spores are much more resistant to environmental stress, including heat, desiccation, and sanitizers [8]. *Bacillus anthracis* spores can survive pasteurization and other thermal processing methods [9]. Autoclaving with steam and pressure (135 °C, 217.2 kPa) for 40 min is generally effective in destroying all pathogens in medical waste. However, heat-resistant spores in building debris were completely destroyed only by two rounds of autoclaving [10]. Formaldehyde (final concentration of 5%) for 1–4 days can kill *B. anthracis* spores in liquid manure and sewage sludge (http://www.fas.org/nuke/intro/bw/whoemczdi986.htm).

Ozone and ultraviolet (UV) light can also kill pathogens but high concentrations of organic matter in foods reduce their effectiveness significantly [11–13].

Chemical warfare agents can be inactivated by oxidizing agents such as hypochlorite and peroxides and by hydrolysis under alkaline or acidic conditions. Degradation products are usually less toxic than the parent compounds, but in some cases further treatment is necessary [14, 15]. Industries using toxic industrial chemicals have developed procedures to deal with accidental spills and releases of these chemicals.

Radionuclides cannot be destroyed or inactivated. There are some methods, such as microfiltration and the use of magnetic particles to remove radionuclides from foods, which decrease the levels of contamination [16, 17] Following the Chernobyl accident,

some of these procedures were used to remove radioisotopes in milk. Some processing methods significantly reduce radioactivity in edible parts of foods. For example, processing of milk into butter and cheese significantly reduces radiostrontium levels because this isotope partitions primarily into the aqueous fraction [18]. These methods would still leave radioactive materials that required disposal.

## 3 FATE OF CONTAMINATED FOOD DURING DISPOSAL

### 3.1 Food

The food matrix itself consists of organic compounds that would be easily degraded in landfills, WWTPs, or incinerators. Since foods contain high moisture levels, their decomposition will produce relatively large amounts of leachate and may rapidly deplete oxygen and increase acidity in landfills. Some liquids with a high organic load (such as milk) may disrupt microbial processes in activated sludge tanks and therefore may be added directly to an anaerobic digester in a wastewater treatment plant.

### 3.2 Biological Agents

MSW landfills and WWTPs) regularly receive pathogenic bacteria, parasites, and viruses in human excreta, pet waste, disposable diapers, and spoiled foods. These are not a problem for well-run disposal facilities. But the presence of some bioterrorist agents in a large volume of food may present risks to workers and to public health if the agents are not inactivated or contained during the disposal process. Data are available on fate of some microorganisms under different disposal scenarios but few studies have investigated the fate of bioterrorist threat agents.

Bacteria, viruses, and prions can attach to soil particles and potentially to landfill materials and may survive for extended periods in landfills [19–22]. Depending on the organism and landfill conditions, pathogens may also be carried in liquids that percolate down through the landfill material (leachate).

Viruses appear to be the least hardy pathogens in landfills. No infective enteric viruses were cultured from fecally contaminated disposable diapers buried in landfills 2–10 years previously [23]. Hepatitis A virus and poliovirus survived more than 3 months in diapers and in landfill leachate at 5 °C but were inactivated within a month at 40 °C [24]. Viruses also persist in soil longer at cooler temperatures and when they adsorb to soil particles, but landfill temperatures are usually in the range of 40–50 °C [19]. Enteric vegetative bacteria appear to survive longer than viruses in landfills with significant numbers of fecal organisms detected in 9–10-year-old landfill samples. Lysimeter studies with simulated refuse showed that survival of bacteria was related to rainfall, refuse content, temperature, and toxicity of leachate. Spores, however, are very resistant to environmental stress and are known to survive for centuries in soils [8].

Pathogens may attach to solid particles during wastewater treatment and settle into sludge. Size and surface properties of microbes as well as pH, ionic strength, and polyvalent cation concentrations in the matrix determine attachment to particles [25]. WWTPs using only primary treatment remove about 12% of *E. coli*, 27% of *Cryptosporidium* oocysts, and negligible amounts of viruses indicating that many pathogens do not bind well to larger particles in settling tanks [26].

Some pathogens are destroyed during aerobic and anaerobic digestion of secondary/tertiary treatment processes but others survive typical wastewater treatment and are present in effluent and/or biosolids [27]. Chlorination and UV light can disinfect effluent before discharge but neither completely inactivate spores, oocysts, and all viruses [28]. Advanced processes, particularly chemical lime treatment combined with chlorination, can drastically reduce levels of bacteria, viruses, and parasitic oocysts in sludge [29].

During the outbreak of foot-and-mouth disease (FMD) in 2001 in the Netherlands, milk was illegally discharged into the sewer system. Since the virus might survive in WWTP and be present in effluent, a quantitative risk assessment for FMD virus transmission to cattle drinking surface water was conducted. Based on available data and estimates for water and virus consumption by cows, it was concluded that discharge of contaminated milk into the sewer system could pose a high risk to cattle farms within 50 km of effluent discharge to surface waters [30].

According to the EPA, more than 90% of medical waste that may contain infectious agents is currently incinerated because temperatures in properly run incinerators are hot enough to destroy all pathogens and toxins. Spore-forming bacteria can be killed within 30 min at 150 °C while other bacteria and viruses are inactivated at temperatures of $<100$ °C. However, an assessment by the EPA of the effectiveness of a medical waste incinerator in destroying heat-resistant bacterial spores demonstrated that some spores may survive in porous or moist materials where microenvironments do not reach the target temperature. In most cases, incineration caused $>6$ log kill of added spores but in some cases only about a 3 log kill occurred [31].

### 3.3 Chemical Agents

Most chemical warfare agents and toxic industrial chemicals would be considered hazardous and food contaminated with them should be sent to hazardous waste landfills or incinerated. However, only about 21 commercial hazardous waste landfills and about 28 hazardous waste incinerators (that normally accept off-site generated wastes) are currently operating in the United States. Disposal of contaminated food in these hazardous waste facilities may not be a practical option due to distance from the contamination incident, volume of the food, and the need for rapid disposal.

Physical and chemical properties of chemical agents deposited in MSW landfills or WWTP are important in determining whether they are volatilized, remain in aqueous or solid phases, or are inactivated by abiotic or biological reactions. Some studies on the behavior of chemical agents have been conducted in aqueous and soil systems but very limited information is available on the phase and fate of chemical agents in landfills and WWTP [32]. Although microbes possess enzymes that can degrade some chemical agents, it is not known whether they would significantly detoxify these agents under natural conditions in a landfill or WWTP [33].

Phase distribution and fate of some potential chemical terrorist agents in a landfill was modeled using Model for Organic Chemicals in Landfills (MOCLA)) [34]. Input parameters for the model include physical and chemical properties of the agents and landfill conditions derived from field data. The expected behavior of other chemical agents in landfills was estimated using MOCLA with similar landfill conditions and physicochemical properties obtained from the literature or estimated by EPI Suite v. 3.20 (Table 2).

According to MOCLA, over 90% of most chemical agents, with the exception of sodium fluoroacetate, the cyanides, Amiton (VG), and VM would be distributed to the solid phase. Most of the remainder would be present in aqueous phase (leachate) with a negligible fraction in the gaseous phase. Even though a large fraction of most agents would be sorbed to the solid phase and therefore presumably be immobile, this does not guarantee that landfill disposal of these agents is safe. It merely represents the phase distribution of the chemicals remaining in a landfill. To address the total risk, the fate of the chemical agents, including transport and degradation, must also be considered.

MOCLA calculates the fate of chemicals in a landfill, including advective transport of volatilized agents into the landfill gas collection system and through the soil cover, diffusive transport of volatilized agents through the soil cover, diffusive transport of soluble and volatilized agents through the composite liner, transformation of aqueous agents by biotic and/or abiotic mechanisms, and transport of soluble agents into the leachate collection system. A general half life of these compounds, obtained from EPI suite, was used in these simulations. This parameter includes oxidation/reduction, hydrolysis, and other reactions. Carbon disulfide and furan are predicted to move through landfills by gas-phase advection and according to Table 2, nearly 60 % of the initial amount would disappear within 5 years. At the end of landfill operations and 30 years of postclosure care, little of these chemicals would remain. However, attention should be directed to the gas monitoring/collection wells.

MOCLA predicts that the cyanide agents will move through liquid-phase advection. Their disappearance rates are relatively slow due to their longer hydrolysis half life and lower Henry's law constant. Nearly 90% would remain after 5 years with about 50% still present after 30 years. Leachate should be monitored for these compounds and properly treated.

For most of the other chemicals, MOCLA indicates that hydrolysis will be the primary fate. Blister agents and most of the nerve agents degrade so rapidly that more than 95% of these chemicals would disappear from a landfill within 5 years. However, information is also needed on the fate of hydrolysis products. Previous studies have reported that some environmentally persistent hydrolysates, lewisite oxide and EA 2192 from VX, are highly toxic to mammals [35].

Thallium and other heavy metals are likely to persist for a long time in landfills and are known to concentrate in biosolids of WWTP.

Fugacity-based analytical models can be used to predict the partitioning, transport, and transformation processes of organic chemicals in an activated-sludge wastewater treatment plant. EPA developed the Sewage Treatment Plant Fugacity Model (STPWIN) in EPI Suite v.3.20 to predict the multiphase partitioning and fate of chemicals in a sewage treatment plant (http://www.epa.gov/opptintr/exposure/pubs/episuite.htm).

STPWIN was used to estimate the fate of chemical terrorist agents (Table 2). Most of the carbon disulfide and some of the furan would be volatilized while much of the fentanyl would be adsorbed on sludge particles. Microbes would degrade substantial amounts of the blood agents, some nerve agents, and warfarin. However, the model indicated that less than 30% of the blister agents and some nerve agents (GD, VG, VM and VX) would be removed and a large fraction of these chemicals would pass through the treatment plant intact and be present in effluent. Effluent would then require additional treatment to remove the residual chemicals.

The major drawback of the STPWIN model is that abiotic transformation is not included in calculations but many blister and nerve agents are known to hydrolyze in

**TABLE 2 Fate of Potential Chemical Terrorist Agents in Landfills and WWTP (estimated by MOCLA and STPWIN)**

| Chemical Agent | | Landfill Phase Distribution (%)* | | Remaining in Landfill (%)* | | Estimated Fate in WWTP (%) | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | In water | In solids | 0.5 yr | 5 yr | Bio degradation | Adsorption to sludge | Volatilized | Present in effluent |
| TICs | Carbon disulfide | 0.5 | 98.8 | 90.1 | 35.7 | 32.7 | 0.58 | 57.4 | 9.36 |
| | Furan | 1.3 | 98.8 | 90.1 | 35.2 | 75.89 | 0.35 | 17.59 | 6.17 |
| Blood Agents | Potassium (sodium) cyanide | 66.4 | 33.6 | 98.9 | 89.6 | 91.72 | 0.33 | 0 | 7.94 |
| | Sodium fluoro-acetate (1080) | 98.4 | 1.6 | 59.5 | 0.4 | 74.43 | 0.62 | 0.02 | 24.93 |
| Incapacitating Agent | Fentanyl | 0.01 | 99.99 | 93.9 | 53.1 | 21.02 | 28.56 | 0 | 50.41 |
| Anticoagulant | Wafarin | 0.1 | 99.9 | 93.3 | 50.1 | 48.12 | 2.56 | 0 | 49.32 |
| Metals | Thallium and its salts | 7.6 | 92.4 | 99.4 | 94.3 | | | | |
| Blister Agents | Sulfur mustard (H/HD) | 0.2 | 99.8 | 0 | 0 | 21.68 | 2.31 | 1.44 | 74.57 |
| | Lewisite (L) | 0.2 | 99.8 | 0 | 0 | 20.96 | 2.57 | 7.51 | 68.96 |
| Organo-phosphate Nerve Agents | Tabun (GA) | 5.9 | 94.1 | 0 | 0 | 74.46 | 0.62 | 0 | 24.92 |
| | Sarin(GB) | 6.8 | 93.2 | 0.5 | 0 | 74.34 | 0.62 | 0.17 | 24.87 |
| | Soman (GD) | 0.6 | 99.4 | 72.9 | 4.2 | 20.83 | 1.65 | 0.21 | 77.30 |
| | GE | 3.5 | 96.5 | 7.3 | 0 | 74.32 | 0.63 | 0.23 | 24.82 |
| | Cyclosarin (GF) | 0.8 | 99.2 | 52.9 | 0.2 | 74.55 | 0.72 | 0.18 | 24.56 |
| | Amiton (VG) | 16.5 | 83.5 | 97.0 | 73.6 | 20.81 | 1.62 | 0 | 87.56 |
| | VM | 30.1 | 69.9 | 93.6 | 51.7 | 20.63 | 1.50 | 0 | 87.87 |
| | VX | 9.5 | 90.5 | 66.4 | 1.7 | 21.22 | 1.88 | 0 | 76.90 |

*Some data from Reference [34].

aqueous systems with half-lives on the order of minutes and days. Some hydrolysis products are also toxic. Biodegradation rate is also a key parameter in this model but little information on the half-life of most chemical agents is available. Half lives for these chemicals were estimated using BIOWIN and the EPA draft method but any inaccuracy strongly affects STPWIN estimates of removal efficiency. The model also assumes complete mixing in the tanks fails to recognize the existence of layers or blankets of settled sludge.

Hazardous wastes can be burned in specially designed incinerators that operate at higher temperatures than medical and municipal waste incinerators. A typical incinerator consists of a gas powered rotary kiln maintaining a temperature $>980\,^{\circ}C$ and an afterburner with a temperature $<1200\,^{\circ}C$. Gases from the afterburner pass through an air pollution control system to remove particulates and other pollutants [36].

Incineration has been used by the US Army as a proven and reliable method for destroying the stockpile of chemical nerve and blister agents [37]. The ash and slag produced during incineration are sent to a hazardous waste landfill and emissions from the stacks pass through a pollution abatement system. A model simulation of destruction of chemical agents showed that, based on the incinerability indexes, an incinerator should be able to destroy chemical warfare agents easily and efficiently [38].

### 3.4 Radiological Agents

Concentration of radioactivity and the isotopes present will determine disposal options for contaminated food. For radioisotopes with short half-lives, contaminated food may be stored securely until radioactivity decayed to very low levels.

WWTP and MSW landfills may be acceptable sites for disposal of foods containing very low levels of radioactivity. The Nuclear Regulatory Commission permits discharge of water soluble radionuclides into sanitary sewer systems within certain limits (Table 1). If food contained greater levels of radioactivity or certain more toxic isotopes, alternative methods of disposal would be needed.

Low levels of radioactivity, from naturally occurring isotopes, industrial waste, and excreta of people undergoing medical procedures, normally pass through WWTP. Some isotopes ($^{131}I$, $^{60}Co$, $^{241}Am$, $^{40}K$, $^{226}Ra$, $^{228}Ra$, $^{89}Sr$, and $^{201}Tl$) are known to settle out with sludge particles and others have been reported to pass through the plant and are present in the discharged effluent [39, 40]. High levels of radionuclides, including $^{60}Co$ used in cancer treatment and $^{241}Am$ in industrial sources, were detected in sewage sludge in the past. In some cases, diluted radioactive materials were discharged into the sanitary system and diluted by millions of liters of liquid from other sources but radioisotopes became concentrated in sludge necessitating expensive cleanup operations [41].

Low level solid radioactive waste in the United States is normally deposited in one of the three operational radioactive waste landfills (Utah, Washington, and South Carolina). Both the concentration of the radionuclides and half-lives of the isotopes determine whether wastes are permitted in these landfills (http://www.nrc.gov/reading-rm/doc-collections/cfr/part061/part061-0055.html).

Potential radiological impact of disposal of large quantities of very low level solid radioactive waste (not more than 4 MBq/metric ton of $\beta/\gamma$ activity in $10^8$ kg/yr) in municipal landfills has been assessed by the UK government [42]. The assessment considered potential exposure of workers at a landfill site, the impact if the leachate from a landfill were directly deposited in a river, and problems that might occur after closing

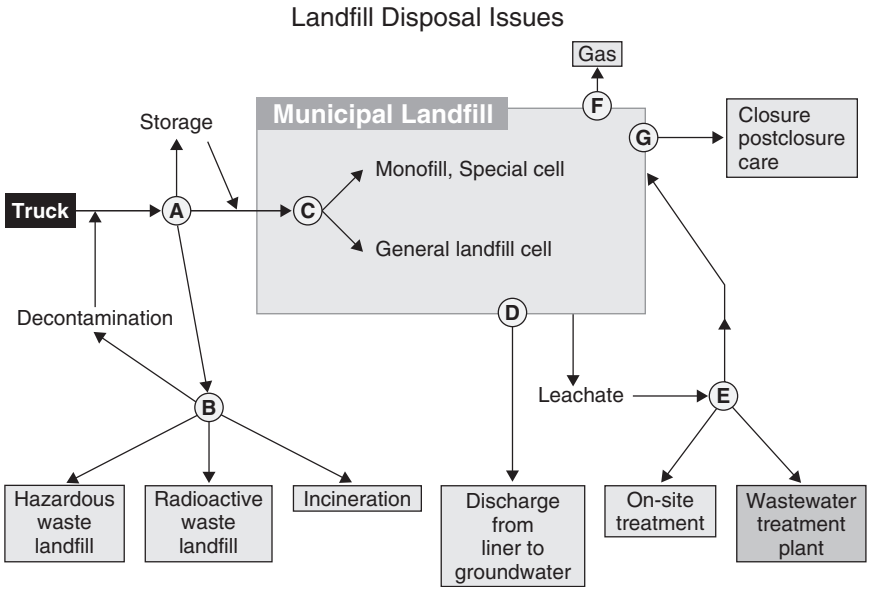



**FIGURE 1** Landfill disposal issues

the site. Results from the study indicated that disposal of $^{3}H$, $^{36}Cl$, $^{90}Sr$, $^{238}U$, $^{239}Pu$ or $^{241}Am$ in landfills at this rate would be safe but disposal of $^{14}C$, $^{60}Co$, $^{137}Cs$, $^{226}Ra$ and $^{232}Th$ may not be safe.

Incineration prior to disposal may be useful in reducing the expected large volume of contaminated food. Incineration does not destroy radioactivity but eliminates organic material, and radioisotopes are then present in a much smaller volume of residual ash, fused slag, fly ash, and volatile compounds. Expected partitioning of different isotopes has been modeled (Table 1). Radioactive and toxic materials can be removed from gas emissions by scrubber filters and will require disposal. The radioactive ash can be immobilized in cement and then transported to a disposal or storage site [43]. Treatment capacities of controlled air incinerators for low level radioactive waste range from 200 to 700 kg/h.

## 4 CRITICAL NEEDS

Landfill operators have long-term responsibility and liability for their sites and depend on the good will of their neighbors and government agencies. WWTPs operate continuously and, as part of the public health system, have a very limited ability to refuse or redirect liquids that they receive. Neither would willingly accept foods containing terrorist agents without sufficient information about survival and fate of the agents. Escape of the agent from a landfill through gases, leachate, or leakage into groundwater is a major concern (Figure 1) as are the costs of increased monitoring for exotic agents, liability issues, risks to workers, and post-closure care and land use. If an agent is not degraded in a WWTP, it will be present in the effluent discharged to surface waters and/or in the biosolids normally spread on agricultural land. An agent may disrupt the metabolic activities of the bacteria performing the important tasks of degrading organic compounds, producing

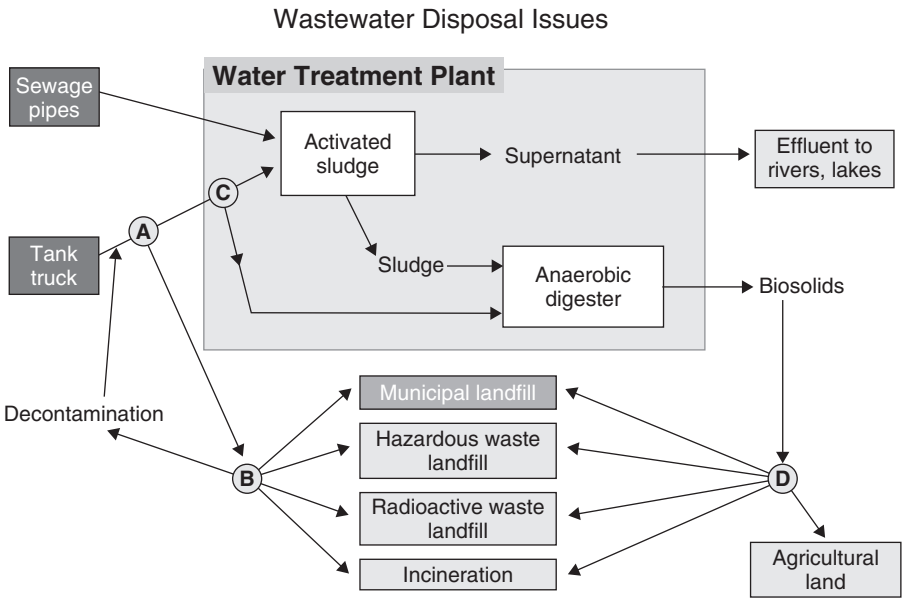



**FIGURE 2** Wastewater disposal issues

methane, and removing nitrogen from wastewater. Vapors or aerosols from activated sludge tanks may present a risk to workers (Figure 2).

Perceived risk for some agents may be greater than the real risk but such issues must be addressed. Despite scientific evidence, neither the waste disposal operators nor the public may trust that the agent has been completely inactivated. Public health and public relations will require long-term monitoring to demonstrate that risk is minimal.

Critical needs include the following:

- greater coordination and communication between federal and state agencies that manage and regulate food and those that manage the environment and security;
- development of regulations, policies, and procedures to define how terrorist wastes are to be managed, where they can be disposed, how they will be monitored, and what liabilities associated with managing these wastes will be assumed by the government and by industry;
- more information is needed regarding the fate of terrorist agents and their degradation products in conventional pollution control systems, such as landfills and WWTPs, so that rational decisions can be made regarding the impacts of accepting contaminated foods;
- planning by pollution control facilities to ensure worker safety and address the potential for inadvertent releases to ensure public safety and protection of the environment;
- increased communication among all stakeholders including food companies, pollution control facilities, renderers, transportation industry, and diagnostic laboratories;
- risk management strategies must be developed to communicate openly and honestly with the public.

## 5 RESEARCH DIRECTIONS

Research on the fate of various terrorist agents in pollution control systems should be investigated soon before the society and disposal industry are faced with a daunting disposal problem. A sound technical basis is needed so that rational decisions can be made about the disposal of large volumes of food contaminated by terrorists.

Future research should be directed to the following:

- investigation of the fate of various agents in different food matrices under conditions similar to those encountered in landfills and WWTP;
- improved analytical methods for various agents in different food matrices;
- feasible methods for decontaminating large volumes of contaminated food;
- effective risk communication strategies.

## REFERENCES

1. Burger, L. L. (1995). *A Chemical Basis for the Partitioning of Radionuclides in Incinerator Operation*, PNL-10364, UC-601, U.S. Department of Energy.
2. Wein, L. M., and Liu, Y. F. (2005). Analyzing a bioterror attack on the food supply: the case of botulinum toxin in milk. *Proc. Natl. Acad. Sci. U.S.A.* **102**, 9984–9989.
3. Raber, E., Carlsen, T. M., Folks, K. J., Kirvel, R. D., Daniels, J. I., and Bogen, K. T. (2004). How clean is clean enough? Recent developments in response to threats posed by chemical and biological warfare agents. *Int. J. Environ. Health Res*. **14**, 31–41.
4. Doyle, M. E., and Mazzotta, A. S. (2000). Review of studies on the thermal resistance of salmonellae. *J. Food Prot*. **63**, 779–795.
5. Rose, L. J., Rice, E. W., Jensen, B., Murga, R., Peterson, A., Donlan, R. M., and Arduino, M. J. (2005). Chlorine inactivation of bacterial bioterrorism agents. *Appl. Environ. Microbiol*. **71**, 566–568.
6. Henghold, W. B. (2004). Other biologic toxin bioweapons: ricin, staphylococcal enterotoxin B, and trichothecene mycotoxins. *Dermatol. Clin*. **22**(3), 257–262.
7. Villar, R. G., Elliott, S. P., and Davenport, K. M. (2006). Botulism: the many faces of botulinum toxin and its potential for bioterrorism. *Infect. Dis. Clin. North Am*. **20**, 313–327.
8. Nicholson, W. L., Munakata, N., Horneck, G., Melosh, H. J., and Setlow, P. (2000). Resistance of *Bacillus* endospores to extreme terrestrial and extra-terrestrial environments. *Microbiol. Mol. Biol. Rev*. **64**, 548–572.
9. Novak, J. S., Call, J., Tomasula, P., and Luchansky, J. B. (2005). An assessment of pasteurization treatment of water, media, and milk with respect to *Bacillus* spores. *J. Food Prot*. **68**, 751–757.
10. Lemieux, P., Sieber, R., Osborne, A., and Woodard, A. (2006). Destruction of spores on building decontamination residue in a commercial autoclave. *Appl. Environ. Microbiol*. **72**, 7687–7693.
11. Blatchley, E. R., Meeusen, A., Aronson, A. I., and Brewster, L. (2005). Inactivation of *Bacillus* spores by ultraviolet or gamma radiation. *J. Environ. Eng*. **131**, 1245–1252.
12. Lytle, C. D., and Sagripanti, J. L. (2005). Predicted inactivation of viruses of relevance to biodefense by solar radiation. *J. Virol*. **79**, 14244–14252.
13. Mahapatra, A. K., Muthukumarappan, K., and Julson, J. L. (2005). Applications of ozone, bacteriocins and irradiation in food processing: a review. *Crit. Rev. Food Sci. Nutr*. **45**, 447–461.

14. Talmage, S. S., Watson, A. P., Hauschild, V., Munro, N. B., and King, J. (2007). Chemical warfare agent degradation and decontamination. *Curr. Org. Chem*. **11**, 285–298.
15. Wagner, G. W., and Yang, Y. C. (2002). Rapid nucleophilic/oxidative decontamination of chemical warfare agents. *Ind. Eng. Chem. Res*. **41**, 1925–1928.
16. Gao, Y., Zhao, J., Zhang, G. H., Zhang, D., Cheng, W. W., Yuan, G. Q., Liu, X. J., Ma, B. Z., Zeng, J. H., and Gu, P. (2004). Treatment of the wastewater containing low-level Am-241 using flocculation-microfiltration process. *Sep. Purif. Technol*. **40**, 183–189.
17. Navratil, J. D. (2001). Pre-analysis separation and concentration of actinides in groundwater using a magnetic filtration/sorption method I. background and concept. *J. Radioanal. Nucl. Chem*. **248**, 571–574.
18. Patel, A. A., and Prasad, S. R. (1993). Decontamination of radioactive milk—a review. *Int. J. Radiat. Biol*. **63**, 405–412.
19. Davies, C. M., Logan, M. R., Rothwell, V. J., Krogh, M., Ferguson, C. M., Charles, K., Deere, D. A., and Ashbolt, N. J. (2006). Soil inactivation of DNA viruses in septic seepage. *J. Appl. Microbiol*. **100**, 365–374.
20. Ma, X., Benson, C. H., Mckenzie, D., Aiken, J. M., and Pedersen, J. A. (2007). Adsorption of pathogenic prion protein to quartz sand. *Environ. Sci. Technol*. **41**, 2324–2330.
21. Morrow, J. B., Stratton, R., Yang, H. H., Smets, B. F., and Grasso, D. (2005). Macro- and nanoscale observations of adhesive behavior for several *E. coli* strains (O157:H7 and environmental isolates) on mineral surfaces. *Environ. Sci. Technol*. **39**, 6395–6404.
22. Rzezutka, A., and Cook, N. (2004). Survival of human enteric viruses in the environment and food. *FEMS Microbiol. Rev*. **28**, 441–453.
23. Huber, M. S., Gerba, C. P., Abbaszadegan, M., Robinson, J. A., and Bradford, S. M. (1994). Study of persistence of enteric viruses in landfilled disposable diapers. *Environ. Sci. Technol*. **28**, 1767–1772.
24. Gray, M., Deleon, R., Tepper, B. E., and Sobsey, M. D. (1993). Survival of hepatitis-A virus (Hav), poliovirus-1 and F-specific coliphages in disposable diapers and landfill leachates. *Water Sci. Technol*. **27**, 429–432.
25. Crockett, C. S. (2007). The role of wastewater treatment in protecting water supplies against emerging pathogens. *Water Environ. Res*. **79**, 221–232.
26. Payment, P., Plante, R., and Cejka, P. (2001). Removal of indicator bacteria, human enteric viruses, *Giardia* cysts, and *Cryptosporidium* oocysts at a large wastewater primary treatment facility. *Can. J. Microbiol*. **47**, 188–193.
27. Shannon, K. E., Lee, D. Y., Trevors, J. T., and Beaudett, L. A. (2007). Application of real time quantitative PCR for the detection of selected bacterial pathogens during municipal wastewater treatment. *Sci. Total Environ*. **382**, 121–129.
28. Blatchley, E. R., Gong, W. L., Alleman, J. E., Rose, J. B., Huffman, D. E., Otaki, M., and Lisle, J. T. (2007). Effects of wastewater disinfection on waterborne bacteria and viruses. *Water Environ. Res*. **79**, 81–92.
29. Rose, J. B., Huffman, D. E., Riley, K., Farrah, S. R., Lukasik, J. O., and Hamann, C. L. (2001). Reduction of enteric microorganisms at the upper Occoquan Sewage Authority water reclamation plant. *Water Environ. Res*. **73**, 711–720.
30. Schijven, J., Rijs, G. B. J., and Husman, A. (2005). Quantitative risk assessment of FMD virus transmission via water. *Risk. Anal*. **25**, 13–21.
31. Wood, J. (2006). Thermal destruction of *Bacillus anthracis* surrogates in a pilot scale incinerator. *Air and Waste Management Association, 99th Annual Conference*, New Orleans, paper #328, 12.

32. Kingery, A. F., and Allen, H. E. (1995). The environmental fate of organo-phosphorus nerve agents: a review. *Toxicol. Environ. Chem*. **47**, 155–184.

33. Singh, B. K., and Walker, A. (2006). Microbial degradation of organophosphorus compounds. *FEMS Microbiol. Rev*. **30**, 428–471.

34. Bartelt-Hunt, S. L., Barlaz, M. A., Knappe, D. R., and Kjeldsen, P. (2006). Fate of chemical warfare agents and toxic industrial chemicals in landfills. *Environ. Sci. Technol*. **40**, 4219–4225.

35. Munro, N. B., Talmage, S. S., Griffin, G. D., Waters, L. C., Watson, A. P., King, J. F., and Hauschild, V. (1999). The sources, fate, and toxicity of chemical warfare agent degradation products. *Environ. Health Perspect*. **107**, 933–974.

36. Santoleri, J. J., Reynolds, J., and Theodore, L. (2000). *Introduction to Hazardous Waste Incineration*. Wiley-Interscience, New York.

37. National Research Council (U.S.) (2007). Committee on review of chemical agent secondary waste disposal and regulatory requirements. *Review of Chemical Agent Secondary Waste Disposal and Regulatory Requirements*. National Research Council, Washington, DC.

38. Denison, M. K., Sadler, B. A., Montgomery, C. J., Sarofim, A. F., Bockelie, M. J. (2004). Computational modeling of a chemical liquid incinerator chamber. *IT3'04 Conference, May 10–14, 2004*, Phoenix, Arizona.

39. Bastian, R. K., Bachmaier, J. T., Schmidt, D. W., Salomon, S. N., Jones, A., Chiu, W. A., Setlow, L. W., Wolbarst, A. B., Yu, C., Goodman, J., and Lenhart, T. (2005). Radioactive materials in biosolids: national survey, dose modeling, and publicly owned treatment works (POTW) guidance. *J. Environ. Qual*. **34**, 64–74.

40. Martin, J. E., and Fenner, F. D. (1997). Radioactivity in municipal sewage and sludge. *Public Health Rep*. **112**, 308–316.

41. General Accounting Office (US). (1994). *Radionuclides at Sewerage Treatment Plants*, GAO/RCEL-94-133. GAO, Gaithersburg, MD.

42. Chen, Q. Q., Kowe, R., Mobbs, S. F., and Jones, K. A. (2007). *Radiological Assessment of Disposal of Large Quantities of Very Low Level Waste in Landfill Sites*, http://www.hpa.org.uk/radiation/publications/hpa_rpd_reports/2007/hpa_rpd_020.pdf.

43. International Atomic Energy Agency (2004). *Predisposal Management of Organic Radioactive Waste*, (IAEA-TECHDOC-427), IAEA, Vienna, Austria.

## FURTHER READING

Clark, B., Henry, G. L. H., and Mackay, D. (1995). Fugacity analysis and model of organic chemical fate in a sewage treatment plant. *Environ. Sci. Technol*. **29**, 1488–1494.

Food Safety Department, World Health Organization (2002). *Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems*, http://www.who.int/foodsafety/publications/general/en/terrorist.pdf.

International Atomic Energy Agency (2006). *Application of Thermal Technologies for Processing of Radioactive Waste*, (IAEA-TECHDOC-1527), IAEA, Vienna, Austria.

Lemieux, P., Thorneloe, S., Nickel, K., and Rodgers, M. (2007). *A Decision Support Tool (Dst) for Disposal of Residual Materials Resulting from National Emergencies*, http://www.epa.gov/nhsrc/pubs/paperDSTDispResidual101007.pdf.

Lund, B. M., Baird-Parker, T. C., and Gould, G. W. (2000). *The Microbiological Safety and Quality of Food*. Aspen Publishers Inc., Gaithersburg, MD.

Palmisano, A. C., and Barlaz, M. A. eds (1996). *Microbiology of Solid Waste*. CRC Press, New York.

# CARCASS DISPOSAL OPTIONS

ABBEY L. NUTSCH AND JUSTIN J. KASTNER
*Kansas State University, Manhattan, Kansas*

## 1 INTRODUCTION

The US agricultural sector represents one of the world's most bountiful and economically valuable food and fiber systems. Animal agriculture comprises a substantial portion of the overall agricultural sector, with the value of US livestock, poultry, and their products sold in 2002 amounting to over $105 billion [1]. However, as delineated in Homeland Security Presidential Directive 9 [2], "The United States agriculture and food systems are vulnerable to disease, pest, or poisonous agents that occur naturally, are unintentionally introduced, or are intentionally delivered by acts of terrorism." The enormity, complexity, and diversity of US animal agriculture systems magnify a number of agricultural security challenges, one of which is carcass disposal. Whether at the hand of accidental disease entry, the weather, or an act of bioterrorism, widespread livestock deaths pose daunting carcass disposal challenges that, if not met quickly and effectively, can spiral into major food agricultural security problems and result in devastating economic losses. This article provides an overview of the options, considerations, and challenges associated with the disposal of large numbers of animal carcasses.

## 2 BACKGROUND

US livestock inventories in 2002 included more than 95 million cattle and calves, over 60 million hogs and pigs, and more than 8 billion broilers and other meat-type chickens [1]. Inevitably, routine animal-production mortalities occur and, as a result of the sheer scale of operations, equate to billions of pounds annually. For example, in 2002, routine mortalities requiring disposal totaled approximately 3 billion pounds [3]. This volume could be multiplied many times over in the event of natural disasters or the intentional or accidental introduction of foreign animal disease. The ever-increasing concentration of modern animal-production operations, combined with the tremendous mobility of food-animal populations, accentuates the country's vulnerability to high death losses due to disease outbreaks. Rapid depopulation and disposal are integral parts of effective disease eradication efforts.

In recent years, various incidents have served to spotlight the challenges associated with carcass disposal; perhaps the most notable and reported-upon is the 2001 foot and mouth disease (FMD) outbreak in the United Kingdom, which saw the disposal of more than 6.5 million animals, primarily sheep [4]. Examples in the United States include outbreaks of low pathogenic avian influenza (AI) in Virginia in 2002, exotic Newcastle disease (END) in southern California in 2002–2003, and the ongoing effort to address chronic wasting disease (CWD) in deer and elk populations. Additionally,

highly pathogenic AI has emerged as a global issue of concern, with more than 40 countries having reported outbreaks of H5N1 in poultry as of early 2008 [5]. The threat of this disease has stimulated a host of planning efforts directed toward responding to potential outbreaks, including the disposal of infected flocks.

Common methods of carcass disposal include, but are not limited to, burial, landfilling, incineration, composting, rendering, and alkaline hydrolysis. A brief overview of these alternatives, including advantages and disadvantages, is provided in this article. More detailed summaries of these and other methods are available from several sources provided in "References" and "Further Reading" [6].

## 3 PLANNING CONSIDERATIONS

With respect to disease or disaster incidents involving animal agriculture, a rapid and effective response is vital to minimizing livestock losses, economic impacts, and public health hazards. Strategies for carcass disposal—especially on a large scale—require preparation well in advance of an emergency in order to maximize the efficiency of response. The roles and responsibilities at the federal level for decontamination and disposal in response to animal, crop, and food incidents have been described in the document "Federal Food and Agriculture Decontamination and Disposal Roles and Responsibilities" [7]. This document is in accordance with the strategies outlined in the US National Response Plan (and its successor, the National Response Framework), and provides additional detail with respect to the key processes, and responsible parties, involved in the disposal of animal carcasses during an animal health emergency. As this document states, "appropriate decontamination and disposal decisions, and the resulting operations, involve multidisciplinary expertise and teamwork" [7, p. 9].

Managing disease eradication efforts is a complex endeavor requiring coordination and cooperation among many parties. Realization of a rapid response requires emergency management plans that are based on a thorough understanding of disposal alternatives that are both appropriate and available in various circumstances. Effective means of carcass disposal are essential regardless of the cause of mortality, but are perhaps most crucial for disease eradication efforts. It may seem straightforward to develop a generic, stepwise disposal-option hierarchy, outlining the most and least preferred methods of disposal. However, for a multidimensional enterprise such as carcass disposal, generic hierarchies may be of limited value as they may not fully capture and systematize the relevant dimensions at stake (e.g. environmental considerations, disease agent considerations, availability of the technology, and cost). Even with a disposal-option hierarchy that, for example, ranks the most environmentally preferred disposal technologies for a particular disease, difficulties arise when the most preferred methods are not available or when capacity has been exhausted. In these situations, decision makers may have to consider less preferred options. In such a scenario (one that is likely to occur in the midst of an emergency), there are tremendous benefits of being armed with a comprehensive understanding of an array of carcass disposal technologies. During times of emergency, it is possible that no single method of disposal will be sufficient and, whether ideally suited or not, multiple disposal options may be necessary.

Numerous issues will impact decisions about large-scale carcass disposal efforts. For any policy designed to provide decision-making guidance, it is necessary to identify the numerous factors that must be considered. The selection of an appropriate disposal

option must incorporate the scientific basis for the technology along with the associated needs of security, transportation, location, and decontamination. An understanding of the regulatory factors, the importance of cooperation and coordination among stakeholders, and the consideration of public opinion are all keys to successfully handling a carcass disposal emergency.

## 4 OVERVIEW OF DISPOSAL ALTERNATIVES

Within the limitations of this article, it is possible to provide only a brief overview of various carcass disposal alternatives. For additional details the reader is referred to "References" and "Further Reading" of this article. Because additional resource materials are continuously being developed, the interested reader is also encouraged to seek newly available materials that may not be reflected in these lists. Following are key attributes, advantages, and disadvantages associated with various disposal options.

### 4.1 Burial

Burial has historically been a common means of disposing of animal carcasses, particularly for routine mortality losses. On-site burial continues to be identified by various state and local authorities as a preferred means of carcass disposal in the event of a disease eradication effort. The suitability of a site for burial can be assessed using a host of characteristics—soil properties; slope or topography; hydrological properties; proximity to water bodies, wells, public areas, roadways, dwellings, residences, municipalities, and property lines; accessibility; and so on. Although many sources concur that these characteristics are important, the criteria for evaluating each can vary considerably among different localities (see Chapter 1 Burial, Appendix A1, in [6]). In some states, geographic information system technology has been used to preidentify sites that are suitable or unsuitable for burial [8–10].

Various sources have estimated the land area that may be necessary for burial (see Chapter 1 Burial, Appendix A2 in [6]), as well as the resources required for excavation [6, 11]. Volume estimates range from 1.2 to 3.5 $yd^3$ per mature cattle carcass (with one adult bovine approximately equivalent to five adult sheep or five mature hogs). One source estimated that an excavation volume of about 92,000 $yd^3$ would be required to bury 30,000 head of cattle; assuming an excavation depth of 8.5 ft, this would be equivalent to about 7 acres of land [12].

Burial as a carcass disposal option is cited as relatively economical, convenient, logistically simple, and relatively quick, as the necessary equipment is generally widely available and the technique is relatively straightforward. If performed on-site, it eliminates the need for transportation of potentially infectious material. These attributes have resulted in burial being a traditionally favored option for carcass disposal.

However, a key drawback of burial is the potential for negative short- and long-term environmental impacts resulting from the products of carcass decomposition. Although much of the pollutant load would likely be released during the earlier stages of decomposition, impacts could continue for many years [13]. Furthermore, the excavation of previous burial sites has demonstrated that carcass material can remain relatively intact in burial sites for very long periods of time, even decades [14, 15].

Other concerns relate to the potential for persistence of disease agents in the environment. Generally, the conditions of burial are thought to limit the survival of the majority of bacterial and viral organisms; however, precise survival times are unpredictable, and spore-forming organisms are known to survive in the environment for very long periods of time. Particular concern surrounds the agents known as *prions*, which are believed to be responsible for transmissible spongiform encephalopathies (TSEs) such as bovine spongiform encephalopathy (BSE) in cattle, scrapie in sheep, CWD in deer and elk, and Creutzfeldt–Jakob disease (CJD) in humans. These agents have been demonstrated to be highly resistant to inactivation processes effective against bacterial and viral disease agents [16], and the scrapie agent has been demonstrated to retain at least a portion of its infectivity following burial for 3 years [17].

The availability of burial as a viable disposal option may be limited by regulatory constraints, lack of sites with suitable geological and/or hydrological properties, or the fact that burial may be prohibitively difficult when the ground is wet or frozen. In some cases, the presence of an animal carcass burial site may negatively impact land value or options for future use. Lastly, as compared to some other disposal options, burial of carcasses does not generate a useable by-product of any value.

One permutation of the burial option is a mass burial site (that is, a site developed specifically for the burial of significant numbers of animal carcasses). The distinction between a large on-site burial location and a mass burial site is not necessarily clear and may simply be a matter of opinion. A mass burial site that employs a more sophisticated approach and incorporates containment measures similar to a landfill would perhaps more appropriately be termed an "*engineered mass burial site*". During the 2001 outbreak of FMD in the United Kingdom, six mass burial sites were created with a collective capacity of 3.5 million sheep carcasses; ultimately about 1.2 million carcasses were disposed in these sites [18]. As evidenced by the UK experience, such sites can play a critical role in disposal efforts during a time of emergency; however, hastily planned or inadequately assessed sites can create significant operational and management problems. There was tremendous public opposition to the use of these mass burial sites in the United Kingdom, sometimes even escalating to the point of violence and vandalism. Opposition was fueled by a failure of authorities to consult and communicate with surrounding communities and local regulatory bodies, as well as a lack of appropriate and thorough site assessments prior to commencing burial operations. If the burial of significant numbers of carcasses is anticipated in the event of an emergency—creating a de facto mass burial site—advanced planning and communication with all stakeholders will be essential.

### 4.2 Landfill

In many US states, disposal of animal carcasses in landfills is an allowed option. However, it may not be an available option, as individual landfill operators can decide whether or not to accept carcass material. Whether real or perceived, potential risks to public health from disposing of animal carcasses in landfills will likely be the most influential factor in the operator's decision to accept carcass material. Depending on the situation, the role of public perception and/or the degree of opposition to the use of landfills for disposal of animal carcass material may be significant or essentially negligible. For example, although landfill capacity could have accommodated 100% of the carcass mate-

rial requiring disposal during the 2001 UK FMD outbreak, only about 16% was disposed of via this route, primarily due to significant local opposition [13]. Conversely, the vast majority of carcass material disposed during the 2002 California END outbreak was disposed of by landfill with little public opposition.

During an emergency or instance of catastrophic loss, time is of the essence, and therefore landfills offer the advantage of disposal infrastructure that is preexisting and immediately available. Furthermore, the quantity of carcass material that can be disposed of via landfills can be relatively large. For example, over 3 million birds were depopulated during the 2002 END outbreak in southern California, with landfills serving as a primary means of disposal. In addition to carcass material, other outbreak-associated materials, such as eggs and litter, were also disposed through landfill.

Landfill sites will have been previously approved with the necessary environmental protection measures, thus representing a disposal option posing little risk to the environment. (Note that risks to the environment may vary depending on the type of landfill and may be greater for small arid landfills that rely on natural attenuation to manage waste by-products.) Another advantage of landfills is the fact that they are present in most locations (although proximity varies). The cost to dispose of carcasses by landfill has been referred to as both an *advantage and a disadvantage*, and would likely depend on the situation. Fees assessed by landfills for disposing of poultry during disease outbreaks in 2002 and 2003 were reported to be about $40–45/t [19]. However, the overall cost of landfill disposal of poultry during the 2002 outbreak of AI in Virginia was reported to be approximately $122/t, when costs of other equipment and transportation of carcass material were considered [20].

Even though disposal by landfill may be an allowed option, and a suitable landfill site may be located in close proximity, landfill operators may not be willing to accept animal carcasses. Additionally, because approval and development of a landfill site is lengthy, difficult, and expensive, landfill owners and planning authorities may not want to sacrifice domestic waste capacity to accommodate carcass material. As landfilling of carcasses represents a means of containment rather than of elimination, long-term management of the waste is required. Another disadvantage associated with landfill disposal is the potential spread of disease agents during transport of infected material to the landfill (a potential concern for any off-site disposal method).

Special procedures may be necessary at the landfill to prevent the spread of diseases. During the 2003 outbreak of END in southern California, the Riverside County California Waste Management Department developed a training video to educate landfill operators and employees on appropriate biosecurity and operational procedures to prevent disease spread [21]. The Virginia Department of Environmental Quality has also developed guidance materials for the disposal of poultry in landfills [22].

Carcass material infected (or potentially infected) with TSE agents may be of special concern. The United States Environmental Protection Agency (US EPA) has outlined recommended practices for disposal of carcasses potentially contaminated with CWD agents [23]. Various risk assessments have concluded that disposal of potentially TSE-infected carcasses in an appropriately engineered landfill site represents very little risk to human or animal health [24, 25]. However, because these agents are not well understood, research is ongoing to determine the mobility and survival of prions in landfill environments [26, 27].

### 4.3 Composting

Composting is a process of aerobic degradation of organic material by microbes; for optimal performance, it requires an appropriate balance of carbon and nitrogen sources, as well as appropriate oxygen and moisture conditions. As a means of carcass disposal, composting has increased in popularity with the decreased availability, increased cost, and/or environmental concerns associated with alternative methods. Composting is also attractive because it can be performed on-site, eliminating the need to transport infected or potentially infected material during a disease outbreak. Where large numbers of carcasses are concerned, composting is generally better suited to the disposal of small- to medium-sized carcasses (e.g. poultry and swine) than large carcasses (e.g. cattle). For disposing of routine mortalities, the use of composting is more common in poultry and hog production than in cattle production [3].

Considerations for the use of composting for disposing of animal carcasses have been summarized by various authors [6, 28–30]. Within the past decade, composting has been used to dispose of poultry during disease outbreaks in the United States and Canada; these experiences have provided valuable insights into the potential issues associated with composting during a disease eradication effort. In 2002, an outbreak of low pathogenic AI affected nearly 200 poultry farms (approximately 4.7 million birds) in Virginia [19, 31]. Composting was used with some success to dispose of a small percentage ($<1\%$) of the resulting carcasses [14]. However, this event highlighted the potential advantages of composting poultry, particularly in-house. In 2004, in-house composting was used to dispose of poultry carcasses resulting from an outbreak of low pathogenic AI on the Delmarva Peninsula (Maryland and Delaware); the outbreak was contained to three poultry farms, despite these operations being located in a dense poultry-production area [31]. In 2004, British Columbia, Canada experienced an outbreak of highly pathogenic AI; composting was used to dispose of approximately half of the 1.2 million birds impacted by the outbreak [30].

Researchers at Iowa State University recently completed an extensive 3-year investigation into the environmental impacts and biosecurity issues associated with composting of mortalities during a time of emergency [32]. During this study, 54 t of cattle carcasses were composted to assess the performance of various cover materials; the potential for soil, water, and air pollution, as well as the survival of the vaccine strains of viruses causing avian encephalomyelitis and Newcastle disease. Under the conditions of their study, the composting process inactivated both viruses within 1 week, regardless of the season of year or the cover material used. On the basis of the results of this project the researchers provide suggested guidelines for composting cattle mortalities during emergency situations. Their results suggest that composting can be a relatively biosecure process when performed properly.

### 4.4 Incineration/Thermal Methods

Thermal means of carcass disposal include open-air burning, fixed-facility incineration, and air-curtain incineration. Because carcasses are composed of approximately 70% water, they are somewhat challenging to incinerate, regardless of the method.

Open-air burning of carcasses—including the burning of carcasses on combustible heaps known as *pyres*—dates back to biblical times. As recently as 2001, it was used as a key means of disposal in a large-scale disease eradication effort, namely the 2001 outbreak of FMD in the United Kingdom [4]. During this outbreak, approximately 30% of

6 million carcasses were disposed of by open-air burning on some 950 burn sites; although some sites featured mass pyres, most were smaller, on-farm burns [18]. Open-air burning may be appealing as a means of disposing carcasses on-site, thereby avoiding the need to transport carcasses to an off-site disposal location. Open-air burning is labor and fuel intensive, can present environmental concerns and public perception issues, and can even precipitate mental health challenges in the agricultural community involved. During the 2001 UK FMD outbreak, carcasses burning on mass pyres "generated negative images in the media" and "had profound effects on the tourist industry" [18, pp. 7, 74]. Other disadvantages of open-air burning include the fact that it is dependent on favorable weather conditions, unsuitable for managing TSE-infected carcasses [33], and may be prohibited by environmental regulations.

Examples of fixed-facility incinerators include crematoria, small carcass incinerators at veterinary colleges, large waste incineration plants, on-farm carcass incinerators, and power plants. Unlike open-air burning and air-curtain incineration, fixed-facility incineration is wholly contained and, usually, highly controlled. Fixed-facility incinerators have been used in the United Kingdom to dispose of BSE-infected carcasses as well as rendered by-products from cattle carcasses considered to be at risk of BSE. Fixed-facility incineration is highly biosecure, as it is capable of inactivating agents of disease including TSEs. However, fixed-facility incinerators are expensive and difficult to operate and manage from a regulatory perspective. Most on-farm and veterinary-college incinerators are of insufficient capacity to be of value during carcass disposal emergencies, and larger industrial waste incinerators are typically not configured to handle carcasses as an input [33].

Air-curtain incineration involves equipment that fan-forces a mass of air through a manifold, thereby creating a "curtain" that traps smoke and significantly reduces the amount of pollutants released into the atmosphere. The process also provides a turbulent environment in which incineration is greatly accelerated—up to six times faster than open-air burning [34]. The process can be accomplished in-ground (trench burners or pit burners) or above-ground using fireboxes. Disposal of carcasses is a relatively new application for air-curtain incineration technology; it has traditionally been used for eliminating land-clearing debris, reducing clean wood waste for landfill disposal, and eliminating storm debris [19, 33].

Air-curtain incinerators have been used for carcass disposal in the wake of natural disasters in the United States [33], and were used to a small degree during the 2001 UK FMD outbreak [4, 18]. Air-curtain incinerators were used to dispose of more than 2000 t of poultry carcasses during the 2002 outbreak of AI in Virginia [14], and have been used in Colorado and Montana to dispose of animals infected with CWD [35]. Air-curtain incinerator capacity depends on the type of equipment and on-site management of the process; throughput capacity has been estimated to be approximately 4 to 6 t of carcasses per hour [34].

Air-curtain incineration is mobile, usually environmentally sound, and suitable for combination with debris removal (e.g. in the wake of a hurricane). However, air-curtain incinerators are fuel intensive (requiring not only a sufficient quantity, but also quality of fuel materials), and can be logistically challenging [33]. Although air-curtain incineration achieves temperatures of 600–1000 °C, because temperatures fluctuate during the process and vary within the burn chamber, there is debate about whether the process is sufficient to ensure the destruction of TSE agents. The cost of air-curtain incineration depends on variables such as carcass species, fuel costs, and equipment type; cost estimates range from about $150 to about $500/t of carcass material [6, 19, 34].

## 4.5 Rendering

Rendering uses physical, thermal, and chemical processes to convert waste animal by-products and mortalities into usable proteins and fats. A detailed history and summary of the rendering industry has been published by the National Renderers Association [36]. According to this report, approximately 40–60% of the live weight of livestock and poultry are not consumed by humans and therefore represent raw materials in the rendering process [36]. From approximately 54 billion pounds of raw materials, about 11 billion pounds each of animal derived proteins and rendered fats are produced annually in the United States, with a production value of about $2.7 billion. About 85% of this output is used as animal feed ingredients [36, 37].

In the wake of the UK BSE epidemic in the mid to late 1980s—which is thought to have been precipitated by the presence of TSE-infected meat and bone meal in cattle feed—concerns about TSEs have resulted in various restrictions on how rendered products can be used in animal feeds. Since 1997, US regulations have prohibited the use of most mammalian protein in ruminant feed. Since BSE was discovered in the United States in 2003, regulatory authorities have sought to strengthen protections against BSE in United States cattle. The appropriateness and availability of rendering as a means of disposal in the event of emergency will depend on many factors, including the nature of the emergency (i.e. whether a disease incident or natural disaster; if a disease event, whether TSEs are of concern) and how the resulting rendered product might be used.

The cost of rendering is influenced by many factors, including the location of the facility in relation to the carcasses' point of origin, energy costs, and the value of the rendered end product. If the end products derived from mortalities cannot be used for feed ingredients, the cost of rendering increases significantly.

The advantages and disadvantages of rendering have been outlined by various sources [14, 38]. Rendering facilities represent preexisting infrastructure, with plants often located near areas of food-animal production. There are few environmental concerns associated with rendering and it requires no long-term management. In some cases rendering could provide a usable end product, which could help off-set carcass disposal costs. However, not all locations are served by a rendering facility, and facilities in close proximity may not have sufficient surge-capacity and/or may not be willing to accept carcasses that result from a disease outbreak. Carcasses must be transported to rendering facilities, which may not be desirable, especially if a rendering facility is in close proximity to other at-risk operations. If rendering is being considered as a possible disposal option in the event of an emergency, discussions with rendering companies should occur at the highest levels prior to an outbreak.

## 4.6 Alkaline Hydrolysis

Alkaline hydrolysis, a relatively new disposal technique pioneered by a private company ($WR^2$), uses alkali and heat to break down biological materials (e.g. proteins, carbohydrates, and lipids); the primary by-product of the process is a sterile liquid effluent consisting of small peptides, amino acids, sugars, and soaps [39]. This effluent must itself be disposed of and/or discharged into municipal waste water treatment systems. Equipment for disposal of animal carcasses by this process is commercially available

in capacities up to 10,000 lb/cycle for fixed-base systems and up to 4,000 lb/cycle for mobile systems. The process has been validated to completely destroy prions; for this reason it has been used to dispose of deer confirmed or suspected of having CWD. At present, because of capacity constraints, the most likely application for this technology is the disposal of TSE-infected materials, rather than the disposal of mass quantities of carcasses during times of emergency. According to the equipment manufacturer, systems large enough to process ruminant carcasses range in cost from about $500,000 to $2 million, with operating costs of approximately $0.07/lb.

## 5 CONCLUSIONS

The ability to respond quickly and effectively to an animal agriculture emergency in which large numbers of carcasses must be disposed of requires management plans that are developed well in advance of an emergency. Although generic guidance documents can provide valuable insights for those tasked with planning for disposal emergencies, the most appropriate event-specific disposal options "will depend on numerous factors, such as the type of disease (e.g. is it contagious to humans or animals), the number of carcasses for treatment/disposal, transportation issues, and availability of treatment/disposal capacity" [7, p. 20]. Disposal plans must also be tailored to the unique conditions existing in each local area at the time of an event. Although disposal of carcasses can present enormous challenges in a time of emergency, effective planning at the local level will help responders manage the process in a way that prevents the spread of disease and protects public health and the environment.

## REFERENCES

1. U.S. Department of Agriculture, National Agricultural Statistics Service (2004). *2002 Census of Agriculture*. United States Summary and State Data.
2. Homeland Security Council. (2004). *Homeland Security Presidential Directive-9*, Subject: Defense of United States Agriculture and Food.
3. Sparks Companies Inc (2002). *Livestock Mortalities: Methods of Disposal and Their Potential Costs*. National Renderers Association, Alexandria, VA.
4. Scudamore, J. M., Trevelyan, G. M., Tas, M. V., Varley, E. M., and Hickman, G. A. W. (2002). Carcass disposal: lessons from Great Britain following the foot and mouth disease outbreaks of 2001. *Rev. Sci. Tech. Off. Int. Epizoot.* **21**(3), 775–787.
5. World Organization for Animal Health (2008). *Outbreaks of Avian Influenza (subtype H5N1) in Poultry (from the end of 2003 to 16 January 2008)*. Accessed 18 Jan 2008 from: http://www.oie.int/downld/AVIAN%20INFLUENZA/Graph%20HPAI/graphs%20HPAI%2016_01_2008.pdf.
6. National Agricultural Biosecurity Center Consortium, Carcass Disposal Working Group (2004). *Carcass Disposal: A Comprehensive Review*. Accessed 4 Feb 2008 from: http://hdl.handle.net/2097/662.
7. United States Environmental Protection Agency. (2005). *Federal Food and Agriculture Decontamination and Disposal Roles and Responsibilities*, http://www.epa.gov/ohs/pdfs/conops11222005.pdf.

8. Iowa Department of Natural Resources (2008). *Iowa DNR Interactive Mapping—Livestock Burial Zones*. Accessed 4 Feb 2008 from: http://csbweb.igsb.uiowa.edu/imsgate/introduction/home.asp.
9. Jacobs, J. (2006). Spatial analysis of mass burial carcass disposal regulations. *National Carcass Disposal Symposium*. 5–7 Dec 2006, Beltsville, Maryland.
10. Hutchinson, S. (2006). Agricultural biosecurity and GIS: a site evaluation model for mass livestock burial. *Annual Meeting of the Association of American Geographers*. Chicago, IL.
11. Gao, Q., Jin, Y., McCarl, B. A., Ward, M. P., Highfield, L., Srinivasan, R., and Jacobs, J. (2007). *Animal Carcass Disposal Under Trial Event*. Accessed 4 Feb 2008 from: http://www.orau.gov/DHS_RE_Summit07/abstracts/Gao.pdf.
12. Lund, R. D., Kruger, I., and Weldon, P. (2000). Options for the mechanised slaughter and disposal of contagious diseased animals—a discussion paper. *Conference on Agricultural Engineering*. 2–5 Apr 2000, Adelaide.
13. UK Environment Agency (2001). *The Environmental Impact of the Foot and Mouth Disease Outbreak: An Interim Assessment*.
14. Flory, G. A., Peer, R. W., and Bendfeldt, E. S. (2006). *Evaluation of Poultry Carcass Disposal Methods used During an Avian Influenza Outbreak in Virginia in 2002*. Virginia Cooperative Extension and Virginia Department of Environmental Quality, http://www.deq.state.va.us/vpa/pdf/Evaluation_of_Poultry_Carcass_Disposal_Methods.pdf.
15. Glanville, T. (2006). Composting for emergency disposal of livestock mortalities. *Emergency Management of Mass Animal Mortality Workshop*. 13–14 Nov 2006, National Center for Foreign Animal and Zoonotic Disease Defense, Austin, TX.
16. Taylor, D. M. (2000). Inactivation of transmissible degenerative encephalopathy agents: A review. *Vet. J.* **159**(1), 10–17.
17. Brown, P., and Gajdusek, D. C. (1991). Survival of scrapie virus after 3 years' interment. *Lancet* **337**(8736), 2.
18. National Audit Office (2002). The 2001 outbreak of foot and mouth disease. In *Report by the Comptroller and Auditor General*. The Stationery Office, London.
19. Brglez, B. (2003). *Disposal of Poultry Carcasses in Catastrophic Avian Influenza Outbreaks: A Comparison of Methods*. Master of Public Health thesis, University of North Carolina, Chapel Hill, NC.
20. Flory, G. A., Bendfeldt, E. S., and Peer, R. W. 2006. Landfilling of poultry carcasses: Lessons learned from the Virginia avian influenza outbreak of 2002. *National Carcass Disposal Symposium*. 5–7 Dec 2006, Beltsville, Maryland.
21. Riverside County Waste Management Department (2003). *Exotic Newcastle Disease 2003 (DVD)*. Riverside County, CA.
22. Flory, G. A., Bendfeldt, E. S., and Peer, R. W. (2006). *Guidelines for Landfilling Poultry Mortality in Response to an Outbreak of Avian Influenza*. Virginia Department of Environmental Quality. Available at: http://www.deq.virginia.gov/vpa/pdf/Landfilling_Fact_Sheet.pdf.
23. U.S. Environmental Protection Agency (2004). *Letter of 12 Nov: Clarification and Revision of April 6, 2004, Memorandum on Recommended Interim Practices for Disposal of Potentially Contaminated Chronic Wasting Disease (CWD) Carcasses and Wastes*. Office of Solid Waste, Washington, DC.
24. DNV. 2001. *Assessment of Risk due to BSE Infectivity from Disposal of Cattle due to FMD*. Report for The Ministry of Agriculture Fisheries and Food.
25. DNV 1997. *Compendium of five Reports: (a) Overview of Risks from BSE via Environmental Pathways, (b) Thruxted Mill Rendering Plant-Risk Assessment of Waste Water Disposal*

*Options, (c) Risks from Burning Rendered Products from the Over Thirty Month Scheme in Power Stations, (d) Risks from Disposing of BSE Infected Cattle in Animal Carcase Incinerators, (e) Assessment of Risk from BSE Carcasses in Landfills*. Report to the UK Environment Agency. Report to the UK Environment Agency, Det Norske Veritas C7243.

26. Schramm, P. T., Johnson, C. J., Mathews, N. E., McKenzie, D., Aiken, J. M., and Pedersen, J. A. (2006). Potential role of soil in the transmission of prion disease. *Rev. Mineral. Geochem.* **64**(1), 135–152.
27. Johnson, C. J., Pedersen, J. A., Chappell, R. J., McKenzie, D., and Aiken, J. M. (2007). Oral transmissibility of prion disease is enhanced by binding to soil particles. *PLoS Pathog.* **3**(7), e93.
28. Kalbasi, A., Mukhtar, S., Hawkins, S. E., and Auvermann, B. W. (2005). Carcass composting for management of farm mortalities: a review. *Compost Sci. Util.* **13**(3), 180–193.
29. DeRouchey, J. M., Harner, J. P., and Murphy, J. P. (2005). Catastrophic mortality composting: is it safe and effective?. *J. Appl. Poult. Res.* **14**(2), 414–416.
30. Wilkinson, K. G. (2007). The biosecurity of on-farm mortality composting. *J. Appl. Microbiol.* **102**(3), 609–618.
31. Bendfeldt, E. S., Flory, G. A., and Peer, R. W. (2006). Is in-house composting a practicable method of disease containment and disposal for turkeys, breeder operations, and multi-level houses?. *National Carcass Disposal Symposium*. 5–7 Dec 2006, Beltsville, Maryland.
32. Glanville, T. D., Richard, T. L., Harmon, J. D., Reynolds, D. L., Ahn, H. K., Akinc, S. (2006). *Final Project Report: Environmental Impacts and Biosecurity of Composting for Emergency Disposal of Livestock Mortalities*. Iowa State University. Accessed 30 Jan 2008 from: http://www3.abe.iastate.edu/cattlecomposting/.
33. Ellis, D. B. (2001). *Carcass Disposal Issues in Recent Disasters, Accepted Methods, and Suggested Plan to Mitigate Future Events*. Political Science Department, Public Administration, Texas State University, San Marcos, p. 128.
34. U.S. Department of Agriculture and Texas Animal Health Commission (1994). *Swine Carcass Disposal Evaluation Using Air Curtain Incinerator System, Model T-359*.
35. U.S. Department of Agriculture, Animal and Plant Health Inspection Service (2003). Risk reduction strategies for potential BSE pathways involving downer cattle and dead stock of cattle and other species: advance notice of proposed rulemaking. *Fed. Regist.* **68**(13), 2703–2711.
36. Meeker, D. (2006). *Essential Rendering—all About the Animal By-products Industry*, D. Meeker, Ed. National Renderers Association, Alexandria, VA, p. 314.
37. National Renderers Association *North American Rendering: the Source of Essential, High-quality Products*, 2nd ed., National Renderers Association, Alexandria, VA.
38. Hamilton, C. R., Kirstein, D., and Meeker, D. (2006). An overview of the rendering industry. *National Carcass Disposal Symposium*. 5–7 Dec 2006, Beltsville, Maryland.
39. WR2 (2008). *Tissue Digestion by Alkaline Hydrolysis*. Accessed 9 Feb 2008 from: http://www.wr2.net/wr2_usa/usa/tissue.html.

## FURTHER READING

National Agricultural Library (2006). *Disposal of Dead Production Animals, Bibliography 1988–2006*. Accessed 17 Jan 2008 from: http://www.nal.usda.gov/awic/pubs/carcass.htm.

National carcass disposal symposium: connecting research, policy, and response. Dec 4–7, 2006. *Conference Presentations*. Beltsville, MD. Available at: http://www.composting.org/NCDS%20Speakers.htm.

# OPTIMAL INVESTMENTS IN MITIGATING AGROTERRORISM RISKS

WILLIAM E. NGANJE
*Arizona State University, Mesa, Arizona*
ANDREW LEWIS
*Risk Management Agency, Kansas State University, Manhattan, Kansas*
WILLIAM WILSON
*North Dakota State University, Fargo, North Dakota*

## 1 INTRODUCTION

Agroterrorism, or a terrorist attack on the food supply, has become a major concern since the September 11, 2001 attacks. Terrorism directed toward the food system could have extremely large human health, economic, and psychological consequences, such as loss of human life, economic disruption, and negative impacts on consumer confidence [1]. Consequently, if there is any intentional tampering by terrorists on the US food system, it could cost the country billions of dollars in order to control or stabilize the situation [2].

This study provides a framework to value investment strategies to mitigate possible agroterrorism occurrences in the food supply chain and to determine where these investments would reduce the most risk. Such a framework could be applied to any food sector at risk from agroterrorism. This study applies the framework to the milk industry. Previous health scares related to milk illustrate the potential for human harm and economic damage. The discovery of the pesticide heptachlor in over 80% of the milk produced in Oahu, Hawaii in 1982 and the resulting drop in milk consumption showed how contamination can financially handicap the milk industry. It could also result in a number of casualties. Wein and Liu [3] illustrate the possibility of a deadly bioterror attack on the milk supply chain, as the botulinum toxin could be released at the holding tank at a dairy farm, a tanker truck transporting milk from the farm to the processing plant, or a raw milk silo at the processing facility.

The current method of record keeping and maintenance is called the *one-step forward/one-step backward* (OSF/OSB) method. This method requires persons who manufacture, process, pack, transport, distribute, receive, hold, or import food into the United States to keep records of the immediate previous sources and immediate subsequent recipients of food [4]. However, this method may be costly, and it could significantly hinder global food trade. The annual total record keeping cost is estimated to be $1.41 billion [5]. In recent years, alternative tracking devices such as radio frequency environmental monitoring(RFEM) technology have emerged as an alternative to track and prevent agroterrorism risks along food supply chains. The potential benefits

of the RFEM technology are that: (i) record real-time data that can be downloaded and analyzed during the process; (ii) could be used to screen for malicious tampering of food containers or packages; (iii) could pinpoint the location of tampering or more importantly could indicate the possibility that a toxic material or infectious agent was added to the product; (iv) could be used for traceability from production to commercialization; and (v) could be used to monitor and record weather conditions, types, amounts, and timing of chemicals applied, disease incidence, insect infestations, and harvest dates [6].

The primary objective of this study is to evaluate the cost-effectiveness of the use of alternative tracking strategies intended to mitigate agroterrorism risks along the milk logistic system. The specific objectives are to determine the costs and risk premiums that the private sector is willing to pay for alternative tracking strategies along the supply chain and where and when along the supply chain investments in alternative intervention strategies will reduce the most risk. The framework developed in this study consists of a stochastic optimization model, a real options model, and the "tomato garden" portfolio of options framework.

## 2 THEORETICAL MODELS

Investment decisions to mitigate agroterrorism risk are made under conditions of risk and uncertainty. Several conceptual frameworks have been used in the literature to model and evaluate investment decisions under conditions of risk and uncertainty [7–11]. These frameworks range from simple mean-variance graphical comparisons of risk and returns to robust development of the expected utility maximization framework. The framework used in this study consists of two steps: (i) quantifying the cost and risk premium associated with alternative tracking technologies; and (ii) identifying areas where investment will reduce the most risk along the supply chain and the incentives to invest in security measures. The first step is accomplished by using stochastic optimization and the expected utility framework, whereas the second step uses real options and the portfolio of options framework.

### 2.1 Stochastic Optimization Model

A stochastic optimization model of a vertically integrated firm is developed to determine the costs, risks, and optimal strategies associated with four alternative tracking technologies: (i) random testing with no lock-out tag or RFEM system installed; (ii) OSF/OSB tracking for bioterrorist events; (iii) tracking with RFEM installed, with testing for contaminants when RFEM signals tampering and random testing elsewhere; and (iv) tracking with RFEM installed with required testing for contaminants at the milk plant and import facilities. The advantage of stochastic optimization over alternative valuation models is that a risk premium can be estimated with multiple stochastic variables in the model [2].

In this model, the total system costs and optimum premium for each strategy are estimated. Stages along the milk supply chain where testing can be implemented include the farm, transport from farm to processing facility, milk silo, pasteurization, postpasteurization tanks, bottling, and transport for export. The total system cost ($C_i$) is defined as:

$$C_i = \sum_{j=1}^{n} T_{ij} \cdot TC_{ij} \cdot S_{ij} \cdot V_{ij} + Q_{ij} \cdot L_{ij} + RFEM_{ij} \tag{1}$$

where $i$ varies from one to four, indicating alternative tracking technologies; $j$ is the location where tests are conducted; $T_{ij}$ is a binary variable indicating test/no test at location $j$; $TC_{ij}$ is the cost of testing per unit (dollars per test) at location $j$; $S_{ij}$ is the sampling intensity at location $j$; $V_{ij}$ is the volume of milk flow at location $j$; $Q_{ij}$ is the volume diverted (quantity not meeting specifications) at location $j$; $L_{ij}$ is quality loss cost per unit at location $j$; and $RFEM_{ij}$ is the cost of installing RFEM or alternative tracking devices at location $j$.

The model is used to estimate the certainty equivalent and quantify the risk premium for the four alternative systems. The risk premium is the difference required for the investor to be indifferent between the alternative tracking strategies. The objective function uses a von Neumann–Morgenstern-type utility function, with increasing relative risk aversion and decreasing absolute risk aversion [12]. This model chooses the optimal testing strategy (where to test and the testing intensity) that maximizes the utility of a vertically integrated firm. The objective is:

$$\begin{aligned} \mathrm{Max}U = E(U(W)) \quad &= \quad \lambda - \exp(-\Phi W^{\eta})) \\ &\text{Subject to } X_j \in Y_j, \end{aligned} \tag{2}$$

where $U$ is utility; $EU$ is the expected utility of the vertically integrated firm; $W$ is the wealth of the vertically integrated firm; $\lambda$ is the parameter determining positiveness of the utility function; exp is exponential power function; $\Phi$ and $\eta$ are parameters which affect the absolute and relative risk aversion of the utility function; $X_j$ is the decision variable vectors of the model; and $Y_j$ is the opportunity cost of the model.

The advantage of using this utility function in the stochastic simulation model is that it is flexible and allows for changes in absolute and relative risk aversion. This utility function also allows us to quantify the cost and risk premium that would make the vertically integrated firm indifferent between a base model (random testing) and the alternative tracking technologies. The parameters of the utility function $\lambda$, $\Phi$, and $\eta$ are fixed and set to 2, 0.01, and 0.5, respectively.

The risk premium is defined as:

$$\pi_i = EV_{\mathrm{BCM}} - C_i \tag{3}$$

where $\pi_i$ is the risk premium for strategy $i$; $EV_{\mathrm{BCM}}$ is the expected value of the base case model with random testing; and $C_i$ is the certainty equivalent of the strategy $i$. The validity of the expected utility framework requires a test for robustness of the results to be evaluated. This is accomplished by performing sensitivity analysis under relative and absolute risk aversion parameters. Cost and risk premium results are used in the real options model to determine the timing of investment decisions.

### 2.2 Real Options Model

The real options approach to agroterrorism prevention assumes that an investor has the opportunity to invest in a prevention strategy and the investor prefers to reduce income volatility. The effect of the uncertainty associated with an agroterrorism event can be valued using a real options valuation procedure, which is a form of a European call option, even though the value of the project is not clearly recognized at the time of the investment. The returns from the real options model work similar to returns from car

insurance investments. Such an investment is made with the intention of never having to use it, but when an attack does occur, a positive payoff is the result from the investment. The model assumes that returns follow a Poisson (jump) and a mixed Brownian motion (continuous) process. The continuous movement of the process is due to production and price variability whereas the discrete jump process can be credited to uncertain agroterrorism actions [10].

The Poisson jump process assumes that the amount of time a firm operates before an agroterrorism event occurs follows an exponential distribution, and if an agroterrorism event occurs, returns are reduced. The advantage of using the Poisson jump process over typical binomial distributions is that it can account for a specific time period and extreme events that typical binomial distributions may miss.

Mohtadi and Murshid [13] used extreme value statistics to evaluate the probability of an attack that would cause the number of fatalities plus injuries to exceed 5000. These probability forecasts were determined for now, 5 years, 10 years, and 25 years into the future. The forecasts were broken down into different categories: chemical agents, biological agents, and radioactive or nuclear agents (CBRN). The results showed that the probability of attack increased if no action is taken to prevent an attack. These results were 0.18, 0.22, 0.26, and 0.35, for now, 5 years, 10 years, and 25 years, respectively. These results were for a CBRN attack in general and were not targeted toward the food sector. However, it was determined that the probability of attack will increase over time in the absence of preventive measures. The probability of an attack on the milk supply chain is scaled down and assumed to be 0.01 and sensitivities are performed for a range of probability values.

The amount of time it takes before a "jump" to a lower level of returns is assumed to be a random variable with a range on the interval $[0, \infty]$. Thus, the probability of the jump occurring at time $T$ is:

$$P(a < T \leq b) = \int_a^b \lambda \, \mathrm{e}^{-\lambda t} \, dt \tag{4}$$

where $t$ is the current time, $\lambda$ is the positive exponential hazard rate parameter, and e is the natural exponential function. The value $\exp(-\lambda t)$ measures the probability of occurrence of an agroterrorism event sufficient to affect firm revenue, whereas $\lambda$ measures the probability of the event occurring just after time $t$. The expectation of $T$ is inversely related to $\lambda$; therefore a subjective determination of the size of $\lambda$ can be made using the investors' prior beliefs [14].

Brownian motion is used to model continuous movement in future returns from an investment. This is also used to describe the probability distribution of the future price of a commodity. Commodity price movements are assumed to follow a log normal distribution, with the amount of time that has passed being dependent on the mean and standard deviation. The following is a typical Brownian motion process equation:

$$dV = \alpha V \, dt + \sigma V \, dz \tag{5}$$

where the increment of the Brownian motion process is represented by $\mathrm{d}z$, with drift parameter $\alpha$ and variance rate $\sigma$. According to Eq. (5) the expected growth rate of $V$ is equal to the sporadic variability plus volatility in the price of the commodity.

The value of an option or an investment opportunity in an agroterrorism prevention strategy, $F(V)$, is defined as the expected present value from investing at the optimal time [10, 15, 20]:

$$F(V) = \max_T E_0[(V_T - K)\mathrm{e}^{-\rho T}] \tag{6}$$

where $T$ is the optimal time to invest; $V_T$ is the expected present value of the investment made at time $T$; $K$ is the sunk cost of the project; e is the natural exponential function; $\rho$ is the discount rate; and $E$ is an expectation operator. The expected present value of the option or investment is a function of state variables (e.g. the decision to not invest or invest in alternative security measures), as well as choice variables (e.g. the amount to spend) at current time $t$. The objective is to maximize future cash flows from the investment.

This study covers two cases: the impact of an intentional attack in the supply chain, and the impact of an unintentional attack in the supply chain. The unintentional attack case is modeled as a dynamic process, which becomes a Bellman equation in continuous time.

$$\rho F(V(x,u,t)) = \max_u \left[\pi(x,u,t) + \frac{1}{dt} E\left[df(V)\right]\right] \tag{7}$$

According to Eq. (7), the normal return per unit time that is required to hold the commodity value $F(V)$ is equal to the immediate profit if the investment is made ($\pi(x,u,t)$), plus the capital gain or loss expected from holding the option ($E[\mathrm{d}f]$). The profit is zero if the investor holds on to the option, and this is the case for the periods before the investment is made. Multiplying this equation through by d$t$ yields

$$\rho F(V(x,u,t))\, dt = E\left[dF(V)\right] \tag{8}$$

This implies that the return on the investment opportunity equals the expected gain from holding the option, which in turn depends on the future value of the commodity. As stated earlier, it is assumed that the expected present value of the investment $V$ develops according to a combined geometric Brownian motion and Poisson jump process of the structure

$$dV = \alpha V\, dt + \sigma V\, dz - V\, dq \tag{9}$$

The term $V$ d$q$ is the Poisson jump process, defining the probability of the agroterrorism event occurring during an extremely small interval of time, d$t$. If d$q$ and d$z$ are independent, then d$q$ can be defined as

$$dq = \begin{cases} 0 & \text{with probability } (1-\lambda) \\ \phi & \text{with probability } \lambda, \end{cases} \tag{10}$$

where $\phi$ is the percentage by which $q$ will change if the agroterrorism event or Poisson occurs ($0 \le \phi \le 1$). The firm quits operating and continues to remain closed if $\phi = 1$.

Hence, in the Bellman equation (8), dF can be expanded using Ito's lemma. This is used for the differentiation of stochastic processes. Now an expression in terms of d$V$ is obtained

$$\rho F(V)\,dt = E\left[F'(V)\,dV + \frac{1}{2}F''(V)\,dV^2\right]$$

$$\rho F(V)\,dt = \alpha V F'(V)\,dt + \frac{1}{2}\sigma^2 V^2 F''(V)\,dt - \lambda\left[F(V) - F((1-\phi)V)\right]\,dt \quad (11)$$

$$0 = -(\rho+\lambda)F(V) + \alpha V F'(V) + \frac{1}{2}\sigma^2 V^2 F''(V) + \lambda F((1-\phi)V)$$

This second order homogeneous differential equation is solved for the value of the investment opportunity, *F(V)*, subject to the following constraints

$$\begin{aligned} F(0) &= 0 \\ F(V^*) &= V^* - K \\ F'(V^*) &= 1 \end{aligned} \quad (12)$$

where $V^*$ is the optimal expected net present value of the project. Numerical simulation methods with Risk Optimizer [16] are used to obtain $V^*$ because of uncertainty in returns and prices that result from agroterrorism. Risk-neutral valuation techniques are used to estimate the real options values for all economic entities along the milk supply chain using a portfolio of options framework.

### 2.3 "Tomato Garden" Option Space Framework

The "tomato garden" option space model, also known as *the portfolio of options*, involves the estimation of two variables: the volatility matrix (product of square root of time and the standard deviation of the net present value (NPV)) and the value-to-cost matrix (ratio of the NPV of the agroterrorism investment to the cost of the investment). Both variables are graphed into a two-dimensional illustration called *the option space*. The value-to-cost variable contains all of the data normally detained in NPV and real options problems, but adds the time value of being able to postpone the investment. The volatility variable measures how much the condition of the world can change before an investment decision must be made. The option space is portrayed by these two variables, with volatility on the vertical axis and NPV/cost on the horizontal axis (Fig. 1) [17].

Typical NPV models used in real options formulations provide only two options: invest or do not invest. By extending the real options analysis into the portfolio of options framework, the investor has the added advantage of having the NPV, two extra metrics, plus six possible actions that reflect what should be done right away, and also indicate the likelihood that an agroterrorism investment will be beneficial in the future. One more advantage of the portfolio of options matrix is that public investment strategies to all economic sectors of the milk supply chain can be represented as nested options. The nested options formulation allows the total investment on agroterrorism to be evaluated more effectively. With this strategy, a sequence of unforeseen events at alternative economic entities can be added into private or public sector investment decisions. For

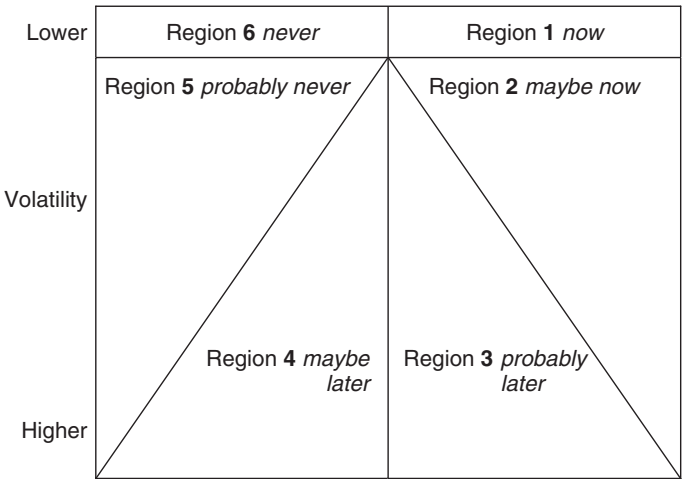



**FIGURE 1** "Tomato garden" option space framework. (Source: Luehrman [17]).

example, public investment may target sectors with the greatest amount of risk, evaluate how the investments in these sectors mitigate agroterrorism risk, and then decide to invest in other sectors with the possibility to further diminish those risks [10].

## 3 DATA AND SIMULATION PROCEDURE

Data were collected for the lot sizes for each of the economic entities (farm level, processing, and retail) of the milk supply chain; tracking and data management costs, including the lock-out tag and RFEM costs; recleaning costs; the quality loss costs; and milk prices. The average on-farm lot size is approximately 1200 gal. This is calculated using the number of farms and total milk cows from 2002 to 2005 [18, 19] and the average milk produced daily, 10 gal, which was obtained from Wein and Liu [3]. The lot size used for the milk truck is 5500 gal and the lot size for the milk silo is 50,000 gal. The pasteurization lot size used is a uniform distribution between 50,000 and 60,000 gal. The postpasteurization tank lot size is 10,000 gal. The bottling for domestic user lot size equals the postpasteurization tank lot size, and the loading lot size for the export user equals the milk truck lot size [3] (Cooper, M. 2006, Personal Communication) [20].

The lock-out tags are placed on the trucks transporting the milk from the farm to the processing facilities. This tag is used on the manhole and the back outlet of the milk truck and is applied after each cleaning. The tags provide security during transportation. The average cost per tag is about $0.21. The average cost of an RFEM unit is approximately $0.45 [6]. The RFEM units provide similar functioning as the lock-out tags but can be used to store data on the origin and quantity of milk from each farm or economic unit to another. They can also be programmed to relate real-time data if tampering occurs at any point along the supply chain. Recleaning costs occur if one of the lock-out tags is broken before the next pickup of milk. The average recleaning cost is approximately $45.00 per cleaning.

The quality loss cost consists of the recall/dumping costs and the lost sales costs. The recall/dumping costs are represented by a triangular distribution with most likely cost of

$1.17/gal. These costs are calculated using the minimum, average, and maximum prices received by farmers from 1995 to 2004 [21]. The lost sales costs are based on the past contamination and sales loss incident in Hawaii and are calculated to be approximately $0.075/gal of contaminated milk [22]. The average preprocessing and postprocessing prices of milk from 1998 to 2004 are $1.18 and $2.84/gal, respectively [21, 23].

Testing costs, test accuracies, RFEM reliability, and the probability of contamination at each stage in the milk supply chain are assumed random and represented by distributions. Testing costs for pathogens and toxins are represented by a triangular distribution with a most likely cost of $25 per test. Testing accuracies are assumed to be uniform distributions ranging between 0.9 and 1.0. The reliability of signaling tampering with the RFEM units is assumed to be uniformly distributed between 0.95 and 0.99 [6]. The probability of intentional contamination is reflected at each stage of the milk supply chain by a Poisson distribution with a mean probability of 0.01 [2]. The size of contamination, if contamination occurs, is assumed to be equal to the lot size and introduced at the point of occurrence.

Real options values are calculated for the vertically integrated supply chain using the data generated from the stochastic optimization model. The average discount rate used is 0.07 and sensitivities on the probability of contamination (the same probabilities as in the stochastic simulation sensitivities) are run to explore their impacts on the real options values. Real options values are also calculated for three major participants along the supply chain: the farm, processor, and importer/retailer.

### 3.1 Simulation Procedures and Assumptions

Three tracking strategies are evaluated for the domestic supply chain. Any testing conducted is assumed to be for *salmonella* and botulinum toxin. The base strategy consists of mandatory testing when the milk arrives at the milk plant for both the domestic and export supply chains and mandatory testing when the milk arrives at the importing facility in the export supply chain. This strategy also includes random testing elsewhere along the supply chain and does not contain the lock-out tag or RFEM unit. It is the common tracking practice in the milk supply chain.

The second tracking strategy is to implement the lock-out tag in the domestic supply chain and the lock-out tag along with RFEM in the export supply chain. This strategy consists of mandatory testing when the milk arrives at the milk plant in the domestic and export supply chains. However, in the export supply chain two different scenarios are examined. The first is to continue to require mandatory testing at the import facility whether or not the RFEM unit signals tampering, and the second is to only require mandatory testing at the import facility when the RFEM unit signals tampering. Random testing is still used for all points along the domestic and export supply chain that did not require mandatory testing.

The third tracking strategy is the OSF/OSB strategy regulation, requiring mandatory record keeping. With this strategy, each sector of the domestic and export supply chains is tested to meet the specifications of the record keeping requirements and other product quality and marketing requirements. This strategy does not contain the lock-out tag or RFEM unit.

Sensitivities are conducted to examine effects of critical parameters, such as costs and risks, on the optimal strategies. These parameters include the probability of

contamination, cost of the lock-out tag/RFEM, reliability of the lock-out tag/RFEM, and the cost of recalls.

The optimal NPV and standard deviation values are simulated using @Risk decision tool software [24]. These values are then used to determine the two main variables used for the portfolio of options framework: NPV/cost and volatility. The portfolio of options model is used to determine whether or not to invest and when the RFEM/alternative strategy should be implemented to reduce most of the risks.

## 4 STOCHASTIC OPTIMIZATION MODEL RESULTS

### 4.1 Domestic Milk Supply Chain

The optimal tracking strategy for the base case in the domestic milk supply chain model is to test only where it is mandatory to test, when milk is received at the milk plant (Table 1). Table 1 shows the buyer and seller risks under each strategy. Buyer risk is the risk that product exceeding tolerances will get into the buyer product stream, and seller risk is the risk that product thought to be within tolerances will be rejected. Buyer and seller risks are minimal in the base case with mean values of 1.10504 E-07 and 2.05301E-17%, respectively. These results indicate that 1.10504 E-07% of lots entering the domestic user flows might be contaminated (buyer risk) and 2.05301E-17% of the lots might be rejected (seller risk). Average systems costs for conducting random testing for pathogens, recleaning, and quality loss are \$0.004545452, \$3.43173E-11, and \$0.00/gal, respectively. The certainty equivalent is \$0.004545452/gal, indicating that the decision maker would require a premium of this amount to be indifferent between this system and one with no testing.

In the second model a lock-out tag system is installed on truck shipments picking up milk from the farm. A mandatory test is applied when the truck arrives at the milk plant and a mandatory recleaning is applied when the lock-out tag is broken before milk pickup. The optimal tracking strategy for the domestic lock-out tag system is to test only when mandatory testing is required. Buyer risks for the lock-out tag system average 1.11372 E-07% with a 95% confidence interval of 6.54687E-08 to 1.13491E-07%. Seller risks average 2.05959E-17% with a 95% confidence interval of 4.98362E-18 to 2.59288E-17%. With the lock-out tag system, buyer and seller risks, although still minimal, are larger than those in the base case. The more security put on the supply chain, the more the risk of rejection of products. The average costs for lock-out tags, testing, recleaning, and quality loss are \$7.63637E-05, \$0.004545452, \$3.43173E-11, and \$0.00/gal, respectively. The results indicate that there is a 95% confidence interval for quality loss costs to be \$0.00/gal and for total system costs to lie between \$0.004617117 and \$0.0046543/gal.

Installing a lock-out tag system increases the certainty equivalent to \$0.004621816/gal from the domestic base case of \$0.004545452/gal. This indicates that the decision maker would require a risk premium of \$0.0000763637/gal to be indifferent between the lock-out tag system and the base case.

The third model simulated is one where tests are applied and information passed OSF/OSB. This requires tests on all lots along the domestic milk supply chain. No lock-out tag or RFEM system is installed and there are no optional testing locations. Average buyer and seller risks are 1.19377E-07 and 5.32244E-07%, respectively. Costs for the OSF/OSB system are the highest of the three domestic systems. Costs for testing, quality loss, and recleaning are \$0.035793613, \$1.83705E-06, and \$3.43173E-11/gal,

**TABLE 1 Domestic Milk Model Optimal Testing Strategy Results**

| | Base Case Random Testing No RFEM/Tag Mandatory Testing at Milk Plant | Random Testing with Tag and Mandatory Testing at Milk Plant | OSF/OSB |
|---|---|---|---|
| Utility | 1.2004 | 1.2004 | 1.2004 |
| Test (1 = yes, 0 = no) and intensity % sampled | | | |
| On farm | 0–NA[a] | 0–NA | 1–100% |
| Milk silo | 0–NA | 0–NA | 1–100% |
| Pasteurization | 0–NA | 0–NA | 1–100% |
| Postpasteurization | 0–NA | 0–NA | 1–100% |
| Bottling | 0–NA | 0–NA | 1–100% |
| Milk plant-truck no signal | 1–100% | 1–100% | 1–100% |
| Milk plant-truck signal | NA | 1–100% | NA |
| Buyer risk | 1.10504E-07 | 1.11372E-07 | 1.19377E-07 |
| Seller risk | 2.05301E-17 | 2.05959E-17 | 5.32244E-07 |
| Costs ($/gal) | | | |
| Cost of testing | 0.004545452 | 0.004545452 | 0.035793613 |
| Cost of tag | 0 | 7.63637E-05 | 0 |
| Cost of recleaning | 3.43173E-11 | 3.43173E-11 | 3.43173E-11 |
| Cost of quality loss | 0 | 0 | 1.83705E-06 |
| Certainty equivalent ($/gal) | 0.004545452 | 0.004621816 | 0.035795458 |
| Comparison to base case | NA | 0.0000763637 | 0.031250006 |

[a]NA is not applicable

respectively. The OSF/OSB system has a certainty equivalent of $0.035795458/gal and a risk premium of $0.031250006/gal. The tighter the security measure results in a greater risk premium.

The buyer risks are similar in all three systems. The seller risks are similar between the base case and the lock-out tag system, but, although still minimal, are higher in the OSF/OSB system. When comparing the costs (testing, lock-out tags, recleaning, and quality loss) and risk premiums, the base case has the lowest total costs and risk premium as expected, followed by the lock-out tag system, and the OSF/OSB system has the highest total costs and risk premium. Decision makers would require a risk premium of $0.03125/gal to be indifferent between the OSF/OSB system and the base case and $0.031173642/gal to be indifferent between the OSF/OSB system and the lock-out tag system.

Sensitivities are conducted for the domestic model on the probability of intentional contamination, cost of the lock-out tag, reliability of the lock-out tag, and the recall costs to determine their impact on the optimal strategies, costs, and risk premiums. Alternative probabilities of contamination ranging from 0.0001 to 0.1 are examined to determine their effect. Over this range of probabilities for contamination, the optimal tracking strategy does not change. Results show that as the probability of contamination in the supply chain increases, buyer and seller risks and certainty equivalents increase, but minimally.

By doubling or halving the cost of the lock-out tag, the buyer and seller risks show no change and the certainty equivalent has minimal changes. When changing the reliability of the lock-out tag, minimal changes occur in the buyer and seller risks, and the certainty equivalent does not change. When fixing the cost of recalls to the minimum, most likely, and maximum values instead of the triangular distribution, the buyer and seller risks and the certainty equivalent show minimal changes. In each of these sensitivities, the optimal testing strategy does not change. One possible explanation for the observed minimal changes is that participants may view terrorist attacks on the food supply as extreme events. Their expectation that the milk supply chain may be attacked carries more weight than the frequency of attack. Similar analyses are performed for the milk export supply chain.

### 4.2 Export Milk Supply Chain

The export base case model also depicts a vertically integrated firm in the milk supply chain that does random testing for pathogens and toxins. This system contains no lock-out tag or RFEM unit and mandatory testing is applied on all lots arriving at the milk plant and the importing facility. The optimal testing strategy for the base case is to test only where it is mandatory, at the milk plant when milk is received and at the import facility when milk is received (Table 2). Buyer and seller risks are minimal with mean values of 1.49081E-13 and 2.22251E-23%, respectively. Average costs for conducting random testing for pathogens, recleaning, and quality loss are \$0.009009742, \$6.70864E-11, and \$0.00/gal, respectively. The certainty equivalent is \$0.009009743/gal, indicating that the decision maker would require a premium of approximately \$0.009/gal to be indifferent between this system and one with no testing.

In the second model, a lock-out tag system is installed on truck shipments picking up milk from the farm and a lock-out tag and RFEM system is installed on truck shipments from the milk plant to importing facilities. A mandatory test is applied when the truck arrives at the milk plant and at the importing facility. The optimal testing strategy for the lock-out tag and RFEM system is to test only when mandatory testing is required. Buyer risks average 1.83304E-07% with a 95% confidence of 1.54713E-07 to 2.01009E-07%. Seller risks average 1.66972E-09% with a 95% confidence interval of 2.30648E-17–7.47412E-09%. With the lock-out tag and RFEM system, buyer and seller risks, although still minimal, are larger than those in the base case. Average costs for testing, lock-out tags and RFEM, recleaning, and quality loss are \$0.009009742, \$0.000194221, \$6.70864E-11, and \$8.09505E-09/gal, respectively. The results indicate that the 95% confidence intervals are between \$0.00 and \$3.62357E-08/gal for quality loss costs and \$0.009180129 and \$0.009224166/gal for the total system. Installing a lock-out tag and RFEM system increases the certainty equivalent to \$0.009203971, which indicates that the decision maker would require a risk premium of \$0.000194228/gal to be indifferent between the lock-out tag and RFEM system and the base case.

In the next scenario, a lock-out tag system is installed on truck shipments picking up milk from the farm and a lock-out tag and RFEM system is installed on truck shipments to importing facilities. A mandatory test is applied when the truck arrives at the milk plant and testing at the importing facility is only mandatory when the RFEM system signals tampering. The optimal testing strategy for this system is to test only when mandatory testing is required. Buyer risks average 1.86531E-07% with a 95% confidence interval of 1.54713E-07–2.03577E-07%. Seller risks average 1.66972E-09% with a 95% confidence

**TABLE 2 Milk Export Model Optimal Testing Strategy Results**

| | Base Case Random Testing No RFEM/Tag Mandatory Testing at Milk Plant and Import Facility | Random Testing With RFEM/Tag Mandatory Testing at Milk Plant and Import Facility | Random Testing With RFEM/Tag Mandatory Testing at Milk Plant and Mandatory Testing at Import Facility Only When RFEM Signals | OSF/OSB |
|---|---|---|---|---|
| Utility | 1.2004 | 1.2004 | 1.2004 | 1.2004 |
| Test (1 = yes, 0 = no) and intensity % sampled | | | | |
| On farm | 0–NA | 0–NA | 0–NA | 1–100% |
| Milk silo | 0–NA | 0–NA | 0–NA | 1–100% |
| Pasteurization | 0–NA | 0–NA | 0–NA | 1–100% |
| Postpasteurization | 0–NA | 0–NA | 0–NA | 1–100% |
| Bottling | 0–NA | 0–NA | 0–NA | 1–100% |
| Import-No Signal | 1–100% | 1–100% | 0–NA | 1–100% |
| Milk plant-truck No Signal | 1–100% | 1–100% | 1–100% | 1–100% |
| Import-signal | NA | 1–100% | 1–100% | NA |
| Milk plant-truck signal | NA | 1–100% | 1–100% | NA |
| Buyer risk | 1.49081E-13 | 1.83304E-07 | 1.86531E-07 | 1.4908E-13 |
| Seller risk | 2.22251E-23 | 1.66972E-09 | 1.66972E-09 | 7.6315E-07 |
| Costs ($/gal) | | | | |
| Cost of testing | 0.009009742 | 0.009009742 | 0.004545456 | 0.0422221 |
| Cost of tag/RFEM | 0 | 0.000194221 | 0.000194221 | 0 |
| Cost of recleaning | 6.70864E-11 | 6.70864E-11 | 6.70864E-11 | 6.7086E-11 |
| Cost of quality loss | 0 | 8.09505E-09 | 8.09505E-09 | 2.6285E-06 |
| Certainty equivalent ($/gal) | 0.009009743 | 0.009203971 | 0.004739686 | 0.04222474 |
| Comparison to base case | NA | 0.000194228 | −0.004270057 | 0.033215 |

interval of 2.30648E-17–7.47412E-09%. With the lock-out tag and RFEM system, buyer and seller risks, although still minimal, are larger than those in the base case. Average costs for testing, lock-out tags and RFEM, recleaning, and quality loss are $0.004545456, $0.000194221, $6.70864E-11, and $8.09505E-09/gal, respectively. The 95% confidence interval for total system costs ranges from $0.004705743 to $0.004740911/gal. The certainty equivalent is $0.004739686/gal with a risk premium of negative $0.004270057.

The third tracking strategy simulated is one where tests are applied and information stored OSF/OSB. This requires tests on all lots along the export milk supply chain in conformity with existing quality requirements. No lock-out tag or RFEM system is

installed and there are no optional testing locations. Average buyer and seller risks in the OSF/OSB system are 1.4908E-13 and 7.6315E-07 %, respectively. Costs for this system are the highest of the three export systems for testing and quality loss. Costs for testing, quality loss, and recleaning are $0.0422221, $2.6286E-06, and $6.7086E-11/gal, respectively. The OSF/OSB system has a certainty equivalent of $0.04222474/gal, and a risk premium of $0.033215/gal.

The buyer risks are the same in both the base case and OSF/OSB models and, although still minimal, higher in both lock-out tag and RFEM cases. The seller risks are lowest in the base case and highest in the OSF/OSB. The seller risks in both lock-out tag and RFEM cases are the same.

Decision makers would require a risk premium of $0.000194228/gal to be indifferent between a system that includes lock-out tags and RFEM units with mandatory testing at the milk plant and import facilities and a system that consists of mandatory testing at the milk plant and import facilities with random testing elsewhere. Decision makers would require a risk premium of $0.033020769/gal to be indifferent between the OSF/OSB case, and the lock-out tag and RFEM system with mandatory testing at the milk plant and import facilities. However, when comparing the base case to the lock-out tag and RFEM system with mandatory testing at the milk plant and at the import facility when the RFEM signaled tampering, the lock-out tag and RFEM system shows a negative risk premium. This means that this lock-out tag and RFEM system would actually cost less than the base case system due to the reduction in testing locations.

Sensitivities are conducted which show that varying the probability of contamination between 0.0001 and 0.1 does not change the optimal tracking strategy, but buyer and seller risks and certainty equivalents increase as the probability of contamination increases. By doubling or halving the cost of the lock-out tag and RFEM, the buyer and seller risks do not change and the certainty equivalent has minimal changes. When changing the reliability of the lock-out tag and RFEM, minimal changes occur in the buyer and seller risks, and the certainty equivalent does not change. When fixing the cost of recalls to the minimum, most likely, and maximum values instead of the triangular distribution, the buyer and seller risks and the certainty equivalent show minimal changes. In each of these sensitivities the optimal tracking strategy does not change.

## 5 REAL OPTIONS MODEL RESULTS

Real options results compare the cost and benefits or value of risk reduction over time and space. Recall that investment opportunities exist when adopting alternative tracking strategies. These opportunities enable firms to decrease variability of income or increase expected value of returns. From the NPV perspective, the increased expected values are compared with the systems costs of the alternative tracking technologies. Results are provided for both a firm that is vertically integrated in the supply chain and also a supply chain that has the major participants operating together but are not vertically integrated under the same company.

Simulated real options values for the vertically integrated domestic milk supply model indicate that the average NPV for a system with lock-out tags and RFEM is $1,591,745 when the probability of contamination of 0.01. The NPV/cost of the model is calculated to be 1.27 with a volatility of 0.0204 (Table 3). When the probability of contamination is altered to 0.0001, 0.001, and 0.1, average NPV equals $1,390,809, $1,590,364, and

**TABLE 3 Real Options Results**

| NPV | NPV | Cost | NPV/Cost | Volatility |
|---|---|---|---|---|
| | | Vertically integrated milk supplier | | |
| | | Domestic | | |
| Base case Pr. 0.01 | $1,591,745 | $1,252,671 | 1.27 | 0.0204 |
| Pr. 0.0001 | $1,390,809 | $1,252,671 | 1.11 | 0.0187 |
| Pr. 0.001 | $1,590,364 | $1,252,671 | 1.27 | 0.0249 |
| Pr. 0.1 | $822,298 | $1,252,671 | 0.66 | 0.0058 |
| | | Export with mandatory testing at milk | | |
| | | Plant and import facility | | |
| Base case Pr. 0.01 | $2,541,260 | $1,628,486 | 1.56 | 0.0023 |
| Pr. 0.0001 | $2,033,066 | $1,628,486 | 1.25 | 0.0028 |
| Pr. 0.001 | $2,371,304 | $1,628,486 | 1.46 | 0.0042 |
| Pr. 0.1 | $2,541,172 | $1,628,486 | 1.56 | 0.0024 |
| | | Export with mandatory testing when | | |
| | | RFEM signals tampering | | |
| Base Case Pr. 0.01 | $2,802,377 | $1,628,486 | 1.72 | 0.0047 |
| Pr. 0.0001 | $2,338,992 | $1,628,486 | 1.44 | 0.0024 |
| Pr. 0.001 | $2,938,368 | $1,628,486 | 1.80 | 0.0048 |
| Pr. 0.1 | $2,799,089 | $1,628,486 | 1.72 | 0.0047 |
| | | Nonvertically integrated milk supply chain | | |
| Producer | $107,067 | $29,820 | 3.59 | 85,571 |
| Milk plant/processor | $6,090,714 | $59,640 | 102.12 | 4,658,444 |
| Importer | $5,525,148 | $59,640 | 92.64 | 4,621,554 |

*Source:* NPV/Cost

$822,298, respectively. The corresponding NPV/cost ratios for these probabilities are 1.11, 1.27, and 0.66, respectively, whereas the corresponding volatility values are calculated to be 0.0187, 0.0249, and 0.0058, respectively. The system cost for the tracking strategy is $1,252,671.

For a vertically integrated milk supplier with RFEM installed and mandatory testing at the milk plant and import facility, the real options values indicate that the average NPV is $2,541,260, with a corresponding NPV/cost value of 1.56 and a volatility value of 0.0023, when the probability of contamination of 0.01. If testing is required only when RFEM signals tampering, the average NPV is $2,802,377, the NPV/cost ratio is 1.72, and the volatility value is 0.0047. The investment cost in both scenarios is $1,628,486. Table 3 shows that the NPV decreases when the probability of contamination drops.

The next step in the results process is to use the calculated NPV/cost and volatility values from the simulated real options results and graph them into the "tomato garden" framework to determine where and when investment in alternative tracking strategies will reduce most of the risks or be cost-effective. On examining the base case value of 0.01 for probability of contamination among all three scenarios for the vertically integrated milk supplier in the portfolio of options, the results indicate that in each of the scenarios the values fall into the area where the investment strategy will be beneficial to implement now (Fig. 2).

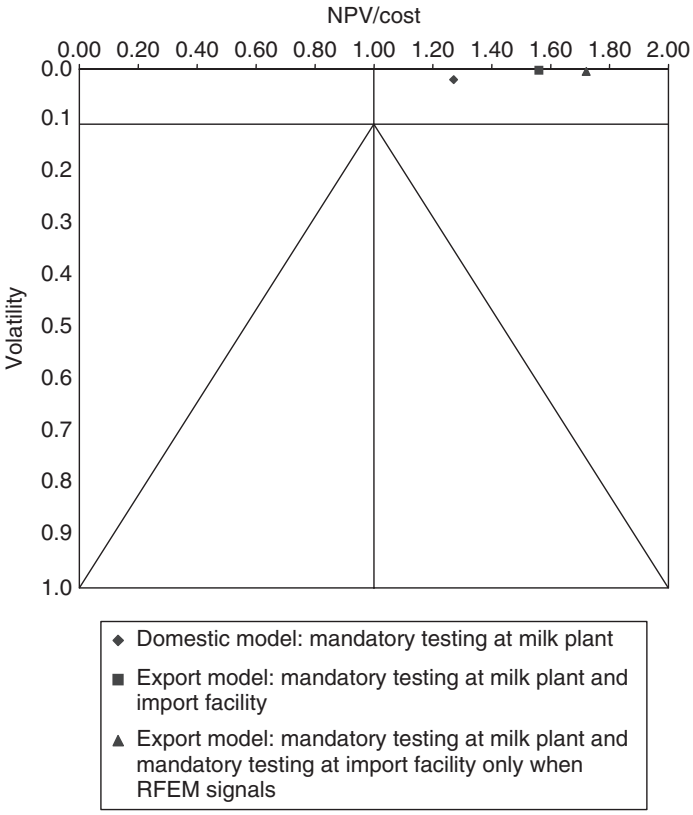



**FIGURE 2** "Tomato garden" option space framework: vertically integrated milk supply chain with probability of contamination of 0.01.

The sensitivity results graphed in the "tomato garden" framework for the probability of contamination of 0.0001 and 0.001 are similar to the base case. These results indicate that in each of the three scenarios for the vertically integrated milk supplier, the values fall into the area where the investment strategy would be beneficial to implement now. The sensitivity results for the probability of contamination of 0.1 show a change from the base case scenarios. In this sensitivity, the results for both export scenarios indicate that the values fall into the area where the investment strategy would be beneficial to implement now, but the domestic scenario results indicate that the values fall into the area where the investment strategy will never be beneficial if implemented.

Results may seem counter intuitive, suggesting that as a risk or probability of attack increases, a vertically integrated domestic firm will not invest in security measures. However, theory suggests that firms can afford to spend on security measures until the marginal benefits are equal to the marginal cost. When costs are greater than benefits from investments, this might suggest the need for external incentives. As the probability of attack increases significantly, public and private efforts may be required to mitigate

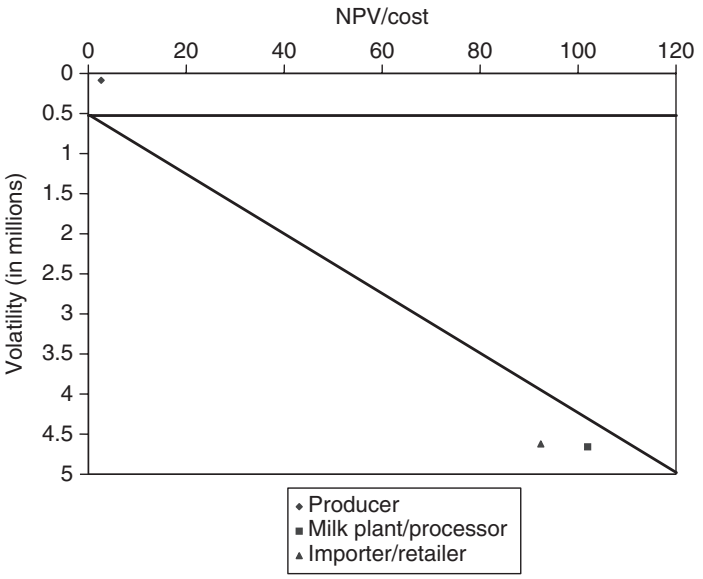



**FIGURE 3** "Tomato garden" option space framework: nonvertically integrated milk supply chain

food terrorism risks. This may be especially true to protect domestic consumers against food terrorism events. This also provides a justification for public sector spending to mitigate food terrorism events.

In the nonvertically integrated milk model, simulated real options values at the farm level indicate that the NPV is $107,067, the NPV/cost ratio is 3.59, and volatility is 85,571 (Table 3). NPV, NPV/cost, and volatility are $6,090,714, 102.12, and 4,658,444, respectively, for the processor and $5,525,148, 92.64, and 4,621,554, respectively, for the importer/retailer. The analysis indicates that for the farm level producer the values fall into the area where it would be beneficial to implement the investment strategy now, whereas the investment strategy would be beneficial probably later for the processor and importer/retailer (Fig. 3).

## 6 CONCLUSIONS

The findings show that as the probability of attack increases, the certainty equivalent and risk premium either do not change or change minimally, which could be due to the perception of the public that the different probabilities of an attack are not viewed as important as whether there is an attack or not. The buyer and seller risks also change minimally when the probability of attack changes, but do increase when the probability increases. However, the change in buyer and seller risks could lead to possible moral hazard issues. Findings also show that the RFEM technology is the more cost-effective tracking strategy compared to the alternative strategies used in mitigating agroterrorism

risks along the milk supply chain. The risk premium is lower for the RFEM tracking investment strategy than in the alternative tracking strategies. These results show a potential for real-time tracking and containment strategies.

The results of both the domestic and export supply chains indicate that no random testing is done. The buyer risks tend to be higher in the domestic model whereas the seller risks tend to be higher in the export model. The testing costs and certainty equivalents are lower in the domestic model due to the fewer number of testing locations and the reduced number of tags along the supply chain.

The real options results suggest that in the vertically integrated milk supply chain it would be beneficial for the domestic and export suppliers to invest in security measures now to reduce most of the risks, with the exception that the domestic suppliers should never invest when the probability of attack is 0.1. Since the results of the domestic supply chain indicate that an investment in food protection measures may not always be beneficial, policy implications may be derived. These policy implications may be that the costs to the domestic milk supply chain should be partly or completely subsidized. This results from the probability of contamination being increased to 0.1. The NPV/cost decreases to below one, which results in the region of never being beneficial in the "tomato garden" option space framework. This provides justification for public sector spending to mitigate food terrorism events. When analyzing the nonvertically integrated milk supply chain, the portfolio of options suggests that the investment strategy would be beneficial to implement now for the farm level entity and probably later for the milk plant/processor and retail/importer.

This study provides a framework for valuing investment strategies to mitigate possible agroterrorism occurrences in the supply chain and determining where these investments would reduce most risks. This framework is applied to the milk industry in this article, but it could also be applied to other food industries that are at risk. Other food products that could be at risk include various produce, honey, peanut butter, seafood, infant formula, baby food, fruit juice, soft drinks, bottled water, and products that use milk as an ingredient, such as yogurt and ice cream [25].

## REFERENCES

1. Onyango, B., C. Turvey, and W. Hallman. 2005. *"Public Attitudes and Perceptions of the Vulnerability of the U.S. Food Chain to Agroterrorism."* Paper presented at American Agricultural Economics Association annual meeting, Providence, RI, 24–27 July.
2. Nganje, W., B. Dahl, W. Wilson, S. Mounir, and A. Lewis. 2007. Valuing private sector incentives to invest in food security measures: quantifying the risk premium for RFEM. J. *Int. Agri. Trade and Dev. Fargo, ND*, **3**(2), 199–216.
3. Wein, L.M., and Y. Liu. 2005. Analyzing a bioterror attack on the food supply: The case of botulinum toxin in milk. *Proceedings of the National Academy of Sciences*, **102**: 9984–9989.
4. Food and Drug Administration, Center for Food Safety and Applied Nutrition. 2004. "Fact Sheet on FDA's New Food Bioterrorism Regulation: Establishment and Maintenance of Records." (December) Available from <http://www.cfsan.fda.gov/~dms/fsbtac23.html>.
5. Food and Drug Administration. 2004. "Final Rule: Establishment and Maintenance of Records Under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002."

(December) Section IV, Part A, and Comment 14. Available from <http://www.cfsan.fda.gov/~lrd/fr04d09a.html>

6. Thompson, J.F. 2004. *Uses of Pedigree Technology's Wireless Sensing and Electronic ID Technology in Agricultural and Food Operations*. Working paper, Pedigree Technologies.
7. Shi, W., and S.H. Irwin. 2005. Optimal Hedging with a Subjective View: An Empirical Bayesian Approach. *American Journal of Agricultural Economics*, **11**: 918–930.
8. Liu, Y., and C.R. Shumway. 2005. *"Empirical Tests of the Refutable Implications of Expected Utility Maximization under Risk."* Paper presented at American Agricultural Economics Association annual meeting, Providence, RI, 24-27 July.
9. Isik, M. 2004. *"Incorporating Risk Preferences into Real Options Models."* Paper presented at American Agricultural Economics Association annual meeting, Denver, CO, 1-4 August.
10. Nganje, W., W. Wilson, and J. Nolan. 2004. Agro-terrorism and the Grain Handling Systems in Canada and the United States. Current Agriculture Food and Research Issues. *A Journal of the Canadian Agricultural Economics Society*, **11**:148–159.
11. Benaroch, M. 2002. Managing Information Technology Investment Risk: A Real Options Perspective. *Journal of Management Information Systems*. Vol. 19, No. 2, pp. 43–84.
12. Wilson, W. and B. Dahl. 2005. Costs and Risks of Testing and Segregating Genetically Modified Wheat. *Review of Agricultural Economics.* Vol. 27(2): 212–228.
13. Mohtadi, H., and A. Murshid. 2005. *"Assessing the Risk of Terrorism Using Extreme Value Statistics."* Working Paper, University of Minnesota & University of Wisconsin at Milwaukee.
14. Pitman, J. 1993. *Probability*. NY: Springer-Verlag.
15. Salin, V., 1998. A real option approach to valuing food safety risks. In *The Economics of HACCP: Costs and Benefits.* L. Unnevehr, Ed. Eagen Press, Minnesota.
16. Palisade Corporation. 1998b. *Risk Optimizer: Optimization with Simulation for Microsoft Excel*. Newfield, NY.
17. Luehrman, T. 1998. *"Strategy as a Portfolio of Real Options." Harvard Business Review*. Sept.-Oct. pp. 89–99.
18. U.S. Department of Agriculture, Economic Research Service (2006a). "Milk Cows and Production by State and Region, 2001-05." Accessed April 17, 2006. <http://www.ers.usda.gov/publications/ldp/xlstables/Dairy%20Farms%20(Ops%20 and%20Licsensed).xls>.
19. U.S. Department of Agriculture, Economic Research Service (2006b). "Dairy Farm Numbers, By State and Region." Accessed April 17, 2006 <http://www.ers.usda.gov/publications/ldp/xlstables/regprod(P).xls>.
20. Cooper, Marv. 2006. Cass-Clay Creamery, Inc. Plant Manager. Personal Communication.
21. U.S. Department of Agriculture, National Agricultural Statistics Service. 2005."Prices Received By Farmers, All Milk." Accessed April 17, 2006 <http://usda.mannlib.cornell.edu/data-sets/livestock/89032/mlkallvf.xls>.
22. Smith, M.E., E.O. van Ravenswaay, and S.R. Thompson. 1988. Sales Loss Determinations in Food Contamination Incidents: An Application to Milk Bans in Hawaii. *American Journal of Agricultural Economics*, **8**: 513–520.
23. U.S. Department of Labor, Bureau of Labor Statistics. 2005. "Retail Price, Milk, Gallon." Accessed April 17, 2006 <http://usda.mannlib.cornell.edu/data-sets/livestock/89032/daprcwmg.xls>.
24. Palisade Corporation. 1998a. *@Risk for Microsoft Excel*. Newfield, NY. **3**(5), 275–280.
25. Acheson, D. 2005. *"Equipping and Educating the Next Generation of Leaders in Food Protection and Defense."*Presentation at the Proceedings of The Institute of Food Technologists = First Annual Food Protection & Defense Research Conference, Atlanta, GA, 3-4 November.

# MID-INFRARED SENSORS FOR THE RAPID ANALYSIS OF SELECT MICROBIAL FOOD BORNE PATHOGENS

LISA J. MAUER AND BRADLEY L. REUHS
*Department of Food Science, Purdue University, West Lafayette, Indiana*

## 1 INTRODUCTION

The goal of sensor research is to provide fast, accurate, and inexpensive methods for detecting chemical and biological contaminants. Sensors based on optical technologies have the advantages of sensor longevity and suitability for continuous monitoring. Optical methods are based on absorption, scattering, or fluorescence of light by the component of interest. Near-infrared (IR) and mid-IR spectroscopy are the most promising of the optical technologies available. IR spectroscopy, on which IR sensors are based, is a form of absorption spectroscopy that can provide both qualitative and quantitative information about the molecules being analyzed. With this method, it is possible to establish the presence of functional groups in a sample and the concentration of the sample components [1]. The measurement of concentration for IR sensors is a one-step relation between the concentration of the component of interest and the detector signal. In IR spectra, any deviation from the baseline (spectra of the control sample) shows the change in the concentration or structure of the component analyzed. Naumann et al. [2, 3] characterized the spectra of bacterial cell into five regions, which were associated with specific chemical groups of the different bacterial components, and concluded that selection of appropriate spectral regions and corresponding weights allowed for detection, identification, and discrimination of bacterial strains.

## 2 FUNDAMENTALS OF INFRARED (IR) SPECTROSCOPY

The fundamentals of IR spectroscopy are described in many references, such as [4], and a brief introduction is provided here to support the understanding needed for pathogen analysis applications. Mid-IR spectroscopy methods are based on studying the interaction of IR light (wavenumbers 4000–400 $cm^{-1}$) with samples. A general schematic for a mid-IR Fourier-transform infrared (FTIR) spectrometer is shown in Figure 1. The IR source in an FTIR emitting radiation is passed through an interferometer (usually a Michelson interferometer with a beamsplitter fixed mirror and moving mirror) that uses interference patterns to make accurate measurements of the wavelength of light. When IR radiation is passed through a sample, some radiation is absorbed and the rest is transmitted to the detector. The energy at which radiation is absorbed correlates to the frequency of

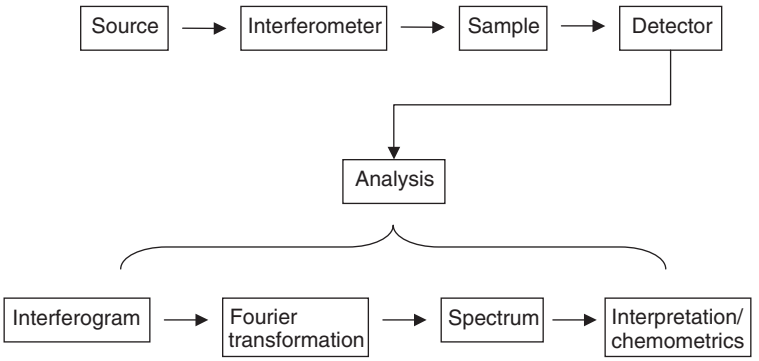



**FIGURE 1** General schematic of a Fourier-transform infrared (FTIR) spectrometer.

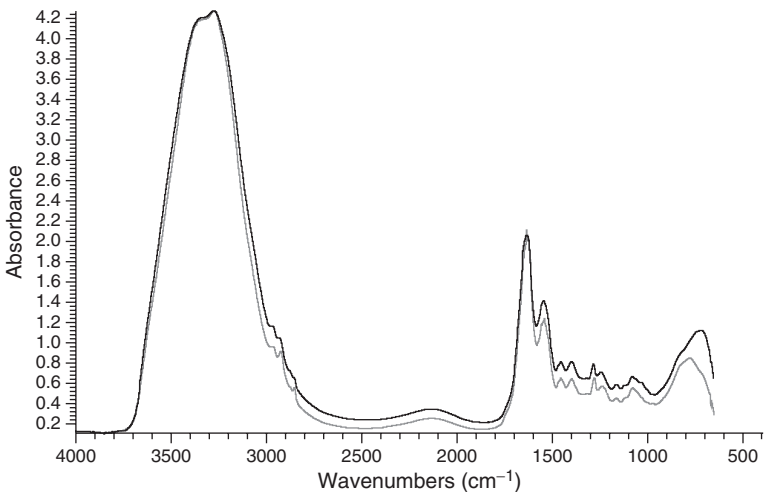



**FIGURE 2** Representative spectra (4000–600 $cm^{-1}$) of bacteria captured on a Metricel filter following the method described by Burgula et al. [5]. Black and gray lines represent the spectrum of *E. coli* O157:H7 and *Salmonella typhimurium*, respectively.

a specific chemical bond vibration in the sample. A functional group will absorb mid-IR radiation if the energy of the IR radiation equals a vibrational energy level difference in the molecule. For many molecules, the fundamental transition from the ground vibrational state to the first vibrational energy level occurs at an energy level, 4000–400 $cm^{-1}$, higher than the ground state. These fundamental transitions appear as peaks in an absorbance spectrum (a plot of the amount of radiation absorbed versus wavenumber, Fig. 2). Some functional groups will also have overtone transitions, excitation to higher energy levels, in the mid-IR range that appear as weak absorbance bands in spectra [4].

The wavenumber positions of absorbance peaks, peak intensities, and peak widths are useful for functional group, cell component, and sample identification. Wavenumber positions of absorbance bands are specific to the functional groups in a sample, thus each sample has a unique "fingerprint" absorbance spectrum. Group wavenumbers, or wavenumber regions in which functional groups absorb IR radiation regardless of other

**TABLE 1 Functional Groups of Major Mid-IR Peaks and Associated Absorbance Peak Wavenumbers**

| Approximate Wavenumber ($cm^{-1}$) | Functional Group Assignment |
|---|---|
| 3500 | OH stretching |
| 3200 | NH stretching (amide A) of proteins |
| 3000–2800 | Fatty acid region |
| 2955 | $CH_3$ stretching of methyl |
| 2930 | $CH_2$ stretching of methylene |
| 2918 | $CH_2$ stretching of methylene in fatty acids |
| 2898 | CH stretching of methane |
| 2870 | $CH_3$ stretching of methyl |
| 2850 | $CH_2$ stretching of methylene in fatty acids |
| 1740 | C = O stretching of esters |
| 1715 | C = O stretching of ester, carboxyl groups |
| 1700–1500 | Amide I and amide II of proteins and peptides |
| 1695–1675 | Amide I band components |
| 1655 | Amide I of $\alpha$-helical structures |
| 1637 | Amide I of $\beta$-pleated sheet structures |
| 1550–1520 | Amide II band |
| 1515 | Tyrosine band |
| 1500–1200 | Mixed region: fatty acid bending vibrations, proteins, and phosphate-carrying compounds |
| 1468 | $CH_2$ bending of methylene |
| 1310–1240 | Amide III band components of proteins |
| 1250–1220, 1084–1088 | $PO_2$ stretching of phosphodiesters |
| 1200–900 | Polysaccharide region: C–O–C, C–O |
| 720 | $CH_2$ rocking of methylene |
| 900–600 | "Fingerprint region" |

(Adapted from Naumann et al. [3], Naumann et al. [7], and Burgula et al. [9]

molecular structures (Table 1), are useful for determining the presence or absence of specific functional groups in a sample [6], and were used by Naumann et al. [2, 3] to classify the spectra of bacteria. Although the general spectra of many bacteria appear similar (such as in Fig. 2), the differences in cell surface structures between bacteria enable differentiation and identification of individual bacterial strains on the basis of spectral differences [7, 8]. Specificity can be derived from spectra by focusing on specific absorbance regions related to those compounds that are diagnostic to a specific pathogen.

By using a library/database of spectra from different types of bacteria, the identification of an unknown bacterium is possible based on spectra matching algorithms (if a spectrum of that type of bacterium is present in the database). Peak intensity becomes important because IR spectra follow the Beer–Lambert law relationship where absorbance ($A_\lambda$) is proportional to pathlength ($l$), absorptivity ($\varepsilon_\lambda$), and concentration ($c$) (Eq. (1))

$$A_\lambda = 1\ \varepsilon_\lambda\ c \tag{1}$$

As the concentration of a molecule increases in the sample, the intensity/height of its absorbance band(s) will also increase (Fig. 3). This facilitates both functional group identification and quantitative assays. If spectra are collected for increasing

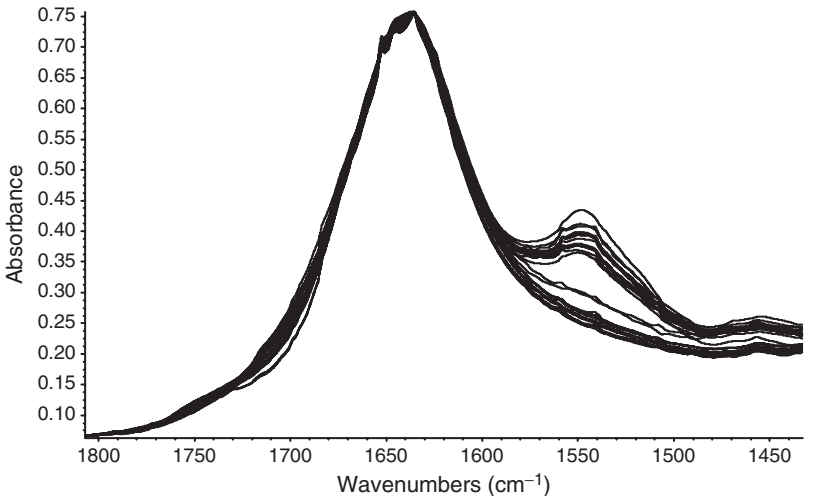



**FIGURE 3** Spectra (1800–1450 $cm^{-1}$) collected hourly from a 24 h growth curve of *E. coli* K12 grown in tryptic soy broth at 37 °C. The initial concentration was 4 CFU/ml at 0 h, the final concentration was 8.5 ± 0.3 log CFU/ml at 24h, and samples were prepared for FTIR analysis following the filtration method described by Burgula et al. [5].

concentrations of bacteria, there will be a corresponding increase in absorbance peak heights in regions characteristic to the cells, as shown in Figure 3. Absorbance peak widths are influenced by the number and strength of functional group interactions with the neighboring molecules, and the overlap of functional group absorbance peaks often occurs with increasing complexity of samples. To facilitate the interpretation of complex spectra, chemometrics approaches are commonly used. Chemometrics algorithms utilize statistical and mathematical techniques to analyze chemical data. Common chemometric approaches include pattern recognition (e.g. hierarchical cluster analysis, principal component analysis, and soft independent modeling of class analogies) and multivariate calibration and prediction (e.g. partial least squares and principal components regression) [10]. For IR sensors, chemometrics enable the interpretation of molecular structural information and correlation to bacterial composition and/or type for both qualitative and quantitative analyses [11–18].

## 3 ADVANTAGES AND DISADVANTAGES OF IR SENSORS

A summary of the advantages and disadvantages of FTIR spectroscopy methods for analyzing microorganisms described by Naumann et al. [7], Smith [4], Naumann [19], Mariey et al. [8], and Burgula et al. [9] is as follows:

### Advantages

1. Nondestructive: the sample remains intact during analysis.
2. Most molecules have IR bands in the mid-IR region (4000–400 $cm^{-1}$)
3. Spectra are unique molecular "fingerprints" that provide information related to functional groups and symmetry.

4. FTIR spectra have enough resolution that absorbances generated from specific pathogens can be differentiated.
5. Relatively fast and easy to use. Most samples can be scanned and spectra analyzed in less than 5 min.
6. Requires very little sample: nano- to microgram.
7. Software is widely available for spectral interpretation using multivariate statistical analysis.
8. May be applied to the field of microbiology for
   - providing information related to bacterial composition and cellular components;
   - screening/taxonomical classification and epidemiological studies;
   - quantification of microorganisms;
   - process control, microbial quality control, and hygienic checks.
9. It is not necessary to know the type of contaminant to successfully identify a potential problem. The advantage of quickly screening a sample for contamination using an IR sensor is balanced with the ability to specifically identify the contaminating substance from its spectra once a deviation from the baseline warrants further investigation.

**Disadvantages**

1. Spectral regions of various components often overlap, which may lead to misinterpretation of results. As samples become more complex, this problem increases.
2. A complete library of spectra for each type of bacteria is recommended to facilitate detection.
3. Surface method.
4. May require expertise in the analysis of spectra for chemotaxonomic classification (especially at the development stage).
5. Atmospheric conditions around the FTIR equipment during testing may affect spectral results.
6. Detection is facilitated by isolating or purifying the bacteria before analysis. Without an isolation step, the mixture of bacteria strains complicates the FTIR spectra.
7. Sample preparation procedures such as culture medium, growth time, and growth temperature may cause variations in spectra.

## 4 BACTERIAL CELL SURFACE COMPONENTS NEEDED FOR CELL IDENTIFICATION

The FTIR and chemometric discrimination of bacterial pathogens reflects many cell surface differences between bacterial species and strains. Although the differences in cell surface structures between Gram-positive and Gram-negative bacteria are considerable, there are sufficient variations in the surface structures between even closely related species, and also within a given species, for effective discrimination. This variation in the presence and abundance of various functional groups (Table 1) results in different spectral fingerprints for each pathogen.

The cell wall of a Gram-positive bacterium, such as *Listeria monocytogenes*, consists primarily of a relatively thick layer of peptidoglycan, a polymer of sugars and amino acids. The peptidoglycan forms a rigid, mesh-like layer over the cytoplasmic membrane that protects the cell protoplast from mechanical damage and osmotic rupture. The crystal lattice structure of the peptidoglycan is due to linear chains of alternating $\beta$-(1,4)-*N*-acetylglucosamine and a $\beta$-(1,4)-*N*-acetylmuramic acid, with each of the latter attached to a 4- to 5-residue peptide. The peptide usually contains L-alanine, D-alanine, D-glutamic acid, and diaminopimelic acid, although the exact structure may differ in different species. The latter three amino acids are not in proteins, and their presence in the peptidoglycan may help to protect the bacterial cell wall against peptidases. The high tensile strength and rigidity of the peptidoglycan yields the unique shape of a given bacterial cell (as opposed to spherical) and provides the protection against osmotic stress.

In Gram-positive bacteria, the thick cell wall (15–80 nm) consists of many layers of peptidoglycan, which are often associated with teichoic or teichuronic acids that are unique to Gram-positive bacteria. Teichoic acids are antigenic polymers of glycerol or ribitol phosphates, and teichuronic acids are chains of uronic acids and amino sugars or other sugar [20]. The variations in the presence and specific structure of various components yields the antigenic properties of the bacterial cell and gives each strain a chemical uniqueness. Also, these polymers are rich in functional groups, such as the carboxyl groups of uronic acids, which will be detected during FTIR analysis. Some strains produce other cell envelope components that are located outside of the cell wall [21], including capsule, such as hyaluronic acid capsule, and proteinaceous appendages. The impact of these components on bacterial identification by FTIR may not be significant, as there is not as much variation to the structures. However, the consistent production of a specific component by a given strain, and the lack of production by another strain would yield clear differences.

In contrast to Gram-positive bacteria, the cell wall of Gram-negative bacteria, such as *Escherichia coli* and *Salmonella* spp., is thin (approximately 10 nm); it consists of a single layer of peptidoglycan inside of a second membrane system, termed the *outer membrane*. The inner leaf of the outer membrane contains the common phospholipids found in the plasma membrane, but the outer leaf, which faces the environment, is unique: it almost entirely consists of lipopolysaccharide (LPS), a molecule found only in Gram-negative bacteria. In fact, LPS production is essential to Gram-negative cells, as mutations that completely block LPS biosynthesis are lethal. The LPS consists of three distinct domains: the lipid A membrane anchor; the nonrepeating core oligosaccharide; and the strain-specific O antigen or O polysaccharide [20, 22].

The lipid A and core are comparatively conserved within, and even among, bacterial species. In contrast, the O antigen, which dominates the surface chemistry of the cell wall, is highly variable among bacterial strains, to the extent that it is a primary source of serotype variation within a species. In addition to structural variation, O antigens are usually polymerized to different extents and demonstrate a range of degrees of polymerization, resulting in the "ladder pattern" that is common in polyacrylamide gel electrophoresis (PAGE) analyses of Gram-negative bacterial extracts [20, 23]. The specific structure of the O antigen yields the "O" designation for a given bacterial strain (such as O157), and hundreds of O antigens have been identified in numerous bacterial species. Although highly variable, O antigens generally display a common structural theme: they consist of relatively small repeats (three to five sugar residues is typical), and they are usually composed of a combination of common sugars (such as glucose,

mannose, fucose, and rhamnose) and unusual sugars. In addition, the O antigen repeat will often carry noncarbohydrate substitutions, such as phosphate, acetate, and pyruvate, on the hydroxyl or amino groups of the sugar residues. For example, in *E. coli* O157:H7 the O157 polysaccharide consists of tetrasaccharide repeats of *N*-acetylgalactosamine, fucose, glucose, and *N*-acetyl-4-amino-4,6-dideoxy-D-mannose. The hydrophobic character imparted by the deoxy sugars and acetyl groups is common in O antigens, and when acid groups are present on the O antigen, they are often esterified. Clearly, these features of bacterial LPS are beneficial in FTIR and chemometric analyses.

Gram-negative bacteria commonly produce a second class of antigens, termed *K antigens* [22, 24, 25]. In contrast to O antigens, the K antigens are highly acidic polysaccharides that form a hydrated, densely charged capsule over the cell wall, and only a fraction of the K antigens on the bacterial cell surface may be directly anchored onto the outer membrane. K antigens generally consist of monosaccharide, disaccharide, or trisaccharide repeating units, which include sialic acid-like sugars or uronic acids. For example, the K1 antigen of *E. coli* is a homopolymer of sialic acid, and the K5 antigen consists of equimolar amounts of glucuronic acid and *N*-acetylglucosamine. The thickness of the capsule varies, but in most strains that produce a capsule, the K antigen polysaccharides are present in abundance.

In summary, O and K antigens are strain specific and are responsible for much of the serotype specificity found within a species. In addition to the hydroxyl groups and glycosidic linkages that characterize polysaccharides, other common chemical features of O and K antigens include phosphate, acetyl, amide, carboxyl, methylene, and methyl groups, the latter of which may be C-linked, as in deoxysugars, or O-linked as a methyl ether or ester. The FTIR spectra of the cell walls will reflect the presence, abundance, and chemical environment of each unique group, resulting in a very specific spectral fingerprint for each strain. As with Gram-positive bacteria, Gram-negative cells also produce other cell surface components, such as flagella, pili, and membrane bound porin proteins, but the tremendous variation in O and K antigen structures yields the maximal discriminatory possibilities in chemometric analysis.

## 5 APPLICATIONS OF IR SENSORS FOR PATHOGEN DETECTION

FTIR methods that can accurately and rapidly identify, classify, quantify, and/or differentiate between many types of bacteria have been reported [2, 3, 8, 26–29]. FTIR is a physicochemical method that allows the chemically based discrimination of intact cells without their destruction and produces complex whole-organism biochemical fingerprints (spectra) that are reproducible and distinct for different bacteria [30]. Spectra can also be collected from cell components and used in pathogen detection and identification [31–33]. A reference library of spectra must be collected for each bacteria of interest, ideally spanning a range of concentrations, growth conditions, and spectral collection parameters. This spectral library is then used to develop chemometric analytical approaches for further sample analysis, such as pathogen detection, differentiation, and/or quantification. Commercial bacterial spectral libraries (e.g. Bruker optics) are available for different species and strains of *Staphylococcus*, *Pseudomonas*, *Bacillus*, *Clostridium*, yeasts, and other microorganisms; however, there is no standard FTIR spectral library for everything.

A wide range of FTIR techniques and scanning conditions have been used for collecting spectra of bacteria. Common techniques are

1. transmission FTIR [16, 26, 27, 29, 34–50],
2. diffuse reflectance FTIR [13, 30, 51],
3. attenuated total reflectance (ATR) FTIR [5, 30–33, 52–60].

Other FTIR techniques that have been used for bacterial analysis include specular reflectance spectroscopy (for study of surfaces), photoacoustic spectroscopy (PAS, for studying highly absorbing samples) [28], and IR microspectroscopy [46, 48].

Scanning conditions are often controlled by manipulating the number of scans, the resolution, and the wavenumber region. In the techniques referenced above, the number of scans ranged from 16 to 256, and the resolution varied from 2 to 16. The number of scans and resolution used should be based on optimizing the signal-to-noise ratio (SNR) for the analysis and available time; increasing the number of scans will increase the time for the analysis, although each scan generally takes less than one second to complete. The SNR can be increased by signal averaging over a number of scans ($n$), leading to an increase of SNR proportional to the square root of the number of scans as follows:

$$SNR \propto (n)^{1/2} \tag{2}$$

However, it is important to note that an increase in the number of scans will not necessarily improve the quality of the spectrum because of variations in the atmosphere over time. SNR can be altered by changing other instrumentation parameters as follows [4, 6]:

- SNR $\alpha$ (measurement time)$^{1/2}$
- SNR $\alpha$ resolution
- SNR $\alpha$ 1/(elapsed time between background and sample).

There is no advantage to decreasing the wavenumber region (4000–400 cm$^{-1}$) over which data is collected because spectral regions within the entire region can be selected and analyzed after complete spectra are collected. Many FTIR spectrometers have a wavenumber cutoff near 700–650 cm$^{-1}$, thereby shortening the useful wavenumber region to 4000–700 cm$^{-1}$.

### 5.1 FTIR Calibration Models

After a spectral library of foodborne pathogens is developed, spectral library searching can be done to compare an unknown spectrum to a collection of known foodborne pathogen spectra, with the resulting "hit quality index" providing a measure of similarity between two spectra [6]. Beyond the general library search, a calibration model can be developed in a two-step process (calibration and validation) to enable detection, differentiation, and quantification of foodborne pathogens. For calibration, spectra are collected from the samples of interest, which contain foodborne pathogens in parallel with standard plate count or other enumeration and identification procedures. This calibration spectra set (also called the *training set*) is used to relate the standard identification/quantification

results to the spectra. Chemometrics, multivariate techniques such as partial least squares and principal components regression, are recommended for analyzing food pathogen spectra that contain overlapping absorbance bands [11–18]. An important advantage of using multivariate methods is the ability to calibrate for foodborne pathogen types and concentrations when they correlate in a complicated, nonspecific way with multiple spectral regions. Validation of the calibration model is done using an independent set of spectra, called the *validation set*, collected from samples with known foodborne pathogen types and concentrations. If results from the validation set fall within acceptable accuracy limits using the calibration model (sometimes reported as root mean square error of prediction (RMSEP) or predicted residual error sums of squares (PRESS)), then the model can be used for analyzing new spectra. Note: it can take numerous samples, sometimes hundreds, to develop a robust calibration model; however, once developed, this model should be indefinitely useful for analyzing samples prepared following the same procedures used in developing the model [10].

## 5.2 Detection

Detecting pathogenic bacteria in a sample using FTIR spectra can be done by (i) identifying a spectral change from the baseline spectra of an uncontaminated sample (food, growth media, antibody-coated capture surface, etc.), and conducting a spectral library search to determine the presence of a known type of bacteria or (ii) identifying an increasing absorbance in the spectral regions characteristic to a bacteria (again verified through a library search) as samples are incubated and spectra recorded over time (Fig. 3). Using the first approach, a change from the baseline will indicate the presence of bacteria, but may not distinguish between living and dead cells (although there may be differences in the spectra of living and dead cells). Differences from a baseline can also be used to detect other bacteria or chemical agents in the sample as long as a spectrum of the "adulterant" is available. A likely more robust and feasible approach for using an IR sensor for differentiating between live and dead cells would be based on cell growth as described in the second approach. This approach would require more time than the first to allow for cell growth and repetitive sampling to establish the increasing absorbances due to increasing cell numbers, but an advantage gained is that these increases in absorbances can also be used to quantify the number of bacteria in the sample.

In the absence of a food matrix, the detection limit of an FTIR microscope is 100 bacterial cells, and differentiation studies are reliable using $10^3$ cells [2, 3, 61]. A benchtop FTIR system was able to detect bacteria when 40 cells were present in the IR beam area [9]; however, this approach required $\sim 10^6$ cells/ml to locate the needed cell number in the beam area due to the comparatively large ATR FTIR crystal surface area.

As samples become more complex than a single strain of cultured bacteria, the number of cells needed for detection (and differentiation and quantification) increases. Numerous spectral analytical approaches have been used to detect the presence of a specific bacteria in a mixture [5, 18, 44, 45, 57, 61, 62]. To reduce the complexity of a sample, traditional microbiological enrichment or selection techniques, or capture techniques, can be used to concentrate the desired bacteria before spectra collection. For example, an antibody capture system such as Dynabeads could be used to bind a target pathogen (such as the *E. coli* O157:H7 bound to Dynabeads; Fig. 4), and spectra of the bound bacteria could be collected to verify the presence of that pathogen. This approach could also

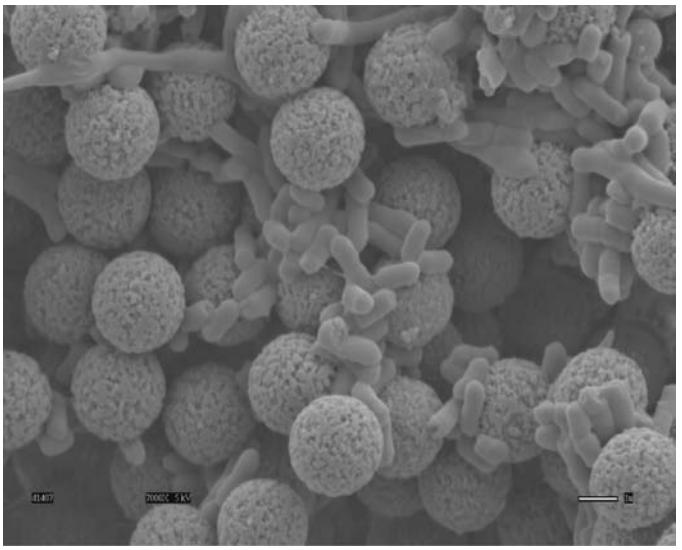


**FIGURE 4** Scanning electron micrograph image of *E. coli* O157:H7 captured on Dynabeads.

be used to determine if there is cross-reactivity of the capture antibody with nontarget microorganisms on the basis of spectral differences between different bacteria.

### 5.3 Differentiation

FTIR methods have been used for discrimination and classification of various microorganisms based on taxonomical classification, susceptibility to environmental stress, and type of growth medium. To enable differentiation, there must be structural differences between samples that appear as spectral differences (different spectral fingerprints based on absorbance peak differences, differing heights, and/or widths of peaks), and the differences must be consistent so that chemometric analyses developed for the spectral libraries and/or spectral-library-matching algorithms will be widely applicable to the samples of interest.

Examples of IR methods and approaches used for bacterial differentiation are listed here. Seven species of *Listeria* and five different serotypes of *L. monocytogenes* were successfully classified using FTIR in combination with discriminant analysis [27]. Discrimination of several distinct microorganisms (*Bacillus amyloliquifacens*, *Bacillus cereus*, *Bacillus subtilis*, *Citrobacter frendii*, *E. coli*, *Listeria innocua*, *Pseudomonas aeruginosa*, *Staphylococcus aureus*, and *Staphylococcus epidermis*) was also successfully achieved with FTIR [63, 64]. A second derivative FTIR spectral method was used as a rapid screening technique for identifying *E. coli* susceptible to $\beta$-lactam and the transconjugants [53]. FTIR methods were also developed to differentiate and detect bacteria (including *E. coli* O157:H7), yeast, and fungi on the surface of food such as an apple or in an apple juice matrix [28, 58, 65]. FTIR analyses discriminated between intact and sonication-injured cells of *L. monocytogenes* [56]. Identification of foodborne bacteria such as *Bacillus*, *Vibrio*, *E. coli*, and others by profiling their fatty acid methyl esters (FAMEs) using ATR FTIR spectroscopy has been reported [66].

### 5.4 Quantification

Because IR spectra follow the Beer–Lambert law relationship (Eq. (1)), the intensities/heights of the absorbance bands are related to the concentrations of functional groups or cells in the sample. Controlled parallel experiments of spectra collection and traditional enumeration methods (such as plate counts) must be used to develop an FTIR spectral database of known concentrations/cell counts of the bacteria of interest and calibration curve based on absorbance levels. Using FTIR, calibration curves were successfully constructed for a two-component system of defined microorganisms to determine their concentrations [45]. Yang et al. [67] used ATR FTIR to enumerate bacteria in foods. In addition to quantifying bacteria, FTIR approaches have also been used to quantify polysaccharides in bacteria [68], for monitoring biofilms [69–71], and for quantifying dextrose uptake in *Candida albicans* microcolonies [40].

### 5.5 Cost Considerations

A major consideration for determining cost and usefulness of a pathogen detection technique is the amount of time required for detection. A summary of time required for pathogen detection by various methods is provided in Table 2. Data collection and analysis using FTIR require less than 30 min (as shown in the biosensors column in Table 2). Currently, the majority of time required for FTIR detection techniques is dependent on sample preparation, for example, enrichment, capture, and drying. A filtration approach used by Burgula et al. [5] reduced the time to detection by rapidly concentrating bacteria suspended in liquids onto a filter and then collecting spectra of the filter surface. Approximately, 100 bacterial cells are needed in the IR beam to enable detection [2, 3]; however, currently more than 100 cells are needed to rapidly concentrate 100 cells in the small area needed. Prices for FTIR spectrometers range from $10,000 to above $100,000 depending on detector types, manufacturer, crystal types (ZnSe crystals cost between $500 and $1000 while diamond crystals are closer to $10,000, but diamonds do not scratch and therefore have an indefinite use expectancy while ZnSe crystals last 6 months to 1 year), and so on. Some FTIR systems require a liquid nitrogen source for cooling. Beyond the initial equipment costs, the cost per sample can be quite low if standard growth media and filtration devices are used.

## 6 CRITICAL NEEDS ANALYSIS

Despite the potential of FTIR spectroscopy to detect and discriminate bacteria, there are limited spectral libraries available and limited studies on differentiation between stressed, dead, and live pathogens. The ability to discriminate between live and dead cells in a food matrix is critical for food safety applications and for making an effective estimate of the number of viable bacteria in foods. There is also a critical need to improve sample handling procedures before introducing the sample onto the FTIR for spectral analysis. Selective capture and concentration techniques are needed to rapidly isolate pathogens from foods; the isolates can be placed on a membrane, filter, crystal, or other surface, and then spectra of these isolates can be collected in a few minutes (again, an FTIR is capable of approximately one scan per second, so the number of scans influences the time needed to generate spectra).

**TABLE 2 Time Comparisons for Pathogen Detection by Various Methods**

| | Detection Time (h) | | | | |
|---|---|---|---|---|---|
| Steps | Conventional Culture | PCR | ELISA | IMS | Biosensors |
| Enrichment | 18–48 | 18–24 | 8–24 | 36–48 | 6–?? |
| Plating | 18–48 | — | — | 18–48 | — |
| DNA extraction | — | 0.5–1.5 | — | — | — |
| Bio- and chemical test | 5–24 | — | — | — | — |
| Serology | 4 | — | — | — | — |
| IMS bead extraction | — | — | — | 0.5 | — |
| Assay | — | 3–4 | 2–4 | — | 0.5 |
| Total time | 3–6 d | 21.5–29.5 h | 10–28 h | 2.5–4 d | 6.5 h–?? |

(Adapted from Dynal [72] and Rand et al. [73])
PCR = polymerase chain reaction
ELISA = enzyme-linked immunosorbent assay
IMS = immunomagnetic separation

## 7 RESEARCH DIRECTIONS

Although FTIR and spectral analysis methods have enabled identification and discrimination of bacteria, barriers to widespread use of this approach include sample preparation (such as 6–8 h culturing on agar media or broth), the sensitivity of the FTIR accessory and analysis used, interference from water absorbance, and the relative expense associated with crystal ATR FTIR surface materials. Research is needed to improve the sample preparation steps, thereby reducing the time for detection. Progress in rapidly concentrating and isolating pathogens from foods will reduce the overall time needed for pathogen detection. By improving sensitivity and specificity of spectral collection and analysis and reducing the time needed for sample preparation, FTIR methods have many potential applications for rapid detection of pathogens from foods.

## REFERENCES

1. Smith, A. L. (1979). *Applied Infrared Spectroscopy: Fundamentals, Techniques, and Analytical Problem Solving*, John Wiley & Sons, New York.
2. Naumann, D., Helm, D., and Labischinski, H. (1991). Microbiological characterizations by FT-IR spectroscopy. *Nature* **351**(6321), 81–82.
3. Naumann, D., Helm, D., Labischinski, H. and Giesbrecht, P. (1991). The characterization of microorganisms by Fourier transform infrared spectroscopy (FT-IR). In *Modern Techniques for Rapid Microbiological Analysis*, W. H. Nelson, Ed. VCH, New York, pp. 67–85.
4. Smith, B. C. (1996). *Fundamentals of Fourier Transform Infrared Spectroscopy*, CRC Press, Boca Raton, FL.
5. Burgula, Y., Khali, D., Krishnan, S. S., Cousin, M. A., Gore, J. P., Reuhs, B. L., and Mauer, L. J. (2006). Detection of *E. coli* O157:H7 and *Salmonella* Typhimurium using filtration followed by FT-IR spectroscopy. *J. Food Prot.* **69**(8), 1777–1784.
6. Smith, B. C. (1999). *Infrared Spectral Interpretation, A Systematic Approach*, CRC Press, Washington, DC.

7. Naumann, D., Schultz, C., and Helm, D. (1996). What can Infrared Spectroscopy tell us about the structure and composition of intact bacterial cells. In *Infrared Spectroscopy of Biomolecules*, H. H. Mantsch, and D. Chapman, Eds. Wiley-Liss, New York, pp. 279–310.
8. Mariey, L., Signolle, J. P., Amiel, C., and Travert, J. (2001). Discrimination, classification, identification of microorganisms using FTIR spectroscopy and chemometrics. *Vib. Spectrosc.* **26**, 151–159.
9. Burgula, Y., Khali, D., Kim, S., Cousin, M. A., Gore, J. P., Reuhs, B. L., and Mauer, L. J. (2007). Review of Mid-IR Fourier-transform infrared (FT-IR) spectroscopy applications for bacterial detection. *J. Rapid Methods Autom. Microbiol.* **15**, 146–175.
10. Beebe, K. R., Pell, R. J., and Seasholtz, M. B. (1998). *Chemometrics: A Practical Guide*, John Wiley & Sons, New York.
11. Freeman, R., Goodacre, R., Sisson, P. R., Magee, J. G., Ward, A. C., and Lightfoot, N. F. (1994). Rapid identification of species within the *Mycobacterium tuberculosis* complex by artificial neural network analysis of pyrolysis mass spectra. *J. Med. Microbiol.* **40**(3), 170–173.
12. Goodacre, R., Neal, M. J., Kell, D. B., Greenham, L. W., Noble, W. C., and Harvey, R. G. (1994). Rapid identification using pyrolysis mass spectrometry and artificial neural networks of *Propionibacterium acnes* isolated from dogs. *J. Appl. Bacteriol.* **76**, 124–134.
13. Goodacre, R., Timmins, E. M., Burton, R., Kaderbhai, N., Woodward, A. M., Kell, D. B., and Rooney, P. J. (1998). Rapid identification of urinary tract infection bacteria using hyperspectral, whole-organism fingerprinting and artificial neural networks. *Microbiology* **144**(5), 1157–1170.
14. Beksac, M., Beksac, M. S., Tipi, V. B., Duru, H. A., Karakas, M. U., and Cakar, A. N. (1997). An artificial intelligent diagnostic system on differential recognition of hematopoietic cells from microscopic images. *Cytometry* **30**(3), 145–150.
15. Kirschner, C., Ngo-Thi, N. A., and Naumann, D. (1999). In *Spectroscopy of Biological Molecules: New Directions*, J. Greve, G. J. Puppels, and C. Otto, Eds. Kluwer Academic Publishers, Dordrecht, pp. 557–558.
16. Udelhoven, T., Naumann, D., and Schmitt, J. (2000). Development of a hierarchical classification system with artificial neural networks and FT-IR spectra for the identification of bacteria. *Appl. Spectrosc.* **54**(10), 1471–1479.
17. Argov, S., Ramesh, J., Salman, A., Sinelnikov, I., Goldstein, J., Guterman, H., and Mordechai, S. (2002). Diagnostic potential of Fourier-transform infrared microspectroscopy and advanced computational methods in colon cancer patients. *J. Biomed. Opt.* **7**(2), 1–7.
18. Gupta, M. J., Irudayaraj, J. M., Schmilovitch, Z., and Mizrach, A. (2006). Identification and quantification of foodborne pathogens in different food matrices using FTIR spectroscopy and artificial neural networks. *Trans. ASABE* **49**(4), 1249–1255.
19. Naumann, D. (2000). Infrared spectroscopy in microbiology. In *Encyclopedia of Analytical Chemistry*, R. A. Meyers, Ed. John Wiley and Sons, Chichester, pp. 102–131.
20. Seltmann, G., and Holst, O. (2002). *The Bacterial Cell Wall*, 1 ed., Springer Publishing Company, Boston, MA.
21. Fischetti, V. A., and Beveridge, T. J. (2006). In *Gram-positive pathogens*, V. A. Fischetti, R. P. Novick, F. F. Ferretti, D. A. Portnoy, and J. I. Rood, Eds. ASM Press, Washington, DC, pp. 3–24.
22. Whitfield, C., and Valvano, M. A. (1993). Biosynthesis and expression of cell-surface polysaccharides in Gram-negative bacteria. *Adv. Microb. Phys.* **35**, 135–246.
23. Whitfield, C. (1995). Biosynthesis of lipopolysaccharide O antigens. *Trends Microbiol.* **3**, 178–185.

24. Jann, K., and Jann, B. (1991). Biochemistry and expression of bacterial capsules. *Biochem. Soc. Trans.* **19**, 623–628.
25. Whitfield, C., and Roberts, S. (1999). Structure, assembly, and regulation of expression of capsules in *E. coli*. *Mol. Microbiol.* **31**, 1307–1319.
26. Haag, H., Gremlich, H., Bergmann, R., and Sanglier, J. (1996). Characterization and identification of actinomycetes by FT-IR spectroscopy. *J. Microbiol. Methods* **27**, 157–163.
27. Lefier, D., Hirst, D., Holt, C., and Williams, A. G. (1997). Effect of sampling procedure and strain variation in *Listeria monocytogenes* on the discrimination of species in the genus *Listeria* by Fourier transform infrared spectroscopy and canonical variates analysis. *FEMS Microbiol. Lett.* **147**, 45–50.
28. Irudayaraj, J., Yang, H., and Sakhamuri, S. (2002). Differentiation and detection of microorganisms using Fourier transform infrared photoacoustic spectroscopy. *J. Mol. Struct.* **606**, 181–188.
29. Oust, A., Moretro, T., Kirschner, C., Narvhus, A. J., and Kohler, A. (2004). FT-IR spectroscopy for identification of closely related lactobacilli. *J. Microbiol. Methods* **59**, 149–162.
30. Goodacre, R., Timmins, E., Rooney, P., Rowland, J., and Kell, D. (1996). Rapid identification of Streptococcus and Enterococcus species using diffuse reflectance-absorbance Fourier transform infrared spectroscopy and artificial neural networks. *FEMS Microbiol. Lett.* **140**, 233–239.
31. Kim, S., Reuhs, B. L., and Mauer, L. J. (2005). Differentiation and classification of crude lipopolysaccharides from *Salmonella* strains using Fourier transform infrared spectroscopy and chemometrics. *J. Appl. Microbiol.* **99**, 411–417.
32. Kim, S., Kim, H., Reuhs, B. L., and Mauer, L. J. (2006b). Differentiation of outer membrane proteins from *Salmonella enterica* serotypes using Fourier transform infrared spectroscopy and chemometrics. *Lett. Appl. Microbiol.* **42**, 229–234.
33. Kim, S., Burgula, Y., Ojanen-Reuhs, T., Cousin, M. A., Reuhs, B. L., and Mauer, L. J. (2006a). Differentiation and classification of crude lipopolysaccharides from *Eschericia coli* strains using Fourier transform infrared spectroscopy and chemometrics. *J. Food Sci.* **71**(2), M57–M61.
34. Helm, D., Labischinski, H., and Naumann, D. (1991a). Elaboration of a procedure for identification of bacteria using Fourier-transform infrared spectral libraries: A stepwise correlation approach. *J. Microbiol. Methods* **14**(2), 127–142.
35. Helm, D., Labischinski, H., Schallen, H., and Naumann, D. (1991b). Classification and identification of bacteria by Fourier-Transform infrared spectroscopy. *J. Gen. Microbiol.* **137**, 69–79.
36. Naumann, D., Keller, S., Helm, D., Schultz, C., and Schrader, B. (1995). FT-IR Spectroscopy and FT-Raman Spectroscopy are powerful analytical tools for the non-invasive characterization of intact microbial cells. *J. Mol. Struct.* **347**, 399–406.
37. Beattie, S., Holt, C., Hirst, D., and Williams, A. (1998). Discrimination among *Bacillus cereus*, *B*. mycoides and *B*. thuringiensis by Fourier Transform Infrared Spectroscopy. *FEMS Microbiol. Lett.* **164**, 201–206.
38. Chen, L., Carpita, N., Reiter, W., Wilson, R., Jeffries, C., and McCann, M. (1998). A rapid method to screen for cell wall mutants using discriminant analysis of Fourier transform infrared spectra. *Plant J.* **16**, 385–392.
39. Schuster, K., Mertens, F., and Gapes, J. (1999). FTIR spectroscopy applied to bacterial cells as a novel method for monitoring complex biotechnological processes. *Vib. Spectrosc.* **19**(2), 467–477.

40. Orsini, F., Ami, D., Villa, A. M., Sala, B., Bellotti, M. G., and Doglia, S. M. (2000). FT-IR microspectroscopy for microbiological studies. *J. Microbiol. Methods* **42**(Special Issue 1), 17–27.
41. Mossoba, M., Khambaty, F., and Fry, F. (2002). Novel Application of a Disposable Optical Film to the Analysis of Bacterial Strains: A Chemometric Classification of Mid-infrared Spectra. *Appl. Spectrosc.* **56**, 732–736.
42. Mossoba, M., Al-Khaldi, S., Kirkwood, J., Fry, F., Sedman, J., and Ismail, A. A. (2005). Printing microarrays of bacteria for identification by infrared microspectroscopy. *Vib. Spectrosc.* **38**, 229–235.
43. Oberreuter, H., Seiler, H., and Siegfried, S. (2002). Identification of coryneform bacteria and related taxa by Fourier-transform infrared (FT-IR) spectroscopy. *Int. J. Syst. Evol. Microbiol.* **52**, 91–100.
44. Oberreuter, H., Brodbeck, A., Von Stetten, S., Goerges, S., and Scherer, S. (2003). Fourier-transform infrared (FT-IR) spectroscopy is a promising tool for monitoring the population dynamics of microorganisms in food stuff. *Eur. Food Res. Technol.* **216**, 434–439.
45. Oberreuter, H. (1998). Quantification of microorganisms in mixed cultures with FTIR spectroscopy. *Workshop FTIR Spectroscopy in Microbiological and Medical Diagnostics*, Berlin, Oct. 15–16.
46. Wenning, M., Seiler, H., and Scherer, S. (2002). Fourier-transform Infrared Microspectroscopy, a novel and rapid tool for identification of yeasts. *Appl. Environ. Microbiol.* **68**, 4717–4721.
47. Guibet, F., Amiel, C., Cadot, C., Cordevant, C., Desmonts, M. H., Lange, M., Marecant, A., Travert, J., Denis, C., and Mariey, L. (2003). Discrimination and classification of *Enterococci* by Fourier transform infrared (FT-IR) spectroscopy. *Vib. Spectrosc.* **33**, 133–142.
48. Ngo-Thi, N. A., Kirschner, C., and Naumann, D. (2003). Characterization and identification of microorganisms by FT-IR microspectrometry. *J. Mol. Struct.* **661–662**, 371–380.
49. Foster, N. S., Thompson, S. E., Valentine, N. B., Amonette, J. E., and Johnson, T. J. (2004). Identification of sporulated and vegetative bacteria using statistical analysis of Fourier Transform mid-infrared transmission data. *Appl. Spectrosc.* **58**, 203–211.
50. Melin, A., Allery, A., Perromat, A., Bebear, C., Deleris, G., and Barbeyrac, B. (2004). Fourier transform infrared spectroscopy as a new tool for characterization of mollicutes. *J. Microbiol. Methods* **56**, 73–82.
51. Gomez, M. A., Perez, M. A., Gil, F. J., Diez, A., Rondriguez, J. F., Rondriguez, P., Domingo, A., and Torres, A. (2003). Identification of species of *Brucella* using Fourier Transform Infrared Spectroscopy. *J. Microbiol. Methods.* **55**, 121–131.
52. Helm, D., and Naumann, D. (1995). Identification of some bacterial cell components by FT-IR spectroscopy. *FEMS Microbiol. Lett.* **126**, 75–80.
53. Bouhedja, W., Sockalingum, G. D., Pina, P., Allouch, P., Bloy, C., Labia, R., Millot, J. M., and Manfait, M. (1997). ATR-FTIR spectroscopic investigation of *E. coli* transconjugants beta-lactams-resistance phenotype. *FEBS Lett.* **412**(1), 39–42.
54. Ellis, D., Broadhurst, D., Kell, D., Rowland, J., and Goodacre, R. (2002). Rapid and quantitative detection of the microbial spoilage of meat by Fourier transform infrared spectroscopy and machine learning. *Appl. Environ. Microbiol.* **68**, 2822–2828.
55. Lin, M., Al-Holy, M., Chang, S.-S., Huang, Y., Cavinato, A. G., Kang, D.-H., and Rasco, B. A. (2005). Rapid discrimination of *Alicyclobacillus* strains in apple juice by Fourier transform infrared spectroscopy. *Int. J. Food Microbiol.* **105**, 369–376.
56. Lin, M., Al-Holy, M., Al-Quadri, H., Kang, D. H., Cavinato, A. G., Huang, Y., and Rasco, B. A. (2004). Discrimination of intact and injured *Listeria monocytogenes* by Fourier

transform infrared spectroscopy and principal component analysis. *J. Agric. Food Chem.* **52**, 5769–5772.

57. Yu, C., and Irudayaraj, J. (2005). Spectroscopic characterization of microorganisms by Fourier transform infrared microspectroscopy. *Biopolymers* **77**, 368–377.
58. Yu, C., Irudayaraj, J., Debroy, C., Schmilovitch, Z. E., and Mizrach, A. (2004). Spectroscopic differentiation and quantification of microorganisms in apple juice. *J. Food Sci.* **69**, S268–S272.
59. Al-Holy, M., Lin, M., Cavinato, A. G., and Rasco, B. A. (2006). The use of Fourier transform infrared spectroscopy to differentiate *Escherichia coli* O157:H7 from other bacteria inoculated into apple juice. *Food Microbiol.* **23**, 162–168.
60. Sivakesava, S., Irudayaraj, J., and Debroy, C. (2004). Differentiation of microorganisms by FTIR-ATR and NIR spectroscopy. *Trans. ASABE* **7**, 951–957.
61. Gupta, M. J., Irudayaraj, J. M., Debroy, C., Schmilovitch, Z., and Mizrach, A. (2005). Differentiation of food pathogens using FTIR and artificial neural networks. *Trans. ASABE* **48**(5), 1889–1892.
62. Gupta, M. J., and Irudayaraj, J. (2004). Spectroscopic quantification of bacteria using artificial neural networks. *J. Food Prot.* **67**(11), 2550–2554.
63. Ngo-Thi, N. A., Kirschner, C., Naumann, D. (1999). In *Spectroscopy of Biological Molecules*, J. Greve, G. J. Puppels, and C. Otto, Eds. Kluwer Academic Publishers, Dordrecht.
64. Rodriguez-Saona, L. E., Khambaty, F. M., Fry, F. S., and Calvey, E. M. (2001). Rapid detecton and identification of bacterial strains by Fourier transform near-infrared spectroscopy. *J. Agric. Food Chem.* **49**, 574–579.
65. Rodriguez-Saona, L. E., Khambaty, F. M., Fry, F. S., Dubois, J., and Calvey, E. M. (2004). Detection and identification of bacteria in a juice matrix with Fourier transform-near infrared spectroscopy and multivariate analysis. *J. Food Prot.* **67**, 2555–2559.
66. Whittaker, P., Mossoba, M., Al-Khaldi, S., Fry, F., Cunkel, B., Tall, D., and Yurawecz, M. P. (2003). Identification of foodborne bacteria by infrared spectroscopy using cellular fatty acid methyl esters. *J. Microbiol. Methods* **55**, 709–716.
67. Yang, H., Ibrahim, S. A., and Seo, C. W. (2005). *Rapid detection, identification, and enumeration of bacteria in foods using FTIR-ATR spectroscopy with chemometrics*, Abstracts of Papers of the ACS 229: U50-U50 135-AGFD Part 1.
68. Marcotte, L., Kegelaer, G., Sandt, C., Barbeau, J., and Lafleur, M. (2007). An alternative infrared spectroscopy assay for the quantification of polysaccharides in bacterial samples. *Anal. Biochem.* **361**, 7–14.
69. Bremer, P. J., and Geesey, G. G. (1991). An evaluation of biofilm development utilizing non-destructive attenuated total reflectance Fourier transform infrared spectroscopy. *Biofouling.* **3**, 89–100.
70. Nivens, D., Schmit, E., Sniatecki, J., Anderson, T., Chambers, J. Q., and White, D. C. (1993). Multichannel ATR/FT-IR spectrometer for on-line examination of microbial biofilms. *Appl. Spectrosc.* **47**, 668–671.
71. Geesey, G. G., and Suci, P. A. (2000). Monitoring biofilms by Fourier transform infrared spectroscopy. In *Biofilms: recent advances in their study and control*, L. V. Evans, Ed. Harwood Academic Publishers, Amsterdam, pp. 253–277.
72. Dynal (2003). *Subject:* Enrichment of *Salmonella - Package Insert*. http://www.dynalbiotech.com/kunder/dynal/DynalPub401.nsf/frames/index.html?open&6=/$all/17E631FD8EEF0836C1256C5400488E13.
73. Rand, A., Ye, J., Brown, C., and Letcher, S. (2002). Optical Biosensors for Food Pathogen Detection. *Food Technol.* **56**(3), 32–39.

# PULSENET: A PROGRAM TO DETECT AND TRACK FOOD CONTAMINATION EVENTS

KARA L. F. COOPER, DUNCAN R. MACCANNELL, AND EFRAIN M. RIBOT
*Centers for Disease Control and Prevention, Atlanta, Georgia*

## 1 INTRODUCTION

An estimated 76 million cases of foodborne illness occur each year in the United States [1], with many more that likely go unreported. The striking incidence of foodborne disease highlights the importance of effective surveillance for the rapid detection of outbreak clusters, and the role that these programs have in maintaining the safety of our food supply [2–5]. In recent years, a number of well-publicized outbreaks have been associated with widely distributed food products. Each outbreak underscores the potential vulnerability of our food supplies to microbial contamination, the threat to public health, and the potential impact to national and international security.

Contamination can occur at any stage of food production, from the originating farm or producer, through processing, packaging, shipping and storage, all the way to the consumer's table. Although changes in regulation, education, and technology over the course of the past century have resulted in an overall improvement in the safety of the foods we eat [2, 4], changing dietary habits and demand for increased variety and seasonality of many food products presents an important challenge to food safety, particularly when many foods are imported from abroad and/or consumed in an uncooked format. Today, many commercially prepared foods are produced or processed at centralized facilities and are widely distributed prior to consumption. Both of these factors facilitate the emergence of disseminated outbreaks, and foodborne contamination may impact multiple counties, states, or countries [6]. Furthermore, the complexity of these production and distribution networks can delay the recognition of foodborne outbreaks or hinder the identification and recall of contaminated products [2–4, 7]. The rapid detection of disease clusters is the critical function of PulseNet, and their association with outbreaks of foodborne disease combines traditional epidemiology with real-time, laboratory-based surveillance systems. In order to be effective, it also requires sufficient coverage, and the active participation of laboratorians and epidemiologists at both the state and federal levels [3, 8, 9].

PulseNet USA was established in 1996 to provide a unified infrastructure for the molecular surveillance of foodborne bacterial infections, and has significantly increased our ability to detect and act upon clusters of foodborne illness by standardizing and coordinating bacterial subtyping in public health laboratories nationwide [10, 11]. Participating laboratories compare DNA fingerprints from foodborne isolates across the country in near real time, and can compare these fingerprints to those from a suspected vehicle or source during the course of an investigation. This secondary capability is particularly

**TABLE 1 Examples of International Outbreaks of Bacterial Foodborne Outbreaks Recognized through PulseNet, 1995–2006**

| Year | Organism | Cases | Countries Involved | Implicated Vehicle | Reference |
|---|---|---|---|---|---|
| 1995 | *S.* Stanley | 250+ | Finland, USA | Alfalfa sprouts | Mahon [51] |
| 1998 | *Shigella sonnei* | 172 | Canada, USA | Parsley | MMWR [31] |
| 1999 | *S.* Muenchen | 207 | Canada, USA | Unpasteurized Orange Juice | MMWR [31] |
| 2000–2001 | *S.* Enteritidis | 168 | Canada, USA | Raw Almonds | Chan [28] |
| 2000–2002 | *S.* Poona | | Canada, Mexico, USA | Cantaloupe | MMWR [29] |
| 2001 | *S.* Oranienburg | 500+ | Austria, Belgium, Denmark Finland, Germany, Croatia Netherlands, Czech Repulic | Chocolate | Werber [27] |
| 2004 | *S.* Enteritidis | 29 | Canada, USA | Raw Almonds | MMWR [30] |
| 2004 | *E. coli* O157:H7 | 3 | Japan, USA | Ground Beef | MMWR [52] |
| 2006 | *E. coli* O157:H7 | 200+ | Canada, USA | Fresh spinach | MMWR [25] |

useful during traceback investigations, and is critical to both attribution and prevention/control efforts [9, 11, 12]. Hundreds of outbreak clusters are identified by PulseNet laboratories each year, prompting dozens of outbreak investigations. From the perspective of biosecurity and preparedness, many of the lessons learned from the investigation and follow up of these cases are equally applicable to scenarios involving intentional contamination. The PulseNet community is committed to improving the capacity and technology needed to respond rapidly to emerging threats and limit the scope of foodborne infections, both within the United States and abroad.

## 2 SCIENTIFIC OVERVIEW

Molecular epidemiology combines the principles of traditional epidemiologic investigation with tools derived from molecular biology to better understand and define the distribution of diseases or markers of interest within a given population [7]. As technology continues to improve, the molecular strain typing of bacteria has evolved significantly, particularly with the introduction and refinement of modern genomic and proteomic approaches [13]. Today, epidemiologic studies of foodborne bacteria rely predominantly upon genotypic methods for characterization and strain type assignment. Although the sensitivity, specificity, and appropriateness of these techniques varies according to both organism and context, pulsed-field gel electrophoresis (PFGE), which involves macrorestriction and fragment analysis of the entire genome, remains the predominant means or "gold standard" for subtyping many bacteria [13, 14].

The application of sophisticated molecular subtyping methods, coupled with informatic platforms that enable rapid comparison and communication of subtyping data, has greatly increased the sensitivity of surveillance systems to detect clusters of foodborne illness that are widely dispersed in space or time [3, 11]. However, detection of a cluster is only the first step, and a rapid but thorough investigation is critical to identify the source of infection and mediate an effective response before additional and preventable cases occur. Molecular subtyping data is often central to this process, helping to separate outbreak-related cases from sporadic infections that would otherwise confound the investigation. Once a contaminated product or vehicle has been identified, molecular data may also be used to provide definitive microbiological confirmation of the source of the infection [2, 4, 7, 9, 12]. Equally, these data may be used in a detailed investigation of affected food production and distribution chains, which may reveal how contamination occurred, and facilitate the development and implementation of measures to prevent similar events in future.

## 3 PULSENET USA

PulseNet USA was established in 1996 in collaboration with the Association of Public Health Laboratories, and has grown from an initial group of five interested public health laboratories to over 70 participants, including county, municipal and state public health departments, federal food regulatory agencies, agricultural, and veterinary laboratories [12]. Standardized PFGE protocols are at the core of PulseNet USA, allowing participating laboratories to rapidly generate PFGE patterns or "fingerprints" that are consistent between laboratories [13, 15, 16]. Once an isolate has been run, the PFGE pattern is compared to other local isolates and uploaded to a centralized and secure database system at the Centers for Disease Control (CDC) in Atlanta. These pattern data are actively curated, with ongoing real-time surveillance for unusual pattern frequencies or trends that may indicate the emergence of an outbreak. The participation of laboratories throughout the country enables the exquisitely sensitive and rapid identification of foodborne outbreak clusters, particularly those that are disseminated over a broad geographic area or protracted period of time.

An important key to the success of PulseNet USA has been the decentralization of subtyping activities to state and local public health laboratories. This decentralized approach has greatly extended the testing capacity of the network, with rapid subtyping occurring on a local level, and without the logistical problems of a centralized testing facility [11, 12]. Decentralization presents its own challenges, however: in particular, the allocation of infrastructure (i.e. equipment, supplies, and trained personnel) and funding, the development and maintenance of highly standardized subtyping and analysis protocols for pathogens of interest, and a means of effective, rapid, and secure communication for data and alerts between network members.

PulseNet relies on the ability to compare data generated by different laboratories in near-real time, and it is therefore necessary to ensure that protocols are standardized, and that data may be rapidly exchanged and compared. Within the PulseNet community, PFGE gel images are analyzed using highly customized image analysis software (BioNumerics, Applied Maths, Sint-Martens-Latem, Belgium), that operate using a basic client–server architecture. Through this software, PFGE patterns and related epidemiological information can be compared against both the local (client) database and against

all patterns that have been submitted to the National database (server) at the CDC. Currently, PulseNet has standardized PFGE protocols and networked databases in place for *Escherichia coli* O157, *Salmonella, Shigella* spp., *Campylobacter, Listeria monocytogenes*, *Vibrio cholerae*, *Yersinia pestis*, and *Vibrio parahaemolyticus* [16–21].

To provide rapid and secure messaging between PulseNet laboratories, a web-based forum has also been implemented to provide rapid alerts to laboratorians and epidemiologists throughout the country, and to provide timely information to the PulseNet community on patterns, tentative clusters, and important administrative or methodological updates. Together, the combination of highly standardized molecular protocols, database-driven curated analysis, and real-time secure communications has led to the discovery of many outbreaks that would likely not have been identified with traditional epidemiological methods [9, 22, 23].

Among its successes, PulseNet was instrumental in the recent identification and investigation of an outbreak of *E. coli* O157:H7 that involved 205 cases from across the United States and Canada [24, 25]. Epidemiologic follow-up of the PulseNet-identified cluster confirmed that 95% of the infected individuals had reported eating fresh, uncooked spinach during the 10 days prior to illness. The association of fresh spinach as a common source was subsequently confirmed by the isolation of the outbreak strain from three open bags of spinach that were recovered from patients' homes. The rapid and conclusive identification of the contaminated food product and implicated lot numbers resulted in faster and more specific consumer advisories, narrowed the recall of affected food products, and almost certainly limited the scope and severity of the outbreak. The origin of the contaminated spinach was traced to fields in several California counties. PFGE analysis of a cross section of environmental isolates from the San Benito area identified an exact match to the outbreak pattern, isolating the likely point of contamination to within a very narrow geographic margin and improving our understanding of predisposing events [24, 26].

With over a decade of successes such as these, PulseNet has proven to be an important tool for detection, investigation, control, and prevention of foodborne outbreaks within the United States (Table 1). Since its inception, national participation has grown to include all 50 states, as well as county and municipal public health laboratories and food regulatory agencies. In an increasingly globalized economy, the internationalization of PulseNet is a logical progression, but one which requires the ongoing cooperation and commitment of many international partners. The expansion of PulseNet coverage into global markets may also help to enhance food safety within the United States by expediting the identification of contaminated imports before or shortly after they enter the domestic food supply. More importantly, PulseNet International will build upon the successful foundations of PulseNet USA to help us better understand the epidemiology and prevention of foodborne infections on a global scale, and enhance food safety and public health throughout the industrialized and developing world.

## 4 PULSENET INTERNATIONAL

Over the past several decades, consumer demand has driven an explosive increase in both the scale and diversity of international food trades [12, 27]. In today's global market place, foods that are produced, processed, and packaged in one part of the world are more likely than ever to cross national borders, for consumption in countries many hundreds or even

thousands of miles away. Foodborne outbreaks may extend well beyond a single region or country, involve multiple imported/exported food products and include, inconsistent recordkeeping, and complex distributorships [6]. These factors can all greatly complicate the identification and investigation of international outbreaks, particularly when the scope of most existing foodborne surveillance systems is limited. In order to adapt to these changing parameters, surveillance programs must look beyond national borders to consider the role of economic globalization, and its impact on the safety of domestic food supplies. Internationalization of programs such as PulseNet will help to safeguard food safety within the United States, among our trade partners and within developing nations, where food and waterborne infections continue to represent a significant cause of morbidity and mortality [12].

### 4.1 Structure and Function

PulseNet International was established as an umbrella organization for independent regional PulseNet networks to provide a cooperative framework for enhanced foodborne disease surveillance on a global scale [12]. Governed by a steering committee that is chaired by the chief of PulseNet USA, PulseNet International currently includes six participating regional networks (USA, Canada, Latin America, Europe, Asia-Pacific, and Middle East) that represent 67 countries across 6 continents (Fig. 1). Expansion onto the global stage began with an informal collaboration between PulseNet USA and Canadian public health officials in 1999. This collaboration proved to be useful almost immediately, with the investigation of an outbreak of 91 cases of *Salmonella enterica* serotype Muenchen in 15 US states and 2 Canadian provinces [28]. Standardized molecular subtyping was able to rapidly identify cases, and suggested an association with the consumption of unpasteurized orange juice, which was later confirmed by epidemiologic follow-up. Cooperation between Canadian and US public health laboratories continued to provide concrete results over the next several years, reinforcing the value of the open and rapid exchange of molecular subtyping information, and its potential—both as an early warning system and as a tool for the investigation of transnational outbreaks [29–34].

The success of this first international collaboration promoted the foundation of PulseNet International. Over the past 5 years, regular organizational meetings have been held between the CDC and public health officials from Canada, Europe, Asia-Pacific, Latin America, and the Middle East to continue expanding the role of PulseNet in global surveillance for foodborne disease. At many of these meetings, the focus has been on establishing necessary infrastructure within each of the regional networks, and the integration of each regional network into PulseNet International. Extensive progress has been made with training in PulseNet Standardized PFGE Protocols, software-assisted gel analysis, and establishment of consistent laboratory and analytic QA/QC programs across each regional network [12]. PulseNet International has the added challenge of establishing effective surveillance networks between regional and national partners, whose public health interests may be overshadowed or complicated by important geopolitical differences. The composition and organizational structure within each of the PulseNet International regional networks is flexible, and may differ according to political, economic, and cultural structures within its membership. Despite these challenges, all regional networks have reached consensus on most core operational


**FIGURE 1** Delineation of the six PulseNet International regions including PulseNet USA, PulseNet Canada, PulseNet Europe, PulseNet Asia-Pacific, PulseNet Latin America, and PulseNet Middle East [35].

issues, and identified appropriate means by which to ensure effective, and equitable laboratory-based surveillance programs between their members.

The rapid exchange and comparison of PFGE pattern data are critical to surveillance functions, and consequently, information technology infrastructure for database access and communications is as necessary as the development of laboratory resources in the field. Data issues are similarly complex, and difficulties have emerged related to the implementation and maintenance of network infrastructure, and the establishment of multilateral agreements for information management and exchange. An ideal compromise might permit PulseNet members to log on to different PulseNet International servers with limited read-only or volatile access to conduct simple queries. If pattern matches are identified that extend beyond the user's home network, relevant epidemiological information, such as isolate source, relevant dates, serotype, and PFGE pattern information would be provided, and outbreak coordinators from all affected jurisdictions would be alerted or invited to participate in an investigation.

The first step in these processes came with the signature of a Memorandum of Understanding between PulseNet USA and PulseNet Canada in 2005, which formalized data-sharing arrangements between the two nations. This agreement granted limited access and cross-querying to public health investigators in both countries.and permitted the direct comparison of PFGE data from Shiga toxin-producing *E. coli* (STEC) and *Salmonella*. It is hoped that this memorandum will be the first of many agreements, both within and between the other regional networks that make up PulseNet International. In the meantime, a secure PulseNet International ListServ has been established to exchange pattern data and communicate related epidemiological information between networks. This approach is more time consuming, since international investigations currently require managers from each regional/national database to manually compare new patterns against their own local pattern database and notify the ListServ if relevant matches are identified.

### 4.2 Food Safety and Bioterrorism: Critical Need for PulseNet International

In recent years, an increase in worldwide terrorist activity has raised the profile of biosecurity, and with it, concerns over the vulnerability of international food supplies to acts of intentional biological or chemical contamination. Biological contamination is of particular concern, since pathogenic microorganisms are relatively easy to acquire, and in the case of bacteria, may be manufactured relatively quickly in significant quantities, with only limited budget and expertise [36–38]. Intentional contamination that occurs early in the supply chain, or before the food leaves its country of origin, may have broad international effects, since contaminated lots may be distributed to multiple countries and sold for consumption well before the contamination is detected. Although the importance of biosecurity has increased in many segments of the food production and trade industries, many aspects of international food supply chain remain vulnerable to attack, and naturally occurring outbreaks involving food imports highlight the feasibility and importance of this threat [38].

Historically, only a handful of cases of foodborne disease have been definitively linked to intentional contamination. A retrospective study of outbreak investigations revealed that 44 (4%) out of 1099 involved causative agents with bioterrorism potential, and of those, intentional contamination was considered as a potential explanation in only six [36]. Modern commercial food distribution systems provide an ideal delivery vehicle for widespread terrorist effect, and the threat, or even perceived threat of intentional contamination of the food supply, reinforces the importance of protection and surveillance as national security priorities [36–38].

It is likely that the intentional contamination of a widely distributed food product will initially resemble the emergence of a naturally occuring outbreak of foodborne disease, with a sudden increase in incident cases, and the implication of a well-known foodborne enteric pathogen [36, 38]. Unless the contaminant is of unusual type, character, or distribution, it is also likely that the emergence of an outbreak will first be detected by PulseNet laboratories as a cluster of identical PFGE patterns, and an outbreak investigation will be initiated. The certainty of intentional contamination may not emerge until well into the investigation of the outbreak, unless the event is publicized by complicit terrorist groups, strain(s) is/are of unusual subtype or character, or if the distribution of cases begins to support deliberate and multifocal contamination. PulseNet data will be crucial to determine the nature and extent of the outbreak, and to support criminal investigations by federal and international law enforcement, should they become necessary.

As with any foodborne outbreak, rapid detection and investigation are essential to mounting an effective response against a biological attack, expediting the traceback and removal of contaminated product(s) from the food supply and limiting the scope of the outbreak. Timely identification and response requires sophisticated laboratory-based real-time surveillance that functions at the level of the national population. Sensitivity and detection lag can both be greatly improved, particularly if frontline laboratories have sufficient capacity to complete and submit subtyping results immediately upon receipt. Ensuring that the public health system is ready to deal with intentional contamination events will require enhancement of preparedness and existing public health infrastructure, and as such, the maintenance of state and territory public health resources is critical [36, 37].

The ultimate purpose of any terrorist attack is to induce significant panic within the civilian population, undermine confidence in government, and threaten civil order [38, 39]. Attacks involving mass casualties and weapons of mass destruction are not necessary to achieve these goals. In fact, scenarios involving limited morbidity and

mortality, but which impact products and services that civilian populations use or are exposed to frequently during the course of daily life, can increase public anxiety and impose significant strain on public health and primary health care systems, even in the absence of an attack [38]. Among many foodborne outbreaks, unease and economic loss are typical with the identification and recall of a food product. Consumer confidence may be significantly eroded by an outbreak involving a particular food or brand, and the resulting aversion may affect individual producers or entire segments of the market. Thus, a biological attack or even a threat against consumer food supplies may incur significant financial cost, even if the direct impact on civilian populations is, or is expected to be low.

To date, the most significant example of intentional and malicious contamination of domestic food supplies occurred in the town of The Dalles, Oregon, in 1984, when followers of Bagwhan Shree Rajneesh contaminated 12 local restaurant salad bars with *Salmonella enterica* serotype Typhimurium in an effort to manipulate the outcome of local elections. Although there were no fatalities, the attack sickened 751 people, with 45 requiring hospitalization for acute salmonellosis. During the investigation of these cases, the possibility of intentional contamination was considered, but before the availability of molecular surveillance systems such as PulseNet, it took an exhaustive, year long study to link the commune to the outbreak [40]. The simplicity and efficacy of these attacks demonstrate the weaponized potential of foodborne bacteria, and their application to the subversion or manipulation of political processes. In the present day, where terrorist ideals extend beyond the Rajneeshee's desire to influence local politics, far faster action for response and investigation is required.

Among the potential biological agents that the CDC cited in a Strategic Planning Workgroup on Biological and Chemical Terrorism were *Clostridium botulinum*, *Salmonella* spp., *E. coli* O157, and *V. cholerae* [41]. In the United States, PulseNet standardized PFGE protocols and databases are already in place for all of these pathogens with the exception of *C. botulinum*, although a protocol is currently under development in collaboration with the Virginia Consolidated Laboratory Services. With an established sentinel network that extends throughout North America, and the cooperation of an increasing number of international partners, PulseNet is ideally positioned for the detection and investigation of foodborne bioterrorism, and is highly optimized for the bacterial agents most likely to be involved.

## 5 RESEARCH DIRECTIONS

Both the present and future success of PulseNet as a laboratory-based surveillance system depend upon its ability to accurately identify, transmit, and interpret bacterial subtyping data. This function must be accomplished rapidly and across a diverse network of national and international laboratories in order to provide timely and actionable information on the type and scope of an emergent outbreak. Although the concept of real-time bacterial subtyping is easy to understand, its implementation, particularly in the context of a broad geographical network, is neither simple nor straightforward.

For one, the process is technology-driven: as a technique, PFGE is highly robust and is amenable to implementation in laboratories with a wide range of resources and expertise. In practice, however, it is a labor intensive and meticulous procedure, and even with highly optimized and standardized protocols, PFGE subtyping of bacteria typically takes between 24 and 48 h from pure culture to a completed fingerprint. Furthermore,

because only a limited number of samples may be run in parallel, this throughput may be restrictive in time-sensitive outbreak situations [16, 18, 19].

More importantly, although PFGE affords a relatively high degree of discriminatory power and epidemiologic relevance [13, 15, 16], it is not always able to accurately resolve differences between outbreak and sporadic isolates, particularly among highly endemic strain types. As PulseNet databases have grown, database analysts have noticed a remarkably high degree of clonality among seemingly unrelated sporadic isolates (i.e. *S. almonella enterica* serotype Typhimurium DT104 complex [42], *S. enterica* serotype Enteritidis phage type 4, 8, and 13a [43], and *E. coli* O157:H7 [13]). When common patterns are encountered in an outbreak situation, it is often impossible to differentiate between potentially outbreak-related isolates and unrelated sporadic infections by PFGE alone, and the mis-identification of unrelated cases can greatly complicate epidemiologic follow-up.

With the increasing feasibility of routine genomic sequencing and high-throughput genetic analysis, the PulseNet methods development laboratory, in collaboration with state (MN, NC, and MA) and federal partners, has begun to develop and implement next-generation subtyping methods to enhance and complement existing PFGE-based protocols. The first of these new methods, multi-locus variable number tandem repeat analysis (MLVA), amplifies a series of short, tandem repeats within the bacterial genome and determines differences in copy number across all loci using capillary gel electrophoresis for high-resolution fragment analysis [44–46]. Interest in the evaluation of MLVA as a subtyping tool first arose after several studies demonstrated its ability to discriminate within highly clonal, PFGE-indistinguishable microorganisms [45, 47, 48], and MLVA has already proven useful in the investigation of outbreaks involving common PFGE patterns [44]. MLVA protocols for *E. coli* O157:H7, non-O157 STEC, *S. enterica* serotype *Typhimurium*, and *L. monocytogenes* are presently undergoing development or validation in our laboratory, and as of this writing, several protocols have been released for limited use by select PulseNet laboratories [7, 13].

The analysis of single nucleotide polymorphisms (SNPs) is also being evaluated as a next-generation subtyping approach, with active development of panels for rapid *E. coli* O157:H7 and non-O157 STEC subtyping/characterization [7, 13, 49]. A key advantage of SNP-based subtyping approaches lies in their genomic ubiquity, and their independence from fragment sizing, which negates the need for complex electrophoretic procedures, pattern normalization, and run times. However, selection and validation of SNP target panels are critical, and must combine sufficient coverage to detect genomic change, while retaining sufficient divergency to accurately discriminate between highly clonal bacterial lineages [49].

The development of meaningful interpretation and classification guidelines to describe and classify genetic changes in terms of strain type requires an extensive catalog of historical isolates, both sporadic- and outbreak associated. Occasionally, techniques prove to be too discriminatory: Several of the MLVA loci, for example, have a high degree of variability that may cause pattern instability even over a relatively short period of time [13, 50]. The continued evaluation of these protocols, in conjuction with PFGE and epidemiological data, should assist in the determination of the degree of variability that can be allowed during an outbreak investigation and the development of appropriate classification guidelines. Of greater concern is that many of the variable number tandem repeat (VNTR) sites that are useful for MLVA are highly specific to a given bacterial species or serotype (e.g. *E. coli* O157:H7 versus non-O157 STEC [13, 44]), and this

greatly limits the range of organisms that can be typed, with a corresponding increase in the number of protocols that must be developed, validated, and maintained.

An advantage of methodologies such as MVLA and SNP analysis is that many laboratories in the United States already have the necessary equipment available, although training and program funding continue to be problematic in many jurisdictions. These issues are accentuated in developing countries, and it is expected that new technologies will be initially integrated into PulseNet in a tiered approach and used primarily in situations where greater discriminatory power is required [12]. Laboratories that cannot justify an investment in new hardware, staff, and supplies would be encouraged to submit isolates to regional core laboratories, where resources for new technology could be centralized and more effectively supported or funded.

Future generations of bacterial subtyping have the potential to be more rapid and less technically demanding, while providing a higher level of epidemiological concordance than PFGE. However, the ultimate utility of these techniques is still being assessed, and their success will depend largely on their amenability to a diverse network of national and international partners. The introduction of any new subtyping technologies to the PulseNet program must be carefully weighed against instrumentation, infrastructural and staffing requirements, the compatibility and reliability of new data relative to existing methods, and by our own capacity to provide training and ongoing support to participating laboratories [12, 13].

With a rapidly expanding network of participating laboratories, PulseNet International is positioned at the forefront of global food safety and biosecurity initiatives. Building upon a history of successes in outbreak detection, response and prevention, it is our hope that the integration of new molecular and informatic technologies will further improve both the foundation and fabric of the PulseNet community, enhancing food safety and public health on a global scale.

## REFERENCES

1. Mead, P. S., Slutsker, L., Dietz, V., McCaig, L. F., Bresee, J. S., Shapiro, C., Griffin, P. M., and Tauxe, R. V. (1999). Food-related illness and death in the United States. *Emerg. Infect. Dis*. **5**, 607–625.
2. Allos, B. M., Moore, M. R., Griffin, P. M., and Tauxe, R. V. (2004). Surveillance for sporadic foodborne disease in the 21st century: the FoodNet perspective. *Clin. Infect. Dis*. **38**(Suppl 3), S115–S120.
3. Sobel, J., Griffin, P. M., Slutsker, L., Swerdlow, D. L., and Tauxe, R. V. (2002). Investigation of multistate foodborne disease outbreaks. *Public Health Rep*. **117**, 8–19.
4. Tauxe, R. V. (1997). Emerging foodborne diseases: an evolving public health challenge. *Emerg. Infect. Dis*. **3**, 425–434.
5. Tauxe, R. V. (1998). New approaches to surveillance and control of emerging foodborne infectious diseases. *Emerg. Infect. Dis*. **4**, 455–456.
6. Tauxe, R. V., and Hughes, J. M. (1996). International investigation of outbreaks of foodborne disease. *BMJ* **313**, 1093–1094.
7. Ribot, E. R., Hyytia-Trees, E., and Cooper, K. (2007). PulseNet and emerging foodborne diseases. In *Microbial Food Contamination*, 2nd ed., C. L. Wilson, Ed. CRC Press, Boco Raton, FL, pp. 3–29.
8. Jones, T. F., Scallan, E., and Angulo, F. J. (2007). FoodNet: overview of a decade of achievement. *Foodborne Pathog. Dis*. **4**, 60–66.

9. Tauxe, R. V. (2006). Molecular subtyping and the transformation of public health. *Foodborne Pathog. Dis*. **3**, 4–8.
10. Gerner-Smidt, P., Hise, K., Kincaid, J., Hunter, S., Rolando, S., Hyytia-Trees, E., Ribot, E. M., and Swaminathan, B. (2006). PulseNet USA: a five-year update. *Foodborne Pathog. Dis*. **3**, 9–19.
11. Swaminathan, B., Barrett, T. J., Hunter, S. B., and Tauxe, R. V. (2001). PulseNet: the molecular subtyping network for foodborne bacterial disease surveillance, United States. *Emerg. Infect. Dis*. **7**, 382–389.
12. Swaminathan, B., Gerner-Smidt, P., Ng, L. K., Lukinmaa, S., Kam, K. M., Rolando, S., Gutierrez, E. P., and Binsztein, N. (2006). Building PulseNet International: an interconnected system of laboratory networks to facilitate timely public health recognition and response to foodborne disease outbreaks and emerging foodborne diseases. *Foodborne Pathog. Dis*. **3**, 36–50.
13. Hyytia-Trees, E. K., Cooper, K., Ribot, E. M., and Gerner-Smidt, P. (2007). Recent developments and future prospects in subtyping of foodborne bacterial pathogens. *Future Microbiol*. **2**, 175–185.
14. Fakhr, M. K., Nolan, L. K., and Logue, C. M. (2005). Multilocus sequence typing lacks the discriminatory ability of pulsed-field gel electrophoresis for typing *Salmonella* enterica serovar Typhimurium. *J. Clin. Microbiol*. **43**, 2215–2219.
15. Barrett, T. J., Gerner-Smidt, P., and Swaminathan, B. (2006). Interpretation of pulsed-field gel electrophoresis patterns in foodborne disease investigations and surveillance. *Foodborne Pathog. Dis*. **3**, 20–31.
16. Ribot, E. M., Fair, M. A., Gautom, R., Cameron, D. N., Hunter, S. B., Swaminathan, B., and Barrett, T. J. (2006). Standardization of pulsed-field gel electrophoresis protocols for the subtyping of *Escherichia coli* O157:H7, *Salmonella*, and *Shigella* for PulseNet. *Foodborne Pathog. Dis*. **3**, 59–67.
17. Cooper, K. L., Luey, C. K., Bird, M., Terajima, J., Nair, G. B., Kam, K. M., Arakawa, E., Safa, A., Cheung, D. T., Law, C. P., Watanabe, H., Kubota, K., Swaminathan, B., and Ribot, E. M. (2006). Development and validation of a PulseNet standardized pulsed-field gel electrophoresis protocol for subtyping of *Vibrio cholerae*. *Foodborne Pathog. Dis*. **3**, 51–58.
18. Graves, L. M., and Swaminathan, B. (2001). PulseNet standardized protocol for subtyping *Listeria monocytogenes* by macrorestriction and pulsed-field gel electrophoresis. *Int. J. Food Microbiol*. **65**, 55–62.
19. Parsons, M. B., Cooper, K. L., Kubota, K. A., Puhr, N., Simington, S., Calimlim, P. S., Schoonmaker-Bopp, D., Bopp, C., Swaminathan, B., Gerner-Smidt, P., and Ribot, E. M. (2007). PulseNet USA standardized pulsed-field gel electrophoresis protocol for subtyping of *Vibrio parahaemolyticus*. *Foodborne Pathog. Dis*. **4**, 285–292.
20. Ribot, E. M., Fitzgerald, C., Kubota, K., Swaminathan, B., and Barrett, T. J. (2001). Rapid pulsed-field gel electrophoresis protocol for subtyping of *Campylobacter jejuni*. *J. Clin. Microbiol*. **39**, 1889–1894.
21. Sealy, T., Kubota, K., and Chu, M. (2003). One-day rapid pulsed-field gel electrophoresis (PFGE) protocol for typing of *Yersinia pestis*. *103rd General Meeting of the American Society for Microbiology*. Washington, DC.
22. Bender, J. B., Hedberg, C. W., Besser, J. M., Boxrud, D. J., MacDonald, K. L., and Osterholm, M. T. (1997). Surveillance by molecular subtype for *Escherichia coli* O157:H7 infections in Minnesota by molecular subtyping. *N. Engl. J. Med*. **337**, 388–394.
23. Bender, J. B., Hedberg, C. W., Boxrud, D. J., Besser, J. M., Wicklund, J. H., Smith, K. E., and Osterholm, M. T. (2001). Use of molecular subtyping in surveillance for *Salmonella enterica serotype typhimurium*. *N. Engl. J. Med*. **344**, 189–195.
24. CALFERT (2007). *Investigation of an Escherichia coli O157:H7 Outbreak Associated with Dole Pre-Packaged Spinach*.

25. CDC (2006). Ongoing multistate outbreak of *Escherichia coli* serotype O157:H7 infections associated with consumption of fresh spinach—United States, September 2006. *MMWR Morb. Mortal. Wkly. Rep*. **55**, 1045–1046.
26. Cooley, M., Carychao, D., Crawford-Miksza, L., Jay, M. T., Myers, C., Rose, C., Keys, C., Farrar, J., and Mandrell, R. E. (2007). Incidence and tracking of *Escherichia coli* O157:H7 in a major produce production region in california. *PLoS ONE* **2**, e1159.
27. Werber, D., Dreesman, J., Feil, F., Van Treeck, U., Fell, G., Ethelberg, S., Hauri, A. M., Roggentin, P., Prager, R., Fisher, I. S., Behnke, S. C., Bartelt, E., Weise, E., Ellis, A., Siitonen, A., Andersson, Y., Tschape, H., Kramer, M. H., and Ammon, A. (2005). International outbreak of Salmonella Oranienburg due to German chocolate. *BMC Infect. Dis.*, **5**, 1.
28. Chan, E. S., Aramini, J., Ciebin, B., Middleton, D., Ahmed, R., Howes, M., Brophy, I., Mentis, I., Jamieson, F., Rodgers, F., Nazarowec-White, M., Pichette, S. C., Farrar, J., Gutierrez, M., Weis, W. J., Lior, L., Ellis, A., and Isaacs, S. (2002). Natural or raw almonds and an outbreak of a rare phage type of Salmonella enteritidis infection. *Can. Commun. Dis. Rep*. **28**, 97–99.
29. CDC (2002). Multistate outbreaks of *Salmonella* serotype Poona infections associated with eating cantaloupe from Mexico—United States and Canada, 2000–2002. *MMWR Morb. Mortal. Wkly. Rep*. **51**, 1044–1047.
30. CDC (2004). Outbreak of *Salmonella* serotype Enteritidis infections associated with raw almonds—United States and Canada, 2003–2004. *MMWR Morb. Mortal. Wkly. Rep*. **53**, 484–487.
31. CDC (1999). Outbreaks of *Shigella sonnei* infection associated with eating fresh parsley—United States and Canada, July–August 1998. *MMWR Morb. Mortal. Wkly. Rep*. **48**, 285–289.
32. Isaacs, S., Aramini, J., Ciebin, B., Farrar, J. A., Ahmed, R., Middleton, D., Chandran, A. U., Harris, L. J., Howes, M., Chan, E., Pichette, A. S., Campbell, K., Gupta, A., Lior, L. Y., Pearce, M., Clark, C., Rodgers, F., Jamieson, F., Brophy, I., and Ellis, A. (2005). An international outbreak of salmonellosis associated with raw almonds contaminated with a rare phage type of *Salmonella enteritidis*. *J. Food Prot*. **68**, 191–198.
33. Naimi, T. S., Wicklund, J. H., Olsen, S. J., Krause, G., Wells, J. G., Bartkus, J. M., Boxrud, D. J., Sullivan, M., Kassenborg, H., Besser, J. M., Mintz, E. D., Osterholm, M. T., and Hedberg, C. W. (2003). Concurrent outbreaks of Shigella sonnei and enterotoxigenic *Escherichia coli* infections associated with parsley: implications for surveillance and control of foodborne illness. *J. Food Prot*. **66**, 535–541.
34. Wu, F. M., Doyle, M. P., Beuchat, L. R., Wells, J. G., Mintz, E. D., and Swaminathan, B. (2000). Fate of *Shigella sonnei* on parsley and methods of disinfection. *J. Food Prot*. **63**, 568–572.
35. El Sedawy, A. (2007), posting date. http://www.pulsenetinternational.org. [Online.]
36. Ashford, D. A., Kaiser, R. M., Bales, M. E., Shutt, K., Patrawalla, A., McShan, A., Tappero, J. W., Perkins, B. A., and Dannenberg, A. L. (2003). Planning against biological terrorism: lessons from outbreak investigations. *Emerg. Infect. Dis*. **9**, 515–519.
37. Sandhu, H. S., Thomas, C., Nsubuga, P., and White, M. E. (2003). A global network for early warning and response to infectious diseases and bioterrorism: applied epidemiology and training programs, 2001. *Am. J. Public Health* **93**, 1640–1642.
38. Sobel, J., Khan, A. S., and Swerdlow, D. L. (2002). Threat of a biological terrorist attack on the US food supply: the CDC perspective. *Lancet* **359**, 874–880.
39. Polyak, C. S., Macy, J. T., Irizarry-De La Cruz, M., Lai, J. E., McAuliffe, J. F., Popovic, T., Pillai, S. P., and Mintz, E. D. (2002). Bioterrorism-related anthrax: international response by the Centers for Disease Control and Prevention. *Emerg. Infect. Dis*. **8**, 1056–1059.
40. Torok, T. J., Tauxe, R. V., Wise, R. P., Livengood, J. R., Sokolow, R., Mauvais, S., Birkness, K. A., Skeels, M. R., Horan, J. M., and Foster, L. R. (1997). A large community outbreak of salmonellosis caused by intentional contamination of restaurant salad bars. *JAMA* **278**, 389–395.

41. CDC (2000). Biological and chemical terrorism: strategic plan for preparedness and response. Recommendations of the CDC Strategic Planning Workgroup. *MMWR Recomm. Rep*. **49**, 1–14.

42. Liebana, E., Garcia-Migura, L., Clouting, C., Clifton-Hadley, F. A., Lindsay, E., Threlfall, E. J., McDowell, S. W., and Davies, R. H. (2002). Multiple genetic typing of *Salmonella* enterica serotype typhimurium isolates of different phage types (DT104, U302, DT204b, and DT49) from animals and humans in England, Wales, and Northern Ireland. *J. Clin. Microbiol*. **40**, 4450–4456.

43. Ridley, A. M., Threlfall, E. J., and Rowe, B. (1998). Genotypic characterization of *Salmonella* enteritidis phage types by plasmid analysis, ribotyping, and pulsed-field gel electrophoresis. *J. Clin. Microbiol*. **36**, 2314–2321.

44. Hyytia-Trees, E., Smole, S. C., Fields, P. A., Swaminathan, B., and Ribot, E. M. (2006). Second generation subtyping: a proposed PulseNet protocol for multiple-locus variable-number tandem repeat analysis of Shiga toxin-producing *Escherichia coli* O157 (STEC O157). *Foodborne Pathog. Dis*. **3**, 118–131.

45. Keim, P., Price, L. B., Klevytska, A. M., Smith, K. L., Schupp, J. M., Okinaka, R., Jackson, P. J., and Hugh-Jones, M. E. (2000). Multiple-locus variable-number tandem repeat analysis reveals genetic relationships within Bacillus anthracis. *J. Bacteriol*. **182**, 2928–2936.

46. van Belkum, A., Scherer, S., van Alphen, L., and Verbrugh, H. (1998). *Short-sequence DNA repeats in prokaryotic genomes*, Vol. 62, p. 275–293.

47. Keys, C., Kemper, S., and Keim, P. (2005). Highly diverse variable number tandem repeat loci in the *E. coli* O157:H7 and O55:H7 genomes for high-resolution molecular typing. *J. Appl. Microbiol*. **98**, 928–940.

48. Lindstedt, B. A., Vardund, T., Aas, L., and Kapperud, G. (2004). Multiple-locus variable-number tandem-repeats analysis of *Salmonella* enterica subsp. enterica serovar Typhimurium using PCR multiplexing and multicolor capillary electrophoresis. *J. Microbiol. Methods* **59**, 163–172.

49. Zhang, W., Qi, W., Albert, T. J., Motiwala, A. S., Alland, D., Hyytia-Trees, E. K., Ribot, E. M., Fields, P. I., Whittam, T. S., and Swaminathan, B. (2006). Probing genomic diversity and evolution of *Escherichia coli* O157 by single nucleotide polymorphisms. *Genome Res*. **16**, 757–767.

50. Noller, A. C., McEllistrem, M. C., Shutt, K. A., and Harrison, L. H. (2006). Locus-specific mutational events in a multilocus variable-number tandem repeat analysis of Escherichia coli O157:H7. *J. Clin. Microbiol*. **44**, 374–377.

51. Mahon, B. E., Ponka, A., Hall, W. N., Komatsu, K., Dietrich, S. E., Siitonen, A., Cage, G., Hayes, P. S., Lambert-Fair, M. A., Bean, N. H., Griffin, P. M., and Slutsker, L. (1997). An international outbreak of Salmonella infections caused by alfalfa sprouts grown from contaminated seeds. *J Infect Dis.* **175**, 876–882.

52. MMWR. (2005). *Escherichia coli O157:H7 infections associated with ground beef from a U.S. military installation–Okinawa, Japan, February 2004.*MMWR Morb. Mortal. Wkly. Rep. **54**, 40–42.

## FURTHER READING

Gerner-Smidt, P., Hise, K., Kincaid, J., Hunter, S., Rolando, S., Hyytia-Trees, E., Ribot, E. M., and Swaminathan, B. (2006). PulseNet USA: a five-year update. *Foodborne Pathog. Dis*. **3**, 9–19.

Hyytia-Trees, E. K., Cooper, K., Ribot, E. M., and Gerner-Smidt, P. (2007). Recent developments and future prospects in subtyping of foodborne bacterial pathogens. *Future Microbiol*. **2**, 175–85.

Sobel, J., A. S. Khan, and Swerdlow, D. L. (2002). Threat of a biological terrorist attack on the US food supply: the CDC perspective. *Lancet* **359**, 874–80.

Swaminathan, B., Barrett, T. J., Hunter, S. B., and Tauxe, R. V. (2001). PulseNet: the molecular subtyping network for foodborne bacterial disease surveillance, United States. *Emerg. Infect. Dis*. **7**, 382–9.

Swaminathan, B., Gerner-Smidt, P., Ng, L. K., Lukinmaa, S., Kam, K. M., Rolando, S., Gutierrez, E. P., and Binsztein, N. (2006). Building PulseNet International: an interconnected system of laboratory networks to facilitate timely public health recognition and response to foodborne disease outbreaks and emerging foodborne diseases. *Foodborne Pathog. Dis*. **3**, 36–50.

# DEVELOPING RISK METRICS TO ESTIMATE RISKS OF CATASTROPHIC BIOLOGICAL AND BIOTERRORIST EVENTS: APPLICATIONS TO THE FOOD INDUSTRY

HAMID MOHTADI

*University of Wisconsin, Milwaukee, Wisconsin and University of Minnesota, Minneapolis, Minnesota*

## 1 INTRODUCTION

This article develops a data-based probabilistic algorithm for food vulnerabilities based on a statistical method known as *extreme value theory* that focuses on the distributional properties of the *maxima* or *minima* of a sequence of random variables. For the purposes of developing this probability metric, the focus is on intentional incidents for which food is a potential vehicle. Such incidents are broadly categorized in the literature as chemical biological and radionuclear (CBRN) events. While the food supply chain can be attacked in a number of different ways, the focus on CBRN-materials is warranted since their deliberate introduction into the civilian population is biased toward targeting the food sector's infrastructure, which provides reach across a wide region. The data are complied under a prior research project [1] funded by the Department of Homeland Security. While this data focuses on intentional CBRN events, there is a second project currently underway that aims at generalizes this data and the approach to accidental food events as well.

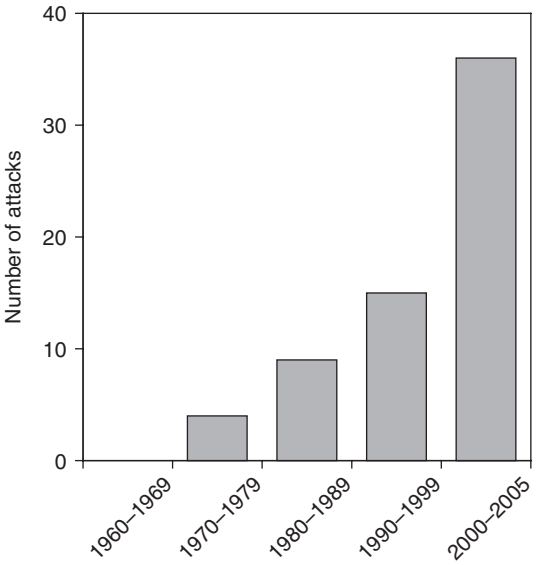



**FIGURE 1** Frequency of attacks on the food or water supply.Based on authors chronology of CBRN events and the sources cited therein

## 2 OVERVIEW

Since 2001, concern over intentional food contamination has been rising. Although the magnitude of health and human impacts or economic damage from intentional or accidental agents has not reached "catastrophic" levels, such a potential remains. For example, the World Health Organization (WHO) has been gravely concerned that food may be used as vehicle for terrorism.[1] Evidence does point to a recent rise in the severity of intentional food attacks (Figure 1). Evidence also suggests that many, if not all, food incidents have the *potential* to be intentionally caused and conversely, many known intentional food incidents may well be reported as accidental before true causes are discovered. The need to protect against such potential catastrophes requires an ability to assign risk to different events. This requires the knowledge of the likelihood of occurrence to each event. Yet, this seemingly simple task has not been possible thus far. The fact that such catastrophic events have fortunately not taken place yet, also implies the absence of hard data from which to build a probability-based risk metric framework. This poses a major stumbling block for a policy of protecting against catastrophic risk or for the developing of private risk markets for such extreme forms of risk.

The remainder of this article is organized as follows. First, data are discussed. Next, the statistical methodology is discussed. Following that, model estimation and statistical evidence on the likelihood of a catastrophic event that involves the use of CBRN material are provided. The final section contains the concluding remarks.

[1]In a (2002) report WHO states [2], "The malicious contamination of food for terrorist purposes is a real and current threat. . . The WHO and its Member States are concerned that chemical, biological or radionuclear agents might be used deliberately to harm civilian populations and that food might be a vehicle for the dissemination of such agents."

## 3 DATA AND THE OBSERVED TRENDS

### 3.1 Data

The data comprises of 448 observations complied from primary-source materials, internet postings, and the existing literature on CBRN-terrorist incidents.[2] The figure of 448 does not represent the universe of all CBRN events, rather it corresponds to the subset of the most publicized, and perhaps therefore, also the most serious incidents.[3] A separate data appendix, prepared by Mohtadi and Murshid [1] which is available online at the National Center for Food Protection and Defense (NCFPD) website provides a case-by-case description of incidents in the dataset (see the URL for Mohtadi and Murshid [1]).

The chronology provides a general description of each incident, along with details on the type of agent employed and the number of casualties that resulted. The data cover a 53-year period from 1952 to 2005. However, prior to 1975 the data on CBRN-activity is particularly sparse. Unlike the Monterey Institute's WMD database, which also focuses on CBRN events, but which also includes hundreds of hoaxes and pranks that do not necessarily relate to possession with intent or actual use some hoaxes, the CBRN data that we have complied also exclude *all* hoaxes. Excluded also are accidental releases of CBRN material such as, for instance, the explosion at Union Carbide's processing plant in Bhopal, India, or the meltdown of the nuclear reactor in Chernobyl, as well as the release of weaponzied anthrax in the Soviet Union in 1978. However, *attacks* that involved a threat to the containment of CBRN material such as acts of sabotage or direct acts of violence committed on CBRN facilities *are* included. Also, another large dataset, known as the *Terrorism Knowledge Base* [maintained at the National Memorial Institute for the Prevention of Terrorism (MIPT)], reported only 56 attacks involving CBRN material, hence the need to compile this data independently.

As in the case of WMD dataset, no attempt is made to distinguish terrorism from criminal activity for at least two reasons: First, because whatever the underlying motivation behind their use, these weapons have the *potential* to do significant harm or create an atmosphere of fear and panic. Thus for instance, on September 14, 2002, when Chen Zhengping tainted his competitor's water supply and pastry dough with rat poison, the underlying motive may have been purely financial, but the incident caused 41 deaths and over 400 hospitalizations.[4] Similarly the Tylenol murders in 1982, which though not linked to terrorist activity, nevertheless created an atmosphere of fear and panic, which by itself would satisfy the definition of terrorism. Second, the use of CBRN, even when they indicate petty crimes, indicate an acceptance amongst the criminally inclined to resort to what would previously have been exotic weaponry.

[2]The sources for the compilation of this data include reviews of recent terrorist incidents that were based on the weapons of mass destruction (WMD) database [3–6] as well as the open literature, such as Jenkins and Rubin [7], Livingstone and Arnold [8], Douglass and Livingstone [9], Hirsch [10], Mullen [11], Thornton [12], Kellen [13], Leventhal and Alexander [14], Kupperman and Woolsey [15], Kupperman and Kamen [16], Mullins [17], Purver [18], Tucker [19], Miller *et al*. [20] Carus [21], Mize [22].

[3]Mohtadi and Murshid [23, 24] provide a detailed survey of the existing terrorism dataset and explain why the need to collect our own data arose.

[4]"China Deaths Blamed On Rat Poison," *CNN*, September 16, 2002, "China Masks a Mass Poisoning," *The Guardian*, September 16, 2002.

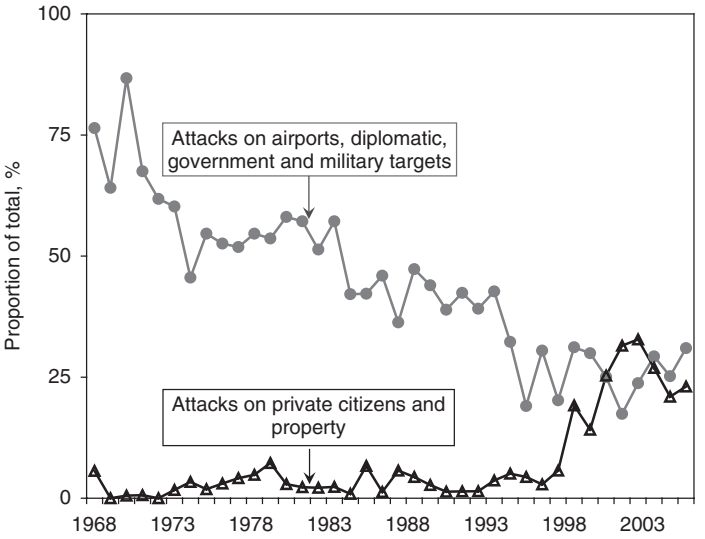



**FIGURE 2** Terrorist targets, 1968–2005.MIPT, *Terrorism Knowledge Base*

### 3.2 Observed Trends

Evidence from the MIPT dataset indicates that there has been an increase in the severity of terrorist attacks over the past decade. For example, almost all of the incidents where mortality or injury exceeded one thousand occurred over the period from 1993 to 2006. Furthermore, it appears that the trend with respect to the choice of weaponry, targets and tactics, indicates a rise in "softer" targets such as attacks on private citizens or private property, and away from "high profile" targets such as the airlines or government and military facilities (Figure 2). To the extent that the food chain also constitutes a softer target, the same trend is observed here as well. Thus, while attacks on the food industry indicate a general rise since the 1960s, when there were no recorded attacks (Figure 2), the most dramatic increase has come since 1999, a trend which is hard to attribute to better reporting alone. Table 1 shows the CBRN attacks between 1950 and 2005 that led to at least 100 casualties.

While there have been attacks on our food and water supply that have involved the use of conventional weapons, there is no reason in particular why terrorists should favor the food supply chain over other potential targets when using such conventional means of attack. The real threat as far as the food chain is concerned is likely to come from chemical, biological or radionuclear contaminants, which can exploit an already present distribution network to maximize the potential for disruption. Of the 448 biological, chemical and radiological incidents that have been recorded, 75 involved either a direct attack or a plan to attack the food or water supply chains.[5]

[5]We define attacks on the food or water supply as any attack that involves tampering with food and beverages with the potential to create large scale casualties. Thus for instance, simple targeted poisonings that are directed at one or perhaps a few specific individuals are not considered an attack on the food chain. However, the incident where contaminated water was handed to Filipino soldiers that led to 19 fatalities and 140 injuries is considered an attack on the food chain. We also regard attacks on livestock or the animal population in a separate category. Attacks on drugs and medication were also considered separately.

**TABLE 1 A few CBRN Events with at Least 100 Injuries or Fatalities**

| Date | Agent | Target | Fatalities | Injuries | Description |
|---|---|---|---|---|---|
| 20-Sep-1984 | *Salmonella typhimurium* | Food or water supply | 0 | 751 | In September 1984, members of a religious cult known as the *Rajneeshees* contaminated salad dressing at 10 restaurants in The Dalles, a small town in Oregon, USA. |
| 6-Sep-1987 | Unknown | Police | 19 | 140 | Up to 19 members of the Philippine Constabulary died during a "fun run" in which an individual handed out bags of ice water contaminated with an unknown agent. |
| 27-Jun-1994 | Sarin | Private citizens and property | 7 | 500 | In June 1994, members of the *Aum Shinrikyo* released sarin gas in Matsumoto, Japan; 7 people died and approximately 500 more were hospitalized. |
| 20-Mar-1995 | Sarin | Private citizens and property/ transportation | 12 | 5500 | On March 20, 1995, one of the deadliest terrorist attacks in history was carried out on the Tokyo subway, by *Aum Shinrikyo*; 12 people died in the sarin-gas attack and over 5500 required treatment. |
| 8-Mar-1999 | Nitric acid | Food or water supply | 0 | 148 | In March 1999, 148 persons were poisoned by nitric acid placed in the food of a restaurant in Luoyang City, China. |
| 5-Apr-2001 | CS gas | Educational Institution | Unknown | 132 | An unknown group attacked schools using CS gas in the Central Highlands, Vietnam; 132 people were treated for ailments—headaches and breathing problems. |
| 8-Aug-2001 | Rat poison | Food or water supply | 0 | 120 | 120 patrons in 16 restaurants became ill after eating noodles that had been contaminated with rat poison in Ningxiang, Hunan Province, China. |
| 14-Sep-2002 | Rat poison | Food or Water Supply | 41 | 400 | 41 people died and 400 became ill after buying breakfast food from a fast-food shop in Tangshan, Nanjing, China. |
| 31-Dec-2002 | Nicotine | Food or water supply | 0 | 111 | 111 people in Byron, USA, fell ill after eating the meat that had been contaminated by a supermarket employee, Randy Jay Bertram, with an insecticide known as *Black Leaf 40*. |
| 23-Sep-2003 | Rat poison | Food or water supply | 0 | 241 | 241 students and staff at the Changhu Township Center Elementary School in Yueyang, Hunan Province, China were poisoned. |

[a]Source: Based on Mohtadi and Murshid's [1] chronology of CBRN events and the sources cited therein.

## 4 METHODOLOGY

Existing food protection efforts have ignored the role of probabilities and instead prioritized investments solely on severity. For example, data on health costs from food contaminations are estimated by the Economic Research Service, United States Department of Agriculture (USDA), and used by various agencies for public policy. This amounts to the implicit assumption that all catastrophic events are equally likely which is a gross error, leading to massive resource misallocation.

The method proposed here addresses this major gap. It does so by invoking the statistical properties of certain distributions, known as *extreme value distributions*, which allow us to use data on ordinary food poisoning events to deduce the probability of large catastrophic events. In effect, information about the "body" (modal part) of these distributions, allows us to extrapolate to the probabilities of catastrophic events that belong to the ***"tail"*** of these distributions.

The key insight explores the limiting behavior of the maxima, $M_n$, of a sequence$\{X_n\}$ of independent random variables with common distribution$F(x)$. At the heart of extreme value theory is the *extremal types theorem* [25, 26], which states if the maxima of sequences of observations converge to a nondegenerate law, $G(.)$, then$G(.)$ belongs to the class of generalized extreme value distributions (GEV):[6]

$$G_\xi(x) = \exp\left\{-\left[1+\xi\left(\frac{x-\mu}{\sigma}\right)\right]^{-1/\xi}\right\}; 1+\xi\left(\frac{x-\mu}{\sigma}\right) \geq 0 \tag{1}$$

where $\mu$ is a *location* parameter, $\sigma$ is a *scale* parameter and $\xi$ is the *shape* parameter that determines the sub-class of distribution from which our observations are drawn. Specifically, $\xi > 0$, $\xi < 0$, and $\xi = 0$ correspond to the Fréchet (heavy tailed), Weibull (bounded tailed), and Gumbel (light tailed) distributions, respectively. The GEV-representation is particularly useful, since it bypasses the need to identify the specific type of distribution to which the extreme value limit law belongs. Instead standard statistical methodology from parametric estimation can be applied to identify the parameters of interest. Other than the work by Mohtadi and Murshid [23], there has been one other study that uses this approach for terrorism data [28], but the authors use the MIPT data, not data based on CBRN events. A related article by Johnson et al. [29] studies the distribution of fatalities in two recent conflicts and show that these distributions follow a power law relationship that has a similar functional structure to the GEV distributions here.

Implicit in the approach adopted here is the assumption that the current experience with CBRN attacks is a good predictor of future CBRN terrorism. While the use of past data to forecast future trends is a common practice, the threat from CBRN weapons is likely to be dynamic as possibly unstable, as terrorists' actions are likely to be a function of an earlier counter-terrorist response by the government and *vice versa* [30]. Yet, it is difficult to imagine how the pattern of response and counter-response could change overnight. If, as is more likely, the dynamics of this process are gradual, an analysis of data can shed important light on the current capabilities of terrorists in addition to highlighting trends in their usage.

[6]See, for example, Coles [27].

## 5 MODEL ESTIMATION

The variation in CBRN dataset is rather limited as the overwhelming majority of attacks failed to cause death or injury. Nevertheless, there is some structure in the tails of the distribution coinciding with certain prominent cases, such as the *sarin* attacks in Japan and the *Rajneeshee* incident in Oregon. CBRN events, however, have apparently caused more injury than death. Following the *sarin* attack in Tokyo, for instance, roughly 5000 affected individuals needed medical treatment, whereas only 12 fatalities were reported. The largest CBRN-related fatalities occurred in Uganda, in which a cult was suspected of poisoning its members with sulfuric acid. Even here, the total number of deaths stood at 200, which pales when compared to the nearly 3000 deaths on September 11. Thus to maximize the variation in the dataset, casualties and injuries are added together. In addition, data prior to 1975 are omitted, since they are very sketchy.

The application of extreme value theory typically involves "blocking" the data into disjoint subperiods of equal length and fitting a GEV distribution to the block maxima. In setting the block size, researchers face a trade-off. "Blocking" too narrowly threatens the validity of the limiting argument, leading to a bias in estimation. Wider blocks, however, will generate fewer maxima, leading to greater variability in our estimates. This article opts for semiannual blocking as this choice seems to provide a reasonable trade-off between bias and variance.

The analysis detailed elsewhere [23, 24], allows for both time trends in the location parameter $\mu$ and the scale parameter $\sigma$, as well as breakpoints in the data. Dummy variables for the data breakpoints included 1980–1905 dummy, 1990–2005 dummy and post-1990 dummy. Based on a combination of the quantile–quantile (QQ) plots and maximum likelihood estimates, the best results are reported as shown in Table 2. These results indicate evidence of trend behavior in the severity of the attacks, as seen by the significance both in the location parameter $\mu$ and the scale parameters, $\sigma$. This is consistent with an increasing number of casualties resulting from the worst attacks each year. However, the fact that the value of the estimated shape parameter, $\xi$, is positive and significant in both models suggests that trend is not all that is at work and that at least some of the extreme variation in the data *must* be explained by the *heavy-tailed* nature of the underlying stochastic model.

***5.0.1 Forecasting Probability of Attacks.*** Based on our estimated two models reported in Table 2, one can calculate the probability of a CBRN attack of various magnitudes and time horizons. These estimates are provided in Table 3. The results suggest that the probability of a large CBRN attack, defined as an attack that inflicts between 1000 and 10,000 casualties (injury or death), is nonnegligible. Using the estimates for the second column of Table 2, which provided the best fit to the data, the likelihood that a CBRN attack (anywhere in the world) causes 1000 or more casualties is 0.40. As noted above, the distribution of CBRN events is characterized by pronounced tails. Consequently the current probability of a 10,000-casualty event is not much lower. Using the specification in Table 2, this value works out to be 0.28.

Obviously, these results are sensitive to how one models extreme variations in the data. Thus, if one believes that extreme observations, post-1990s, are better captured by a right shift of the location as opposed to scale parameter, then the current risk of an event leading to 10,000 casualties is relatively low—somewhere between 0.05 and 0.10 (not reported here). However by implication, a continuation of these trends would imply

**TABLE 2 GEV Parameter Estimates Fitted to CBRN Data**

| | | – | – |
|---|---|---|---|
| $\mu$ | Constant | 0.0096 | 0.0227 |
| | | (0.00) | (0.01) |
| | Trend | 0.0103 | 0.0227 |
| | | (0.00) | (0.01) |
| | 1980–1905 dummy | | |
| | 1990–2005 dummy | | |
| | Post-1990 trend | | 0.0267 |
| | | | (0.03) |
| | Post-1994 trend | | |
| | | – | – |
| $\sigma$ | Constant | 0.0168 | 0.0357 |
| | | (0.01) | (0.00) |
| | Trend | 0.0183 | 0.0365 |
| | | (0.01) | (0.00) |
| $\xi$ | | 1.1979 | 0.5446 |
| | | (0.24) | (0.19) |
| Negative log likelihood | | 94.6 | 99.3 |

[a]Estimation was done in *R* using the **Introduction to Statistical Modeling of Extreme Values** (ISMEV) package. The ISMEV package is based on software written by Stewart Coles. Estimates are based on the log of the maximum number of fatalities and injuries over a six month period. Standard errors are reported in parentheses. The last row reports the negative log likelihoods for each model.

**TABLE 3 Probability of CBRN and non-CBRN Attacks of Various Severities**

| | | | |
|---|---|---|---|
| 1000 | Current risk | 0.31 | 0.40 |
| 5000 | | 0.27 | 0.31 |
| 10,000 | | 0.25 | 0.28 |
| 1000 | 5-year forecast | 0.34 | 0.47 |
| 5000 | | 0.30 | 0.38 |
| 10,000 | | 0.28 | 0.34 |
| 1000 | 10-year forecast | 0.37 | 0.54 |
| 5000 | | 0.32 | 0.44 |
| 10,000 | | 0.31 | 0.41 |
| 1000 | 20-year forecast | 0.42 | 0.67 |
| 5000 | | 0.37 | 0.56 |
| 10,000 | | 0.35 | 0.52 |

[a]The two columns report probabilities of CBRN events of various magnitudes within any given year, corresponding to the two parameter estimates of the two columns in Table 2, respectively.

that the future risk of a large event would be much higher. These values probably also overestimate the risk. In short, in whatever way, we choose to model the distribution of casualties from CBRN events, the presence of a nonstationary component is undeniable. As a result, the *recurrence* (return) period of these events is expected to decline with time.

## 6 CONCLUSION

This short article presents an overview of the ongoing research into the assessment of the risk of bioterrorism in the food sector. The analyses are based on nearly 450 observations from 1950 to 2005, but with a focus on the 1975–2005 period. The focus is on intentional and terrorist events at a global scale involving chemical, biological or radionuclear agents, agents that are especially likely to be associated with the food sector as the channel for their dissemination. The analytical method for assessing this risk derives from a statistical technique known as extreme value theory that is tailored to the estimation of "tail" probabilities for rare but catastrophic events. It has been applied to financial crisis, to earthquake predictions and to weather patterns. This study is one among the first efforts to also apply this to terrorism events. In our other articles, another data set (MIPT) consisting of over 25,000 observations were also used as a benchmark to compare the risk of terrorism in the food sector with terrorism at large.

The findings are somewhat alarming. For example, if we focus on catastrophic CBRN events, that is those with large numbers of casualties, we see a rise in their severity. Correspondingly, the average reoccurrence period for such attacks is on the decline, while their probability is on the rise as time goes by. Similar trends underline the findings with respect to terrorist attacks more generally that were documented elsewhere. Since food is a prime candidate for CBRN agents, the implication of this finding is self-evident. By quantifying such risks, this line of research has opened a path toward rationalizing the private and public sector decisions involving extreme risk forms, including both the public policy for ranking risk mitigating strategies and the also the development of private risk markets for catastrophic forms of risk.

## REFERENCES

1. Mohtadi, H. and Murshid, A. (2006). *A Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks: 1950-2005*, published at the website of the National Center for Food Protection and Defense (NCFPD), at http://www.ncfpd.umn.edu/docs/GlobalChron.pdf.
2. World Health Organization, Food Safety Department (2002). *Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems*.
3. Cameron, G., Pate, J., McCauley, D., and DeFazio, L. (2000). 1999 WMD terrorism chronology: incidents involving sub-national actors and chemical, biological, radiological, and nuclear materials. *Nonprolif. Rev*. **7**(2), 157–174.
4. Pate, J., and Cameron, G. (2001). *Covert Biological Weapons Attacks Against Agricultural Targets: Assessing the Impact Against U.S. Agriculture*, Discussion Article 2001-9, John F. Kennedy School of Government, Harvard University.
5. Pate, J., Ackerman, G., and McCloud, K. (2001). *2000 WMD Terrorism Chronology: Incidents Involving Sub-National Actors and Chemical, Biological, Radiological, or Nuclear Materials*, Center for Nonproliferation Studies report, Monterey Institute of International Studies, Monterey.
6. Turnbull, W., and Abhayaratne, P. (2003). *2002 WMD Terrorism Chronology: Incidents Involving Sub-National Actors and Chemical, Biological, Radiological, and Nuclear Materials*, Center for Nonproliferation Studies report, Monterey Institute of International Studies, Monterey.
7. Jenkins, B. M. and Rubin, A. P. (1978). New vulnerabilities and the acquisition of new weapons by nongovernment groups. In *Legal Aspects of International Terrorism*, S. Evans and J. F. Murphy, Eds. Lexington Books, Lexington, MA, pp. 221–276.

8. Livingstone, N. C. and Arnold, T. B. (1986). *Fighting Back: Winning the War against Terrorism*. Lexington Books, Lexington, MA.
9. Douglass, J. D., Jr. and Livingstone, N. C. (1987). *America the Vulnerable: The Threat of Chemical and Biological Warfare*. Lexington Books, Lexington, MA.
10. Hirsch, D. (1987). The truck bomb and insider threats to nuclear facilities. In *Preventing Nuclear Terrorism: The Report and Articles of the International Task Force on Prevention of Nuclear Terrorism*, P. Leventhal and Y. Alexander, Eds. Lexington Books, Lexington, MA, pp. 207–222.
11. Mullen, R. K. (1987). Nuclear violence. In *Preventing Nuclear Terrorism: The Report and Articles of the International Task Force on Prevention of Nuclear Terrorism*, P. Leventhal and Y. Alexander, Eds. Lexington Books, Lexington, MA, pp. 231–247.
12. Thornton, W. H. (1987). *Modern Terrorism: The Potential for Increased Lethality. Langley Air Force Base, VA: Army- Air Force Center for Low Intensity Conflict*, CLIC Article.
13. Kellen, K. (1987). The potential for nuclear terrorism: a discussion, with appendix: nuclear-related terrorist activities by political terrorists. In *Preventing Nuclear Terrorism: The Report and Articles of the International Task Force on Prevention of Nuclear Terrorism*, P. Leventhal and Y. Alexander, Eds. Lexington Books, Lexington, MA, pp. 104–122.
14. Leventhal, P. and Alexander, Y. (1987). *Preventing Nuclear Terrorism: The Report and Articles of the International Task Force on Prevention of Nuclear Terrorism*. Lexington Books, Lexington, MA,
15. Kupperman, R. H. and Woolsey, R. J. (1988). *Techno-Terrorism. Testimony before the Technology and Law Subcommittee of the Judiciary Committee May 19, 1988*, U.S. Department of Justice.
16. Kupperman, R. H. and Kamen, J. (1989). *Final Warning: Averting Disaster in the New Age of Terrorism*. Doubleday, New York.
17. Mullins, W. C. (1992). An overview and analysis of nuclear, biological, and chemical terrorism: the weapons, strategies and solutions to a growing problem. *Am. J. Crim. Justice* **16**(2), 95–119.
18. Purver, R. (1995). *Chemical and Biological Terrorism: The Threat According to the Open Literature*. Canadian Security Intelligence Service.
19. Tucker, J. B. (2000). *Toxic Terror: Assessing Terrorist Use of Chemical and Biological Weapons*. MIT Press, Cambridge, MA.
20. Miller, J., Broad, W., and Engelberg, S. (2001). *Germs: Biological Weapons and America's Secret War*. Simon & Schuster Adult Publishing Group, London.
21. Carus, W. S. (2002). *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*. Fredonia Books.
22. Mize, K. (2004). *Classical Radiological Dispersal Devices*. Internet document, http://www.nlectc.org/training/nij2004/mize.pdf.
23. Mohtadi, H. and Murshid, A. (2007a). *How secure is our food? A Risk-Based Approach to Assessing Food Sector Vulnerability*, Working Article, University of Minnesota and Wisconsin-Milwaukee.
24. Mohtadi, H. and Murshid, A. (2007b). The risk of catastrophic terrorism: an extreme value approach. *J. Appl. Econom*. Forthcoming.
25. Fisher, R. A. and Tippett, L. H. C. (1928). Limiting forms of the frequency distribution of the largest and smallest member of a sample. *Proc. Camb. Philol. Soc*. **24**, 180–190.
26. Gnedenko, B. V. (1943). Sur la distribution limite du terme maximum d'une serie aleatoire. *Ann. Math*. **44**, 423–453.

27. Coles, S. G. (2001). *An Introduction to Statistical Modeling of Extreme Values*. Springer Verlag, London.
28. Bogen, K. and Jones, E. (2006). Risks of mortality and morbidity from worldwide terrorism: 1968:2004. *Risk Anal*. **26**(1), 45–59.
29. Johnson, N., Spagat, M., Restrepo, J. A., Bohórquez, J., Suárez, N., Restrepo, E., and Zarama, R. (2005). *From Old Wars to New Wars and Global Terrorism*, Universidad Javeriana--Bogotá, Documentos de Economía 002339.
30. Michel-Kerjan, E. (2003). Large scale terrorism: risk sharing and public policy. *Revue. d'Economic Politique*. **113**, 625–648.

## FURTHER READING

Embrechts, P., Klüppelberg, C., and Mikosch, T. (1997). *Modelling Extremal Events for Insurance and Finance*. Springer Verlag, Berlin.

Enders, W. and Sandler, T. (2005). After 9/11: is it all different now? *J. Conflict Resolut*. **49**, 259–277.

Kunreuther, H., Doherty, N., Goldsmith, E., Harrington, S., Kleindorfer, P., Michel-Kerjan, E., Pauly, M., Rosenthal, I., and Schmeidler, P. (2005) *TRIA and Beyond: Terrorism Risk Financing in the US*, Wharton Risk Management and Decision Process Center, University of Pennsylvania, Report.

Kunreuther, H., Meszaros, J., Hogarth, R. M., and Spranca, M. (1995). Ambiguity and underwriter decision processes. *J. Econ. Behav. Organ*. **26**, 337–352.

Sandler, T. and Enders, W. (2004). *Transnational Terrorism: An Economic Analysis*, Working article, University of Southern California.

# WATER

# WATER INFRASTRUCTURE AND WATER USE IN THE UNITED STATES

ROBERT PITT
*University of Alabama, Tuscaloosa, Alabama*
SHIRLEY E. CLARK
*Pennsylvania State University, Harrisburg, Middletown, Pennsylvania*

## 1 OVERVIEW

As reported by the Environmental Protection Agency (EPA) [1], as recently as the mid-nineteenth century, drinking water supply and wastewater disposal focused on bringing drinking water to the population and carrying wastewater away, with minimal thought to treatment. Near the beginning of the twentieth century, health concerns started to force communities to address treatment. In 1872, Poughkeepsie, NY, introduced slow sand filtration to reduce turbidity in drinking water, which also removed the microbial contaminants that were responsible for typhoid, dysentery, and cholera epidemics. In 1908, Jersey City, NJ, introduced drinking water disinfection treatment using chlorination to further reduce disease outbreaks associated with drinking water. On the wastewater side, the EPA further pointed out that, if the wastewater received any treatment prior to 1900, it consisted of physically separating solids and floating debris from the water prior to a surface water discharge (e.g. primary treatment only). The nation's first wastewater filtration facility was built in 1907 in Gloversville, NY. In 1916, Chicago, IL, constructed an activated sludge treatment plant (secondary treatment).

The 1972 Clean Water Act required that all publicly owned treatment works provide secondary treatment of wastewater. By 1996, fewer than 200 systems, out of 16,204 nationwide, had not met this requirement. In 1974, the Safe Drinking Water Act established the current system of nationwide standards for drinking water contamination. Amendments to the SDWA have continued to improve drinking water quality by regulating contaminants that were not identified in 1974, or for which additional health data is not known. These amendments require the reduction of the allowable concentration in finished water. This vital infrastructure, however, is being threatened by an increasing gap between the funding needs to continue to provide the nation with safe drinking water and proper wastewater treatment and disposal and the amount being invested. Recent needs

surveys and gap analyses have noted that a significant increase in expenditures is needed to ensure continued national security in the clean water industry.

## 2 WATER USE BY SECTOR

The availability and use of water resources in the United States is strongly dependent on the distribution of the waters. Table 1 shows how water is distributed in the continental United States (distribution and replacement data from Ref. 2).

Even though the vast portion of all water in the United States is associated with groundwater, the annual turnover (replacement) of that water is relatively small.

Soil moisture and stream flow likely provide the greatest amount of annual replacement of this groundwater; however, in many areas, the replacement rate is less than the usage rate. Stream flows and other surface water bodies, though smaller in quantity than groundwater, are the most accessible forms that are readily available for development. Unfortunately, they are also most subject to large year-to-year variations owing to periods of drought and excessive rainfalls.

Figure 1 shows the size of the water withdrawals in the United States by source and Figure 2 shows how water withdrawals in the United States are used for various purposes [3]. In the 1960s, total withdrawals totaled about 320 billion gallons per day, or about $430 \times 10^9$ $m^3$ per year. Approximately 20% was from groundwater sources, while the remainder was from surface water sources (68% was from freshwater surface sources and 14% was from saline surface sources). Groundwater withdrawals are greater than the replenishment rates in a number of critical aquifers in the country, leading to deeper and deeper wells and more frequent abandonment of wells, plus concerns about land subsidence. In recent years, the total amount of withdrawals has continued to increase, especially for thermoelectric power cooling, irrigation, and for public water supplies. In 2000, the total withdrawal rate was estimated to be about 400 billion gallons per day, and groundwater still comprised about 20% of the total withdrawals. Most of these withdrawals are eventually discharged to surface waters as waste cooling waters, irrigation return flows, or treated industrial and domestic wastewaters.

**TABLE 1 Volume of Water in the Continental United States and Annual Flux**

| | Volume ($\times 10^9$ $m^3$) | Volume (%) | Replacement period (yr) | Flux ($\times 10^9$ $m^3$/yr) |
|---|---|---|---|---|
| Groundwater—shallow (<800 m deep) | 63,000 | 43.2 | >200 | <315 |
| Groundwater—deep (>800 m deep) | 63,000 | 43.2 | >10,000 | <6.3 |
| Freshwater lakes | 19,000 | 13.0 | 100 | 190 |
| Soil moisture (top 1 m of soil) | 630 | 0.43 | 0.2 | 3150 |
| Salt lakes | 58 | 0.04 | >10 | <5.8 |
| Average in stream channels | 50 | 0.03 | <0.03 (<11 days) | 1700 |
| Water vapor in atmosphere | 190 | 0.13 | >0.03 (>11 days) | <6300 |
| Frozen water in glaciers | 67 | 0.05 | >40 | <1.7 |

Data from Ref. 2.

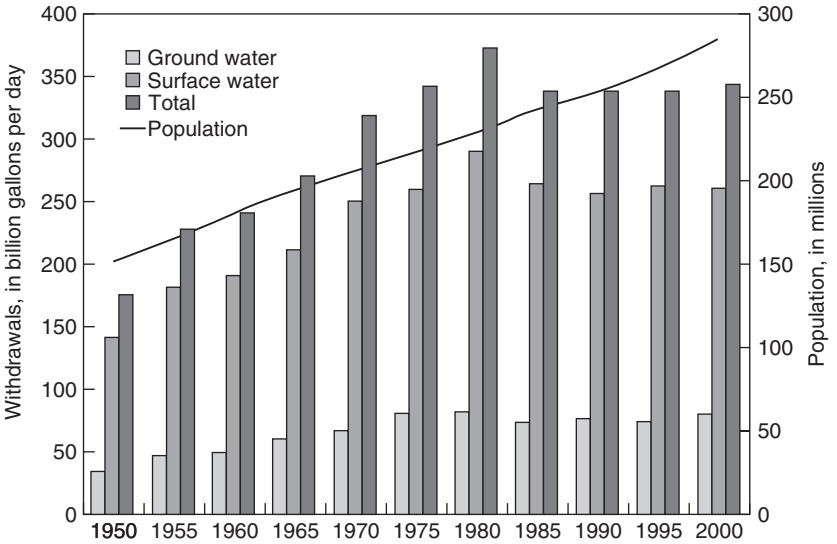



**FIGURE 1** Trends in population and freshwater withdrawals by source, 1950–2000 [3].

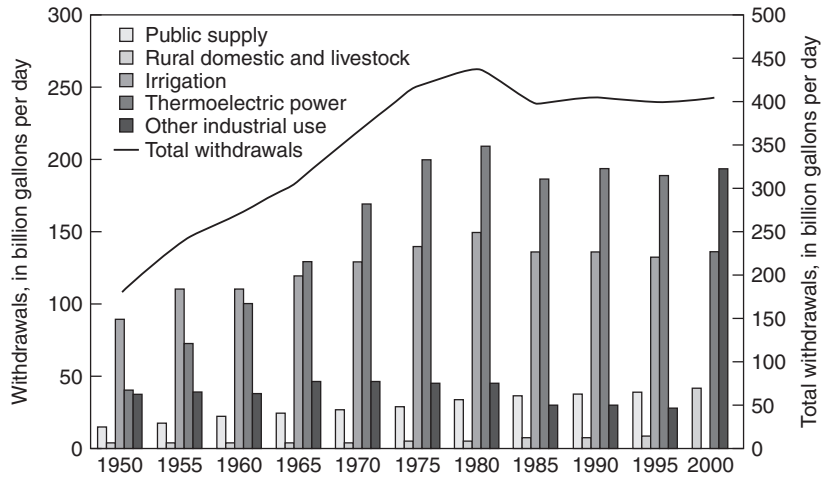



**FIGURE 2** Total water withdrawal for public supply, rural, irrigation, thermoelectric power, and other industries in the United States [3].

## 2.1 Agricultural Water Use

Figures 3 and 4 show how different crop use irrigation water in the eastern United States and in the western United States. Rice is the major irrigated crop in the east (in almost 5 million acre-ft per year), while alfalfa is the most irrigated western crop (using about 15 million acre-ft per year). Orchards also are irrigated with substantial amounts of water throughout the country. Total irrigated land in the United States has grown substantially and now comprises about 55,000 acres (relatively steady since the late 1970s), while it was only about 8000 acres in 1900 and 25,000 acres in 1949 [4].

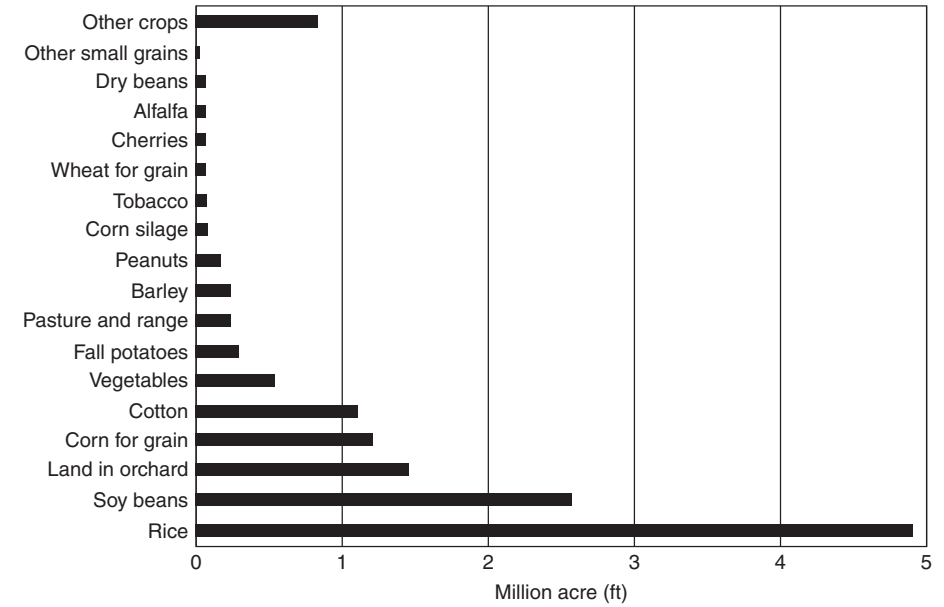



**FIGURE 3** Eastern water applications by crop, 1998 [5].

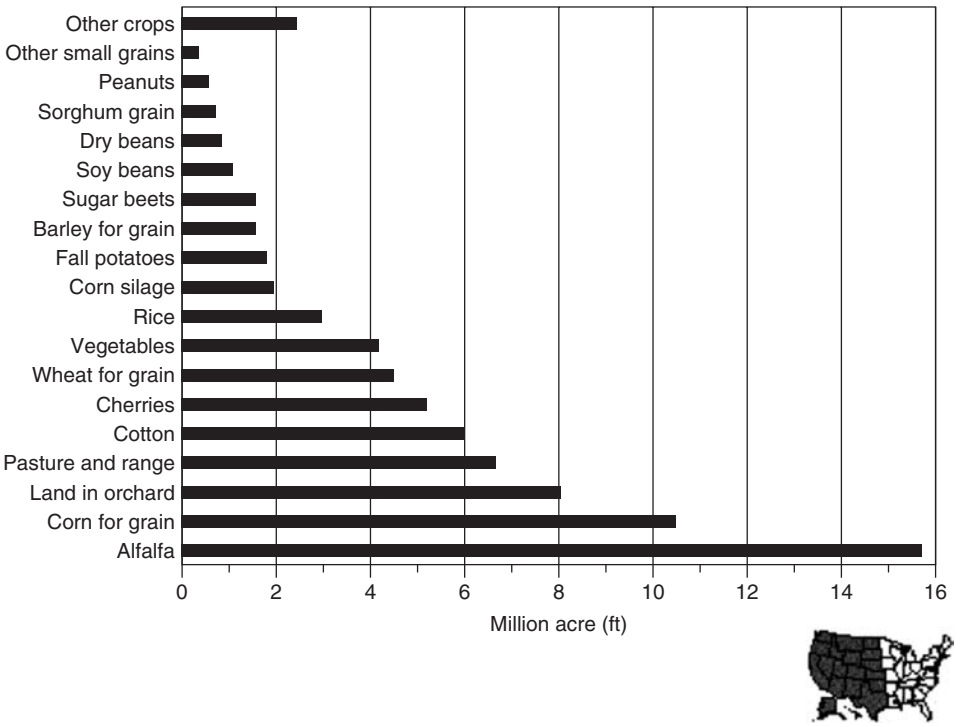



**FIGURE 4** Western water applications by crop, 1998 [5].

### 2.2 Domestic Water Use

Domestic water demand from public water supply utilities has increased faster than the general population growth over the past 50 years. Figure 2 shows that the per capita domestic water use has increased from about 117 gal/person/day in 1950 to more than 180 gal/person/day in 1995. During this time period, the US population has increased from about 150 to about 270 million people, resulting in a 2.8 times increase in domestic water withdrawals over this period. The water supplied by public water supplies also serves institutional, commercial, and some industrial uses, and is more than what is used in a household. These additional uses are included in the calculations for per capita (or per person) daily uses, such as those reported above. Table 2 shows the typical household water use alone, which is generally slightly less than half of the total water supplied by a public water utility on a per captia basis. It is interesting to note that only about 40% (34.5 gal/person/day) of this total needs to be supplied by highly treated water, associated with drinking, kitchen, dishwasher, bathing, and laundering uses. The other household waters can be supplied by poorer quality water, as it is not consumed and not associated with human contact. Most of this other water is simply used to carry wastes to the treatment plant where the wastes are then removed from the water (at great cost).

### 2.3 Public Water Supply Treatment

According to the EPA [7] there are approximately 158,000 public drinking water systems in the United States that serve at least 25 people or have at least 15 service connections (Table 3). These systems serve most people in the United States (282 million). Approximately 53,000 of these public drinking water systems are community water systems that supply water year-round to residents. However, just 8% of those 53,000 systems (4034) serve 81% of the population.

Besides the 53,000 community water systems noted in Table 3, there are about 19,000 nontransient noncommunity water systems (a public water system that regularly supplies water to at least 25 of the same people at least six months per year, but not year-round. Some examples are schools, factories, office buildings, and hospitals, which have their own water systems) and about 86,000 transient noncommunity water systems (a public water system that provides water at a location such as a gas station or campground where people do not remain for long periods of time). These other public water systems serve

**TABLE 2 Typical Personal Water Use by an Urban Family of Four**

| Activity | Per Capita Daily Use (gallons) | % of total |
|---|---|---|
| Drinking and kitchen water use | 2 | 2 |
| Dishwasher (3 loads per day) | 3.75 | 4 |
| Toilet (16 flushes per day) | 24 | 28 |
| Bathing (4 baths or showers per day) | 20 | 23 |
| Laundering (6 loads per week) | 8.5 | 10 |
| Automobile washing (2 car washes per month) | 2.5 | 3 |
| Lawn watering and swimming pools | 25 | 29 |
| Garbage disposal unit (1% of all other uses) | 0.75 | 1 |
| Total | 86.5 | 100 |

Ref. 6.

**TABLE 3 Community Water System Population Served (January 2006 data)**

| | Very Small (<500) | Small (501–3300) | Medium (3301–10,000) | Large (10,001–100,000) | Very Large (>100,000) | Total |
|---|---|---|---|---|---|---|
| # systems | 29,666 | 14,389 | 4748 | 3648 | 386 | 52,837 |
| Population served | 4,925,748 | 20,851,292 | 27,514,714 | 102,747,558 | 126,304,807 | 282,344,119 |
| % of total systems | 56% | 27% | 9% | 7% | 1% | 100% |
| % of population | 2% | 7% | 10% | 36% | 45% | 100% |

Ref. 7.

**TABLE 4 Water Sources for Community Water Systems (January 2006 data)**

| | Groundwater | Surface water | Total |
|---|---|---|---|
| # systems | 40,018 | 11,737 | 51,755 |
| Population served | 89,539,197 | 191,130,147 | 280,669,344 |
| % of systems | 77 | 23 | 100 |
| % of population | 32 | 68 | 100 |

Ref. 7.

about an additional 20 million people. In terms of numbers of systems, most of the systems obtain their water from groundwater sources. In contrast, most of the population is served by surface water supplies (Table 4).

Traditional surface water treatment for drinking water includes sedimentation (often after chemical coagulation and flocculation), filtration, and disinfection. Groundwater treatment may skip the sedimentation and filtration steps, if the source water is sufficiently clean. Many modifications to these processes exist based on the quality of the source water used. Table 5 lists the types of treatment systems serving public water supplies. The 2435 treatment plants that were surveyed were a small sample of the total number of treatment plants in the country. The table also shows that most water treatment plants still use disinfection, with no additional treatment. This is likely because many systems have groundwater sources with low sediment loads that do not require sedimentation and filtration. There are few obvious trends in the treatment technologies used for the different sized systems. Ion exchange, membranes, and other chemical treatment methods are represented in all plant sizes. However, community water softening is more common with the smaller plants.

During the 2005 fiscal year, the EPA [7] reported health-based violations by states. These violations were either for treatment technique problems, or for exceeding the maximum contaminant level (MCL) numeric standards. From 2% (Alabama) to 33% (Washington, D.C.) of the systems had reported violations. These violations affected <1% (Delaware) to 98% (Washington, D.C.) of the population served in each state or

**TABLE 5 Types of Water Treatment Plants Serving Public Water Supplies (Percentage)**

| | 100 or less | 101–500 | 501–3300 | 3301–10,000 | 10,001–50,000 | 50,001–100,000 | 100,001–500,000 | Over 500,000 | All Sizes |
|---|---|---|---|---|---|---|---|---|---|
| Disinfection with no additional treatment | 67.0 | 52.9 | 47.5 | 31.8 | 33.5 | 37.3 | 43.9 | 68.5 | 49.4 |
| Other chemical treatment | 7.0 | 19.8 | 10.7 | 25.1 | 12.1 | 10.6 | 3.6 | 1.5 | 14.3 |
| Ion exchange, activated alumina, aeration | 0.0 | 9.1 | 20.1 | 16.7 | 19.0 | 19.3 | 11.9 | 13.9 | 12.5 |
| Other filtration (not direct or conventional) | 12.4 | 10.8 | 4.9 | 4.7 | 6.9 | 3.7 | 5.7 | 0.2 | 8.0 |
| Direct filtration | 0.7 | 1.5 | 1.0 | 3.1 | 3.8 | 3.1 | 3.6 | 2.8 | 1.7 |
| Conventional filtration | 1.1 | 0.7 | 3.5 | 8.2 | 13.5 | 18.9 | 17.3 | 9.1 | 4.4 |
| Membranes | 1.6 | 0.4 | 0.2 | 0.6 | 0.0 | 0.4 | 0.6 | 0.2 | 0.5 |
| Softening | 10.2 | 4.8 | 8.9 | 9.6 | 9.7 | 5.0 | 4.9 | 2.3 | 7.8 |

Data from Ref. 8.

district. Systems using groundwater supplies had a much greater number of violations than systems using surface water supplies. Between the years 2001 and 2005, the number of violations in the country has steadily increased from 82,655 to 118,420, although the population affected appears to have randomly varied from year to year (ranging from about 13 million to 26 million). Most of the violations were for microbial (about 45,000 violations) and for lead and copper violations (about 13,000) in the FY 2005. Of these violations, the most common problems were related to meeting the total coliform rule/turbidity criteria (about 35,000 violations). By far, most of the violations were associated with very small systems (e.g. they had about 10 times the violation rate per number of systems compared to the very large systems).

## 2.4 Wastewater Treatment

Traditional municipal biological wastewater treatment consists of the following steps: sedimentation, biological treatment (often through an activated sludge process), secondary clarification, filtration, and disinfection. Biosolids are generated from the waste activated sludge. Figure 5 shows the increasing percentage of the US population served by centralized wastewater treatment systems. Most of the remaining population is served by household septic tank systems. The first wastewater treatment plants in the United States were built in the late 1800s and used primary treatment with physical sedimentation of solids and floatation/skimmer removal of floating material before discharges to nearby receiving waters. Activated sludge treatment plants (secondary treatment) were built starting in 1916, although they were not required throughout the country until 1972. Almost 99% of all wastewater treatment plants provided secondary treatment by 1996.

Table 6 is from the *Clean Watersheds Needs Survey Report to Congress* [9] and indicates the number of facilities reporting in the survey as a function of facility size. Most of the plants are relatively small (the median size is $<1$ MGD), although most of the nation's wastewater is treated in much larger plants (median size in the 10–100 MGD range). The

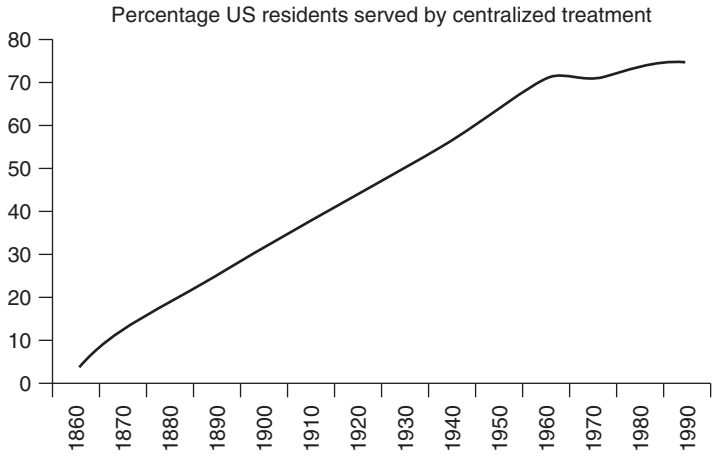



**FIGURE 5** Percentage of US residents served by centralized wastewater treatment plants [12].

**TABLE 6 Wastewater Treatment Facilities by Flow Capacity (not All States Reporting)**

| Design Flow Range (MGD) | Number of Facilities | Total Future Design Flow Capacity in Range (MGD) |
|---|---|---|
| 0.001–0.1 | 6112 | 298 |
| 0.1–1 | 7223 | 2750 |
| 1–10 | 3525 | 12,081 |
| 10–100 | 748 | 19,873 |
| 100 and greater | 64 | 15,040 |
| Total | 17,674 | 50,042 |

MGD = millions of gallons per day [9].

**TABLE 7 Technologies Used in Wastewater Treatment Facilities in the United States (2000 survey)**

| | Number of Facilities Reporting | Future Design Capacity (MGD) | Percent of US Population |
|---|---|---|---|
| Less than secondary | 27 | 481 | 1.2 |
| Secondary | 9463 | 20,008 | 31.9 |
| Greater than secondary | 5739 | 26,239 | 43.2 |
| No discharge | 2221 | 2,579 | 6.5 |
| Partial treatment | 224 | 734 | n/a |
| Total | 17,674 | 50,041 | 82.8 |

See Ref. 9.

different types of treatment technologies employed in the wastewater treatment facilities surveyed by the EPA are shown in Table 7. As previously noted, almost all of the US wastewater treatment facilities provide at least secondary treatment, with almost half of the population's sewage now receiving advanced treatment (e.g. filtration and/or biological nutrient removal). For example, within the next decade, many wastewater plants in the Chesapeake Bay watershed will be investigating and/or installing either biological nutrient removal (BNR) or enhanced nutrient removal (ENR) treatment strategies in response to the nutrient discharge caps enacted in several of the watershed's tributary states.

## 2.5 Distribution and Conveyance Systems

Limited information is available about the amount of additional infrastructure (piping, pumps, storage tanks, pump stations, etc.) in the drinking water distribution and waste water collection systems. One estimate, from the American Water Works Association database, states that there were approximately 1.43 million km (867,000 mi) of municipal water piping in the United States in 2000 [10]. One estimate of the amount of sanitary sewer pipe in the United States as of 1980, is approximately 1.2 million km (4 billion ft), up from an earlier estimated length of pipe in 1960 of 500,000 km (300,000 mi) [11].

## 3 WATER AND WASTEWATER INFRASTRUCTURE COMPONENT NEEDS

In 2002, the US EPA conducted an analysis of the infrastructure needs associated with the nation's clean water (wastewater and stormwater treatment and disposal) and drinking water (treatment and supply) systems for the 20-year period from 2000 to 2019. In the preface to the report, the Assistant Administrator for Water stated the following reasons for conducting this analysis:

> As our economy and population grow, we must periodically take a good look at the challenges ahead and reassess our nation's needs for infrastructure to ensure clean and safe water. By "infrastructure" we mean the pipes, treatment plants, and other critical components that deliver safe drinking water to our taps and remove waste water from our homes and other buildings. Recognizing the importance of having a common understanding of the challenges ahead, the US Environmental Protection Agency (EPA) undertook a "Gap Analysis" to review the historical patterns of infrastructure investment, compare it to projections of future needs, and provide a transparent assessment of the gap between needs and spending.

The report found that much of the current gap is associated with deferred maintenance, inadequate capital replacement, and a general aging of the infrastructure. In addition, population growth and increasing water consumption have also contributed to the critical needs facing the nation's water systems. Although this gap may be very large if not addressed (about $400 billion for clean water, which they define as treating wastewater, and about $300 billion for drinking water), they concluded that it would largely disappear if municipalities increased their clean water and drinking water spending at a modest real rate of growth of 3% per year over this 20-year period.

In the 20 years since the mid-1970s, communities spent about $1 trillion on drinking water treatment and supply and wastewater treatment and disposal works. However, future investments are needed to keep pace with growth in demand and to replace and repair deteriorating water infrastructure. Table 8 lists the typical expected service life for various water system components. Many of these components have long expected lives, but they also require substantial maintenance efforts to ensure continued high levels of service. Without continued maintenance, natural deterioration will significantly reduce the usefulness of the components.

The EPA [8] also reported an AWWA study that concluded that expenditures to repair and replace deteriorating infrastructure will increase steadily over the next 30 years. The 1996 Clean Water Needs Survey reported major categories of future expenditures, as shown in Table 9. The total costs were $225 billion dollars in 2001.

One indication of the recent growth in water system infrastructure is illustrated in Figure 6 [8] which shows the miles of sanitary sewer pipes installed per decade. Figure 7 is a plot showing the expected average age of this installed wastewater collection network. The expected average age is expected to increase to more than half of the service life estimate by 2050. Table 10 shows the classification of the condition of this pipe network

**TABLE 8 Useful Life of Drinking Water and Wastewater Components [8]**

| **Wastewater Components** | |
|---|---|
| **Useful Life** | **Component** |
| 80–100 | Collections |
| 50 | Treatment plants—concrete structures |
| 15–25 | Treatment plants—mechanical and electrical |
| 25 | Force mains |
| 50 | Pumping stations—concrete structures |
| 15 | Pumping stations—mechanical and electrical |
| 90–100 | Interceptors |
| **Drinking Water Components** | |
| **Useful Life** | **Component** |
| 50–80 | Reservoirs and dams |
| 60–70 | Treatment plants—concrete structures |
| 15–25 | Treatment plants—mechanical and electrical |
| 65–95 | Trunk mains |
| 60–70 | Pumping stations—concrete structures |
| 25 | Pumping stations—mechanical and electrical |
| 65–95 | Distribution systems |

**TABLE 9 1996 Clean Water Needs by Category [8]**

| | |
|---|---|
| New collectors and interceptors | 11% |
| Treatment works | 22% |
| Separate sanitary sewer overflow (SSO) corrections | 41% |
| Phase 1 stormwater | 4% |
| Combined sewer overflow (CSO) control | 22% |

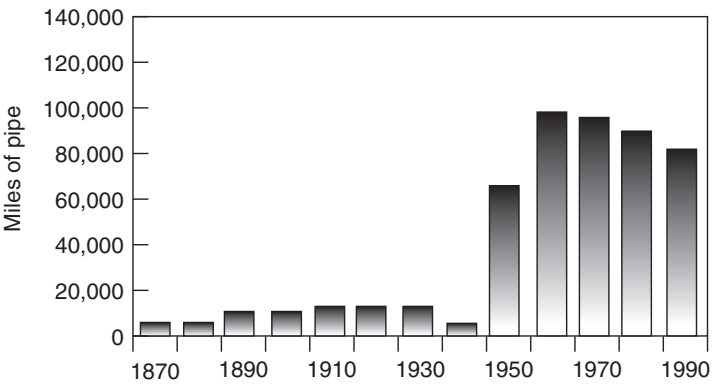



**FIGURE 6** Sanitary Sewer Pipe Installed per Decade [8].

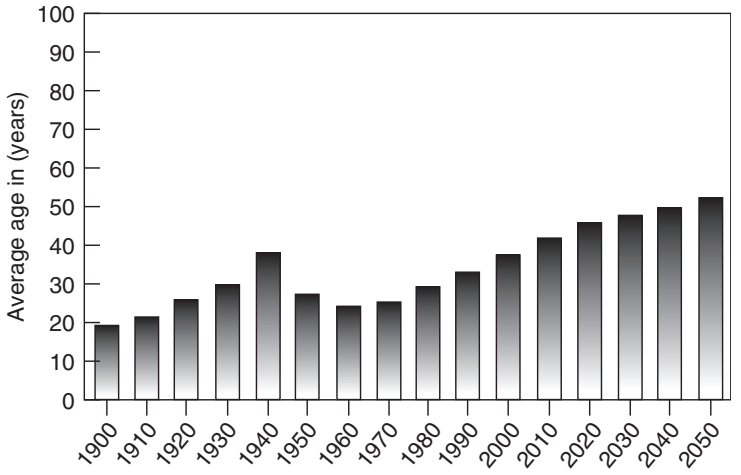



**FIGURE 7** Average Age of Wastewater Collection Pipe [8].

**TABLE 10 Deterioration of Sanitary Sewer Pipe Network with Time [8]**

| Year | Excellent | Good | Fair | Poor | Very Poor | Life Elapsed |
|---|---|---|---|---|---|---|
| 1980 | 69% | 19% | 3% | 3% | 2% | 5% |
| 2000 | 43 | 17 | 18 | 14 | 2 | 7 |
| 2020 | 33 | 11 | 12 | 13 | 23 | 9 |

from 1980 to expected 2020 conditions. The increased amount of poor, or worse, condition pipe is very obvious, and is likely to cause increasing failures (sanitary sewer overflows (SSOs), breakages, and flow capacity losses).

The needs survey and gap analysis is known to underestimate the gap for stormwater drainage and treatment systems. As indicated above, about 4% of the calculated gap is associated with Phase I stormwater communities. Locklear [13] notes that the need surveys recently conducted do not consider many documented stormwater issues. It is felt that the next needs survey, scheduled to be conducted in 2008, will be more comprehensive and accurate. As an example, the 2000 Needs Survey identified $5.5 billion over the next 20 years to address stormwater management needs, based on data from 19 states and the District of Columbia. However, a recent stormwater needs survey conducted by the California section of the ASCE (*the Infrastructure Report Card* [14]) identified this same amount just for their state.

The Water Infrastructure Network report released in 2001 states that if the water and wastewater infrastructure fails, the nation "risks reversing the public health, environmental, and economic gains of the last three decades [15]."

## REFERENCES


1. EPA (2002). *Community Water System Survey 2000*, EPA 815-R-02-005A, Office of Wastewater, Washington, DC. (Presented in *The Water Encyclopedia*, 3rd ed., CRC, Boca Raton, 2007.)
2. Federal Council for Science and Technology (1962). Panel on Hydrology, *Scientific Hydrology*, *Washington DC*. (Presented in *The Water Encyclopedia*, 3rd ed., CRC Press, Boca Raton, 2007.)
3. Hutson, S. S. et al. (2004). *Estimated Use of Water in the United States in 2000*. U.S. Geological Survey Circular 1268, www.usgs.gov (Presented in The Water Encyclopedia, 3rd ed., CRC, Boca Raton, 2007).
4. Fierro, P. and E. K. Nyer (2007). *The Water Encyclopedia*, 3rd ed., CRC Taylor & Francis, Boca Raton.
5. ERS (1988). *1988 Farm and Ranch Irrigation Survey*, USDA, www.ers.usda.gov. (Presented in The Water Encyclopedia, 3rd ed., CRC, Boca Raton, 2007.)
6. U.S. Water Resources Council. (2002). *Second National Water Assessment, The Nation's Water Resources 1975–2000*. (Presented in The Water Encyclopedia, 3rd ed., CRC, Boca Raton, 2007.)
7. EPA (2006). *FACTOIDS: Drinking Water and Ground Water Statistics for 2005*, Office of Water (4606M), Washington, DC, EPA 816-K-03-001, 15 p.
8. EPA (2002). *The Clean Water and Drinking Water Infrastructure Gap Analysis*, Office of Water (4606M), Washington, DC, EPA 816-R-02-020, 54 p.
9. EPA (2003). *2000 Clean Watersheds Needs Survey Report to Congress*, Office of Wastewater, Washington, DC, www.epa.gov/owm/mtb/cwns/2000rtc/cwns2000-appendix-c.pdf. Accessed October 25, 2007.
10. Brongers, M. P. H. (2006). *The Cost of Corrosion: Drinking Water & Sewer Systems*, CC Technologies, Dublin, OH, URL: http://www.corrosioncost.com/utilities/water/index.htm. Accessed: October 31, 2007.
11. Kollar, K. L. (1966). *Regional Requirements for Sewer pipe in Sewage Utilities*, U.S. Department of Commerce. (Presented in The Water Encyclopedia, 2nd ed., CRC, Washington DC, 1990.)
12. EPA (2003). *Draft Handbook for Management of On-Site and Clustered (Decentralized) Wastewater Treatment Systems*, Office of Water, Washington, DC, EPA/PA 823/P-03/001. (Presented in The Water Encyclopedia, 3rd ed., eRC, Boca Raton, 2007.)
13. Locklear, H. H. P. (2007). Mind the gap. *Stormwater*. Vol. 8, No. 8, pp 84–88.
14. ASCE California Section (2006). *Infrastructure Report Card 2006. A Citizen's Guide*, www.ascecareportcard.org/. Accessed October 26, 2007.
15. Water Infrastructure Network (2001). *Infrastructure Now: Recommendations for Clean and Safe Water in the 21st Century*, http://www.winwater.org/reports/winow.pdf. Accessed Oct 27, 2007.


## FURTHER READING


Chin, D.A. (2006). *Water Resources Engineering*, 2nd ed., Prentice Hall, Upper Saddle River, NJ.

EPA Urban Watershed Management Branch (2007). http://www.epa.gov/ednnrmrl/.

EPA's "Surf your watershed" homepage (2007). http://www.epa.gov/surf/.

# PROTECTING WATER INFRASTRUCTURE IN THE UNITED STATES

JONATHAN G. HERRMANN, KATHLEEN A. NICKEL, AND AMELIA D. MCCALL
*National Homeland Security Research Center, U.S. Environmental Protection Agency, Cincinnati, Ohio*

## 1 INTRODUCTION

Ensuring clean and safe water has been the responsibility of the US Environmental Protection Agency (EPA) since it was formed in 1970. Water infrastructure was designated one of a number of critical infrastructures for the United States, and EPA was designated the lead federal agency responsible for protecting water systems by Presidential Decision Directive 63 (PDD-63) [1]. Following the terrorist attacks of September 11, 2001, water system protection became an even more important national public health and safety priority. Beginning with the *Public Health Security and Bioterrorism Preparedness and Response Act* (Bioterrorism Act) of 2002 and continuing with a series of Homeland Security Presidential Directives (HSPDs), both Congress and the White House have further recognized the water sector as a critical infrastructure deserving protection from threats and intentional attacks.

Federal agencies and water utilities have been directed by both the legislative and executive branches of government to take steps that heighten the security and protection of the water sector. Consistent with these legislative and executive requirements, EPA has taken many actions, in collaboration with partners from the water industry, academia, and other government agencies, to better protect the nation's water infrastructure. This article contains an overview of some of these actions as well as an appendix that describes contaminants of interest to the water sector.

## 2 WATER SECURITY

In the United States, water systems are vitally important to public health. These systems may be government owned or privately held facilities that draw water from underground aquifers or surface water sources (i.e. rivers, lakes, and reservoirs). Approximately, 90% of the United States' population is supplied by water from one of these systems [2]. A public water supply consists of a water source, conveyance systems (e.g. pipes and pumps), a treatment plant, and storage facilities. Wastewater systems are also part of the

water sector. These systems consist of sewer pipes, storm water drains and ditches, a treatment plant, and a body of water that receives the treated effluent and storm water runoff.

**BOX 1 HSPD SIDEBAR**

Shortly following the terrorist attacks of 2001, the Office of the President began issuing a series of HSPDs, which task federal departments and agencies with specific responsibilities and communicate presidential decisions concerning national homeland security policy.

- [*] *PDD 63: Critical Infrastructure Protection.* (1998) mandated that public and private organizations must be able to maintain the continuity of the US critical infrastructure in the event of a terrorist attack. Critical infrastructure includes the physical and cyber-based systems that are essential for the economy and the government to operate at a minimum level. Water systems were identified as a critical infrastructure.
- *HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection.* (2003) established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and key resources and to protect them from terrorist attacks. Water infrastructure protection is explicitly tasked to EPA, whose responsibilities include conducting or facilitating vulnerability assessments of the sector and encouraging risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.
- *HSPD-8: National Preparedness.* (2003) required the establishment of a national domestic all-hazards preparedness goal and described the way federal departments and agencies will prepare for a response to a national incident. It includes a system for assessing the nation's overall readiness to respond to major events, especially those involving acts of terrorism.
- *HSPD-9: Defense of United States Agriculture and Food.* (2004) established a national policy to defend agriculture and food systems against terrorist attacks, major disasters, and other emergencies. It required EPA to build upon/expand current drinking water monitoring and surveillance programs.
- *HSPD-10: BioDefense for the Twenty-first Century.* (2004) directed agencies to develop standards, protocols, and capabilities to address the risks of contamination following a biological weapons attack and to develop strategies, guidelines, and plans for decontamination of persons, equipment, and facilities—including water infrastructure.
- *HSPD-19: Combating Terrorist Use of Explosives in the United States.* (2007) established a national policy and called for the development of a national strategy and implementation plan on the prevention and detection of, protection against, and response to terrorist use of explosives in the United States.

[*]HSPD-7 specifically supersedes PDD 63.

The important role that the nation's water sector plays in providing the public with clean and safe water has made water security a national priority. The Bioterrorism Act of 2002 required water utilities serving more than 3300 people to complete vulnerability assessments of their facilities and then prepare emergency response plans. EPA provided guidance, computer-based tools, and, in some cases, funding to assist the utilities in conducting their vulnerability assessments. Understanding their facilities' vulnerabilities provides owners and operators with a means of prioritizing activities and investments to protect their utility's assets.

As the lead federal agency for ensuring the security of the water sector, EPA works closely with experts from the water industry to continually improve the ability of water and wastewater utility owners and operators to prevent, detect, respond to, and effectively recover from attacks on their systems. EPA has been guided in this effort by national organizations and associated experts, including the National Drinking Water Advisory Council (NDWAC), the American Water Works Association (AWWA), the Water Environment Federation (WEF), the National Research Council (NRC) of the National Academies, and EPA's Science Advisory Board (SAB). The expertise provided has helped EPA identify data needs and research gaps. The research needs and information gaps are being addressed either by EPA scientists and engineers or researchers in other organizations with a strong interest in water systems research and water sector protection.

## 2.1 Recommendations of the National Drinking Water Advisory Council

The Water Security Working Group (Work Group) was charged by the NDWAC with identifying security practices, incentives for improvements in security, and measures of security progress. In response to this charge, the Work Group reached consensus on 14 findings that (i) established the features of active and effective security programs, (ii) identified ways government personnel and others might encourage utilities to adopt and maintain active and effective programs, and (iii) suggested utility-specific and national measures of water sector security progress [3].

The Work Group suggested three aggregate performance measures that would provide an indication of progress with respect to securing the nation's drinking water:

1. Implementation of "active and effective" security programs as measured by the number of utilities implementing the 14 program features (Box 2).
2. Reduction in security risk as measured by the number of high security-risk assets lowered to medium- or low risk (based on the results of vulnerability assessments).
3. Reduction in the inherent risk potential of utility operations as measured by a reduction in the use of hazardous substances by utilities and specifically the number of utilities that convert from gaseous chlorine to other forms of chlorine or other treatment methods [3].

**BOX 2 FOURTEEN FEATURES OF AN ACTIVE AND EFFECTIVE WATER SECURITY PROGRAM**

1. Make a commitment to water security
2. Promote security awareness
3. Identify those in charge
4. Assess vulnerabilities—keep vulnerability assessments up to date
5. Identify security priorities and resources
6. Employ protocols to detect contamination
7. Monitor threat level information
8. Develop measures to assess security program
9. Incorporate security into emergency response plans
10. Establish controls to restrict access
11. Identify sensitive information and restrict access to sensitive communications
12. Incorporate security into construction designs
13. Implement strategies for communication with employees, response organizations and customers
14. Forge partnerships with community, infrastructures, and response organizations

## 2.2 Critical Infrastructure and Key Resource Sector-Specific Plan

As NDWAC's Work Group was evaluating the security practices of the water industry and contemplating its recommendations, EPA was conducting a complementary evaluation. As required by HSPD-7: Critical Infrastructure Identification, Prioritization, and Protection [4], the Department of Homeland Security prepared a National Infrastructure Protection Plan that mandated the development of and established the framework/guidelines for drafting sector-specific plans (SSPs). EPA, as the sector lead, prepared the SSP for water. The SSP specifically laid out a number of security goals and objectives for the sector:

**Goal 1: Sustain protection of public health and the environment**

- *Objective 1.* Encourage integration of security concepts into daily business operations at utilities.
- *Objective 2.* Evaluate and develop surveillance, monitoring, and warning capabilities to recognize risks, and develop response capabilities to respond to those warnings.
- *Objective 3.* Develop a nationwide laboratory network for water quality that integrates federal and state laboratory resources and uses standardized diagnostic

protocols and procedures, or develop a supporting laboratory network capable of analyzing water quality for security threat agents.

**Goal 2: Recognize and reduce risks in the water sector**

- *Objective 1.* Improve identification of vulnerabilities with the intent of increasing the sector's overall security posture.
- *Objective 2.* Improve identification of potential threats through information sharing between sector partners (water utilities; national associations; and federal, state, and local governments).
- *Objective 3.* Identify public health and economic impact consequences of man-made or natural incidents to improve utility risk assessments.

**Goal 3: Maintain a resilient infrastructure**

- *Objective 1.* Emphasize continuity of drinking water and wastewater services as they pertain to utility emergency preparedness, response, and recovery planning.
- *Objective 2.* Explore and expand implementation of mutual aid agreements/compacts in the water sector.
- *Objective 3.* Identify and implement key response and recovery strategies.
- *Objective 4.* Increase understanding of how the sector is interdependent with other critical infrastructure sectors.

**Goal 4: Increase communication, outreach, and public confidence**

- *Objective 1.* Communicate with the public about the level of security and resilience in the water sector, and provide outreach to ensure the public's ability to be prepared for and respond to a natural disaster or man-made incident.
- *Objective 2.* Enhance communication and coordination among utilities and federal, state, and local officials and agencies to provide information about threats.
- *Objective 3.* Improve relationships among all water sector security partners through a strong public–private partnership characterized by trusted relationships [5].

In addition to its own goals and objectives, the SPP acknowledged the performance measures offered by the Work Group and is aligning these measures with its own aforementioned goals [5].

## 3 RESEARCH ON WATER INFRASTRUCTURE

Science and technology are powerful tools being used to achieve the goal of securing our nation from terrorist threats and attacks. Internationally recognized experts in diverse fields of science and engineering are dedicated to this goal. Researchers at EPA and throughout the federal sector are developing strategies and techniques that help prevent, prepare for, and recover from public health and environmental emergencies arising from intentional attacks on our nation's infrastructure.

One of EPA's most ambitious research initiatives was the development of the *Water Security Research and Technical Support Action Plan* (herein referred to as the *action plan*) [6]. The action plan defines numerous projects that result in strategies and tools to protect water infrastructure. The plan was developed following multiple meetings, held in late 2002 through early 2003. These meetings involved stakeholders from the water sector, public health officials, emergency and remedial response personnel, and

representatives from other federal agencies. Following the meetings, and as part of its own evaluation of potential threats, EPA developed a plan to meet the water sector's security needs. The action plan identifies projects under way or planned by EPA. The action plan is written in such a way that other organizations can also conduct projects that are identified. The National Academy of Sciences reviewed the action plan in May and July of 2003, subsequently endorsing it. The action plan was implemented in October of 2003.

Research conducted under the action plan has resulted, and will continue to result, in products that support the water sector in several ways. These products are (i) strategies to prevent damage from attacks, (ii) tools to rapidly detect contamination, (iii) techniques to rapidly contain contamination and mitigate contamination impacts, and (iv) methods to support rapid recovery following an attack. The action plan reflects EPA's interests in physical and cyber attacks as well as contamination events involving chemical, biological, and radiological contaminants.

### 3.1 Protecting Drinking Water Systems from Physical and Cyber Attacks

Physical attacks range from minor acts of vandalism to major incidents that can result in damage to structures such as pumps, pipelines, and storage facilities. These attacks can disrupt service, resulting in loss of potable water to residences and industries, and loss of water for emergency services such as fire control. Disruption in service by the water sector can quickly result in a public health emergency not only due to shortages in drinking water but also due to failure to supply water to critical and interdependent facilities, such as medical facilities and energy plants. Cyber attacks, as they relate to the water sector, generally affect the supervisory controls and data acquisition (SCADA) equipment that is used to operate treatment plants and distribution systems. SCADA systems are used to automate plant operations such as the opening and closing of valves, addition of treatment chemicals, and operation of pumps. Plant operations could be impacted by hackers who disrupt these operations.

With support from EPA and the water industry, the American Society of Civil Engineers (ASCEs) has developed voluntary design standards for new construction, reconstruction, and retrofitting water facilities with a focus on security. The standards include minimum security standards for SCADA and other computer systems used by the water industry. The design standards are available on the ASCE website (http://www.asce.org/wise). In addition, EPA is developing recommendations for countermeasures, such as redundant systems to mitigate the impacts of attacks. The Agency has also issued information on establishing collaborations with other water utilities and sectors to share information and resources in preparation for and response to service disruptions.

Continually analyzing threats is important not only for protecting the water sector, but also for understanding the cascading effects on interdependent sectors. Recently, local, state, and federal officials and representatives from private industry met to review a case study involving a power outage in the Washington, DC, area and its impacts on various sectors. The analysis resulted in several lessons learned and functioned as a "wake-up call" to the participants. The incident evaluated was a Category 2 hurricane that resulted in an extensive, yet short-term power outage. Participants realized the need for additional planning to successfully manage a longer-term crisis. Lessons learned from the exercise are summarized in Box 3.

**BOX 3 LESSONS LEARNED FROM HURRICANE CASE STUDY**

- Staffing.
  - prepare contingency staffing plans;
  - cross-train employees and minimize multiple responsibilities for individuals;
  - prepare for long-term events (staff sustainability);
  - consider and plan for the needs of employees' families;
  - use Emergency Operations Center (EOC) and resources from other agencies and organizations (i.e. Parks and Recreation Department, trade associations, neighboring jurisdictions, and larger utilities).
- Communications.
  - provide redundant communication technologies (800 MHz radios, amateur radio, and cell phones)
  - develop protocols for regular interagency and interdisciplinary communication;
  - enhance timeliness and effectiveness of communication to the public, including alternative methods to communicate emergency measures when standard modes, such as television and radio, are not available due to power loss.
- Practice urban forestry planning and regular tree trimming to prevent downed trees and limbs that, in turn, can down power lines.
- Identify sources for rapid financial aid.
- Improve fuel supplies and stockpiles for response and recovery.
- Establish or improve upon mutual aid and assistance agreements [7].

### 3.2 Identification of Drinking Water Contamination Threats and Threat Scenarios

The combination of a contaminant and the circumstances of its use comprise a threat scenario. EPA has made significant progress in identifying priority contaminants and evaluating how they might be used to harm the water sector. Threat scenarios were identified and prioritized through an analysis of the potential health effects of the contaminant, the availability and quantity of the contaminant needed to cause harm, and the modes by which the contaminant could be introduced to a drinking water system. Because they provide information on water sector vulnerabilities, the threat scenarios are contained in classified documents.

EPA has initiated several projects to better understand the nature of contaminants of interest. These projects include compilation of information on the properties of these contaminants into a comprehensive, computer-based tool with links to information and databases maintained by multiple agencies. These sources provide information about toxicology, personal protective equipment, disposal guidance, and more that need to be easily and quickly accessed during an emergency.

Since many of these contaminants have not previously been considered for use in intentional attacks, additional study is needed to fully understand their impacts on human

health and the environment. Although some, such as the chemical warfare agents, have been studied by the military, their impacts on the general public health would in all likelihood be more protective. Exposure to levels of contaminants that would not result in health impacts to young, healthy individuals could have tragic results for sensitive populations such as the immune compromised and the elderly in the nation's general population.

Research is under way to supplement the current knowledge base on contaminants of interest. Because of the hazards posed by these contaminants, EPA and its partners are working to identify surrogates and simulants. Surrogates and simulants are chemical, radiological, or biological agents that behave in a manner similar to the contaminants of interest, but because they are not as toxic or pathogenic, they can be more safely used in research experiments. Researchers from government and industry worldwide are interested in the identification of these surrogates and simulants to support their research.

### 3.3 Improving Analytical Methodologies and Monitoring Systems for Drinking Water

A water utility's ability to rapidly contain contaminated water and manage the consequences of a contamination event is very important. It is dependent on the water utility's ability to quickly detect a change in water quality and identify the contaminant(s) responsible for that change. Experiments involving water quality sensors' responses to contamination in a water distribution system are being conducted by EPA. Contaminants are injected into distribution system simulators, and the responses of commercially available water quality sensors are evaluated. Common water quality sensors are being tested because many water utilities already use them to monitor general water quality and are knowledgeable about their operation and maintenance. It is anticipated that these same sensors will be successful in alerting a utility to intentional contamination events.

Experiments conducted to date involved challenging 20 water quality sensors to detect over 25 contaminants injected into the distribution system simulators.

Water utilities most commonly monitor free and total chlorine, total organic carbon (TOC), specific conductance, oxidation reduction potential (ORP), pH, and turbidity as indicators of general water quality. Of all the water quality sensors tested, those monitoring free chlorine and TOC detected the widest array of contaminants. Both free chlorine and TOC levels were changed by the presence of the contaminants in the water. For example, herbicides and pesticides produced a large decrease in free chlorine and an increase in TOC due to their organic content.

Compounds such as inorganic arsenite decreased free chlorine but did not affect TOC. Biological suspensions of nonpathogenic *Escherichia coli* and spore-forming bacteria (meant to simulate the bacteria that cause anthrax) were also tested. When tested in their growth media, free chlorine was consumed and TOC increased. It was not the bacteria themselves that were detected by the sensor, but the growth media. Military agents such as nerve, choking, blister, and blood agents were tested at an off-site facility capable of handling these contaminants of interest. Free/total chlorine and/or TOC detected all four of these types of contaminants. The laboratory experiments showed that the use of on-line water quality sensors as part of a contamination warning systems is feasible, and as a result, field testing is being piloted at water utilities around the United States.

Although the ability of water quality sensors to rapidly detect changes in water quality is encouraging, currently available sensors cannot define the specific contaminant responsible for the change. Laboratory analysis is necessary to identify the contaminant(s) in the water. Complicating the laboratories' task is a lack of validated analytical methods that can be used to confirm the identity of contaminants in water samples. Many of the contaminants of interest with respect to intentional contamination of water supplies have not previously been considered as terrorist threats. As such, methods to detect many of these contaminants in water have not been developed, or if developed, have not been tested with stringent quality controls and then validated through a multiple laboratory process.

To begin to address this issue, EPA compiled *Standard Analytical Methods for Use Following a Homeland Security Event (SAM)* [8]. This document was prepared to ensure that all laboratories use the same analytical methods following a homeland security incident so that results are comparable. SAM includes the best, currently available methods. Some of the methods are routinely used in nonenvironmental applications, such as medical diagnostics, but have not been applied to environmental matrices, such as water. Efforts are under way to adapt these methods for use with environmental samples that have interferences not experienced with clinical samples. Candidate methods will be put through a rigorous process of validation by multiple laboratories. It is only after successful completion of multilaboratory validation that a method will be considered acceptable as a standard method.

Successful analysis of biological agents in water involves a unique complication. The concentrations of microbes in water samples may be very low compared with those typically seen in clinical samples (e.g. blood). Detection of very low concentrations of microbes in water can be difficult: analogous to finding a needle in a haystack. Yet there are no agreed upon safe levels for many microbes in water. Thus, it is necessary to detect the proverbial needle. To do so, the sample must be concentrated; in other words, the amount of water in the sample must be reduced while retaining the microbes. EPA has developed an ultrafiltration apparatus and a tested protocol to concentrate microbes in water samples and increase the probability of detection. The apparatus uses nonreactive hollow fiber membranes (polysulfone or low protein binding membranes) as the preferred medium for filtering.

The system operates with 5–10 lb/in.$^2$ difference between the sample and concentrate reservoirs. This difference forces water through the membrane. Microbes cannot pass through the membrane, while some water is forced through the membrane by the pressure differential. The ultrafilter concentrates the microorganisms and sends them to the concentrate reservoir. The concentrate recirculates and mixes with more undiluted sample until the entire volume has been reduced to a target volume. A successful prototype of the apparatus has been built and tested. Preliminary test results indicate that water samples ranging in volume from 10 to 1000 l can be concentrated down to approximately 250 ml. Concentration reduces the risks associated with transporting large quantities of contaminated water samples in addition to aiding the analysis by increasing the probability of detection.

Effective sample collection, preparation, and analytical methods are imperative to rapid detection and containment of contamination. Equally critical is the establishment of a network of capable and well-equipped laboratories. EPA is working to establish a network of laboratories that can perform both presumptive and confirmatory analysis of environmental samples. The model for this network is Centers for Disease Control

and Prevention (CDC)'s laboratory response network (LRN) for clinical samples, which has been in operation for many years. Consistent with the CDC model, the environmental response laboratory network (ERLN) will consist of many laboratories capable of performing presumptive analyses using methods available in the open literature.

Fewer labs, employing rigorous quality assurance protocols, will have the capability for confirmatory analyses. Still fewer (reference) laboratories will have access to classified methods and these laboratories would be capable of detailed analysis and forensic investigations. In the case of environmental samples, presumptive analyses will be performed by water utility laboratories, hazardous materials teams, and contractor laboratories; confirmatory analysis will be reserved for state and federal government laboratories; and finally, federal government labs (i.e. EPA and Department of Energy) will maintain reference laboratory capabilities.

### 3.4 Containing, Treating, Decontaminating, and Disposing of Contaminated Water and Materials

Containing contaminated water in a distribution system is a challenge due to the quantity and velocity of the water moving through the system. By the time suspicious water quality is detected, the water may have reached an exposure point (i.e. household, manufacturing plan, and medical facility). There are financial, technical, and health implications associated with shutting down a distribution system. As such, it is imperative to not only rapidly detect changes in water quality in a distribution system, but also understand the significance of these changes such that responsible risk management decisions can be made. EPA has developed software to help utility managers understand the fate of contaminants in their distribution systems, to optimally place water quality sensors, and to interpret data collected by these sensors.

A computer model, EPANET, is commonly used by water utilities to understand flow and contaminant transport through distribution systems. Until recently, EPANET has been limited to tracking the dynamics of a single chemical transported through a network of pipes and storage tanks, such as a fluoride used in a tracer study or free chlorine used in a disinfection decay study. EPA has released an extension to EPANET called *EPANET-MSX* (MultiSpecies eXtension) that considers multiple interacting species in both the water flow and on the pipe walls. This capability has been incorporated into a stand-alone program as well as a toolkit library of functions that programmers can use to build customized applications. The software can be downloaded free of charge from the EPA website (http://www.epa.gov/nhsrc/news/news073007a.html). EPANET-MSX allows users the flexibility to model a wide range of chemical reactions of interest including free chlorine loss, the formation of disinfection by-products, nitrification dynamics, disinfectant residuals, and adsorption on pipe walls. Homeland security researchers are particularly interested in modeling the fate and transport of contaminants of interest in drinking water distribution systems.

In addition to models that predict contaminant fate in a distribution system, EPA has developed a computer-based sensor placement optimization tool (SPOT). Given the current state of sensor technology and the interest in better understanding water quality in distribution systems, many water utilities have been installing water quality sensors as part of a contamination warning system. As discussed in the previous section, research has shown that in the presence of contaminants, water quality sensors are able to detect changes in free chlorine, TOC, ORP, specific conductance, and other parameters. SPOT

allows users to select design objectives and compare and contrast the benefits of different sensor placements.

Water quality monitoring stations can provide information about general water quality conditions only at a specific location and time. If these monitoring stations are isolated from each other, detecting a contaminant and its movement is extremely difficult. This limitation is compounded by the fact that water quality at a given location can be highly variable, with several factors affecting it including pump and tank operations, system demand, and source water quality. To address these factors, EPA's research program has developed "Canary", an event detection system (EDS) named for the "canary in a coal mine" analogy. Canary is a software program that processes data from water quality sensors in real time and predicts whether the recorded water quality changes are the result of a contamination event or natural variations in water quality. Sophisticated algorithms incorporated into EDS tools like Canary can efficiently mine large amounts of water quality data produced by monitoring stations and detect anomalies that are indicative of contamination or other water quality problems. The early detection system tool implemented as part of a contamination warning system is critical to the performance and reliability of the system

The success of any computer modeling tool is dependent on the quality of its input data. The environmental fate of chemical, biological, and radiological contaminants needs to be better understood if models are to perform optimally. Of particular interest is what happens to contaminants when dispersed in source waters (e.g. rivers, lakes, and groundwater), water treatment plants, or distribution systems (e.g. pipelines and storage tanks).

Concentrations of chemical, biological, or radiological contaminants in source waters will, in many cases, be reduced to below levels of concern through dilution and routine treatment at a drinking water plant. In cases where even very low levels of contaminants produce toxicity or aesthetically unpleasant results, dilution may not provide adequate safety assurances. This is particularly true, posttreatment, in the distribution system. Also, some contaminants may attach themselves to pipe walls in a water distribution system, resulting in the slow release of contaminants back into the water. Attachment could be directly onto the pipe wall material, the biofilm layer, or corrosion-inhibiting layers intentionally deposited on the pipe walls.

A better understanding is needed regarding which contaminants may attach to the interior of the water distribution system and how they can best be removed. EPA is currently researching the fate and persistence of various contaminants in distribution systems and conducting experiments using a variety of decontamination and inactivation techniques to determine their effectiveness. Decontamination in this context refers to the removal of contamination; whereas, inactivation refers to the diminishment or elimination of a contaminant's toxicity or pathogenicity. Ultimately, a guide that documents the effectiveness of decontamination and inactivation techniques will be produced.

Although complete and rapid removal or inactivation of contamination is the goal following a terrorist attack on a water supply, this goal may not always be achievable. For some contaminants, flushing the pipes or treatment of the water by chlorination or other methods may be sufficient to remove them. However, for other chemicals, disposal of contaminated piping and treatment system components may be necessary. To assist utilities faced with the prospect of disposing of these materials, EPA developed a web-based decision support tool (DST). The DST assists in the disposal of residues from

the cleanup of contaminated water systems and other structures by providing information needed for selection of an appropriate disposal facility.

Included with this information is pertinent regulatory requirements and facility contact and permit information. The tool contains the ability to quickly estimate quantities and characteristics of residues produced during cleanup operations so that cost trade-offs between decontamination and disposal can be evaluated early in the process of restoring a contaminated facility. This information is then incorporated into the detailed waste profiles needed to negotiate contracts with disposal facilities and transportation companies. The DST provides information to assist in decision making relevant to decontamination and disposal of materials associated with drinking water treatment plants, distribution systems, water-using equipment and appliances, wastewater treatment plants, and a number of types of buildings. The disposal tool is available for use with permission and can be accessed through the EPA website (http://www.epa.gov/nhsrc/news/news083005d.html).

Whenever drinking water systems are incapacitated, alternative supplies of water must be provided. Plans must be in place to provide clean and safe drinking water to customers. Until recently, contingency plans most commonly addressed drought and short-term disruptions. In consideration of the potential for long-term disruptions resulting from intentional attacks on water systems, contingency approaches for providing drinking water need to be reevaluated. Innovative approaches such as transportable or modular units that can treat water at different locations must also be considered. In fact, the Bioterrorism Act required a review of methods for providing alternative water supplies.

EPA has begun an evaluation of water supplies and delivery system alternatives for systems of various sizes and geographical areas, and will consider types of water sources, adjacent systems and interconnection, system redundancies, pressure sources, and portable capabilities. Such an evaluation has benefits that go beyond a terrorist attack. These benefits include improved preparedness for natural hazards (e.g. earthquakes, floods, and tornadoes) or accidents (e.g. line breaks and chemical tank failures). Contingency planning is nothing new. The Safe Drinking Water Act of 1974 required all water utilities to prepare contingency plans that would be implemented during an emergency. These plans have, however, been reevaluated with increased vigor as utilities were required to perform vulnerability assessments as part of the Bioterrorism Act of 2002.

The vulnerability assessments focused on seven water system components that might incapacitate the system. These include the water source, treatment facilities, transmission and distribution lines, storage facilities, water system personnel, records (plans and operating manuals), and indirect components (electric power, supplies and materials, communications including telemetry and facility and personnel security). Using the results of their vulnerability assessments, water utilities have begun to implement additional contingencies. Many have added system redundancies such as backup pumps and extra storage, and have defined emergency water sources and negotiated mutual aid agreements with neighboring utilities.

### 3.5 Targeting Impacts on Human Health and Informing the Public of Risks

An important component of a contingency plan is communication with mutual aid providers, government, and the public. Although there are many formulas for effective communication during a crisis, all require careful planning, thoughtful message preparation, simplicity, and accuracy. Working with communication experts, EPA evaluated several approaches for communication during crises and adopted a process called

*message mapping*. A message map is developed taking into account a number of factors. Most important is the recognition that under stress most people can comprehend and retain only a very few pieces of critical information.

A successful message map focuses on only three points and presents these points at a level of simplicity understandable to people with an education four grades lower than the target audience. Other important factors for inclusion in a successful message map are statements of compassion and optimism, citation of credible third parties, and truthful and accurate information. EPA has prepared numerous message maps for its own use in preparation for crises and has provided training to many of its partners on the techniques [9]. A report and video tutorial on the process of message mapping and examples of message maps can be found on the EPA website (http://www.epa.gov/nhsrc/news/news040207.html).

Despite the importance of planning, much of the information that will need to be communicated during a crisis is situation specific. During the emergency, quick and easy access to accurate information will be necessary. Some of this information pertains to the properties of the contaminants and their impact on human health and the environment. work is under way to better understand the contaminants of interest with respect to terrorist events, including defining levels of exposure to the contaminants below which there are no health concerns or at which the use of protective equipment is required (i.e. advisory levels). This information is very important to determine when evacuation is needed and when safe occupancy can be resumed.

Biological agents pose the greatest challenge, compared with chemical and radiological agents, in predicting health outcomes. Developing a scientifically acceptable method of performing microbial risk assessments (MRAs) is an EPA priority. In the past, MRAs have been addressed mostly by risk assessors trained to perform chemical risk assessments. Most MRAs to date have focused on the hazardous characteristics of the microbial agent with little appreciation for the complex interactions involving host susceptibility or the factors governing environmental exposure. Consequently, there is no consensus methodology to assess risks associated with microbial agents intentionally released into the environment (e.g. water, indoors and outdoors).

The unique challenge of assessing risks associated with exposure to pathogens is that microbial agents are capable of replicating and changing after being released. Adding to that complexity, homeland security experts are concerned that microbial agents may be genetically modified to enhance virulence or promote dissemination. These modifications could increase the harm to those exposed or increase the number of those exposed. The delivery concentration of these modified agents may also be higher than the dose normally received through natural transmission pathways (i.e. person-to-person and animal-to-person).

Although MRA is a fledgling science, strides are being made. Studies are under way to advance the science in the following key areas:

1. understanding the key properties related to microbe detection;
2. developing protocols for the design of novel and advanced sampling and analytical methods;
3. identifying and testing highly efficient biological aerosol sampling devices;
4. understanding genomic reengineering of characteristics such as virulence, detection capability, and antibiotic resistance;

5. understanding physical modifications of biological agents in aerosols to increase their airborne dispersion;
6. recognizing physiological and biochemical processes involving pathogenic-induced infectivity and disease; and
7. understanding the fate and persistence properties of biological agents in order to design decontamination protocols for cleanup and reentry into buildings and outdoor areas (Tonya Nichols, Ph.D., Personal Communication, 2007).

EPA is involved in studies to advance MRA in several important ways, including (i) physiological models development, (ii) bioaerosol studies, and (iii) pathogenicity assessments.

***3.5.1 Physiological Models.*** A scientifically credible risk assessment is dependent on accurate data and knowledge of how the microbes impact the human body at varying exposure levels (i.e. dose–response).

Since experimentation using human and animal subjects is necessarily highly restricted, models must be developed that can reasonably predict health outcomes. EPA has been involved with two model development efforts that are advancing the field of MRA:

*Physiological Assessment of Microbial Effects (PhAME) Workgroup*. The PhAME Workgroup is a multiagency team formed to develop innovative approaches to defining the exposure–dose–response continuum for inhaled microbial pathogens. Developing a method to establish advisory levels requires examining the available toxicological, infectivity, and virulence information on each biological threat agent, followed by a statistical analysis of the data. A comprehensive knowledge base is needed to structure the available data from human and animal exposures in order to permit more rigorous statistical analysis via a variety of commercially available analytical tools. To address this need, the PhAME Workgroup has been responsible for developing the pathogen information catalogue (PI Cat), which is a comprehensive knowledge base on dose assessment.

The PhAME Workgroup has been using this knowledge base and other government resources to develop physiologically based infectivity models that extrapolate information on contaminant effects to humans based on animal dose–response data. Data on particular species (e.g. guinea pigs, rats, and monkeys), which are housed in the PI Cat, can be used to determine survival curves. Physiologic extrapolation models (PEMs) can be designed to extrapolate survival curves from animals to humans (Tonya Nichols, Ph.D., Personal Communication, 2007).

*Physiologically Based Biokinetic (PBBK) Models*. PBBK models are being developed using the rabbit model. The model evaluates the fate of inhalational anthrax in the rabbit, by assessing the deposition of spores in the lung, germination of the spores, the spread of bacteria during disease, and the effect of immunization. The data can then be extrapolated to predict low-dose infectivity of anthrax in humans. This information will contribute to health and exposure assessments needed to derive cleanup goals.

***3.5.2 Bioaerosol Studies.*** Relatively little is known about how everyday activities could influence human exposure to biological contaminants. EPA is conducting targeted research that advances the knowledge and understanding of the fate and transport of microorganisms in air and water, and the potential risk to humans from exposure to

organisms released by various modes of delivery. EPA has identified and engaged organizations to collaborate in this effort. Understanding the behavior of biological agents in water-based aerosols, which could be created if water distribution systems become contaminated, has been an area of great interest to EPA and public health organizations.

Most aerosol research to date involves evaluating biological agents as inert particles. EPA's key contribution to this area has been to design and conduct experiments to not only determine the extent of biological contamination, but also assess the survivability of the agent being delivered through the aerosolization pathway. For example, if the agent does not survive aerosolization or the decay rate is known to be rapid, a decontamination or cleanup effort may not be necessary. To test survival and dissemination, agents have been grouped into representative classes as follows:

- naturally occurring waterborne agents;
- spores that are extremely hardy and environmentally persistent;
- vegetative bacterial cells, which are not normally environmentally persistent.

Biological contaminants in tap water may become aerosolized in droplet or vaporized form during use, thus creating three routes of potential entry into a susceptible host: inhalation, ingestion, and dermal exposure. In order to more reliably assess the risk of exposure to pathogens in these situations, studies are being conducted to better understand the dynamics of exposure to contaminated aerosol droplets and vapor, and in particular, the behavior and viability of pathogenic microorganisms contained in water droplets and vapor generated at varying water temperatures under varying environmental conditions.

In addition to influencing public health advisories, the information generated from these studies will impact how cleanup activities are conducted. For example, contaminated water could be aerosolized by decontamination activities (water spray), as well as by showering performed during personnel decontamination upon exiting the contaminated environment. Modifications to these practices will be necessary if it is determined that through aerosolization, these pathways spread contamination or increase human exposure to pathogens.

***3.5.3 Pathogenicity Assessments.*** In MRA, not only survivability and transport of biological agents are to be considered but pathogenicity, or the ability of a microbe to cause disease, must also be evaluated. Pathogenicity assessments are analogous to the better-understood hazard assessments for chemicals; however, they consider the many complexities associated with disease processes. For example, there is much interplay between the disease agent (strain specificity), the host immune response (susceptibility), and the exposure pathway (route of entry). Figure 1 depicts how biological and chemical risks are equated. EPA is developing a methodology for conducting pathogenicity assessment that involves a novel application of the epidemiological disease triangle. The disease triangle describes the interplay of three critical factors in the infectious disease process: (i) susceptible host, (ii) pathogen, and (iii) favorable environmental conditions.

Understanding the characteristics of the pathogen, particularly its virulence (i.e. relative ability of a microbe to cause disease) is a major goal of hazard characterization. Virulence factors, ranging from membrane structures to excreted toxins, provide a

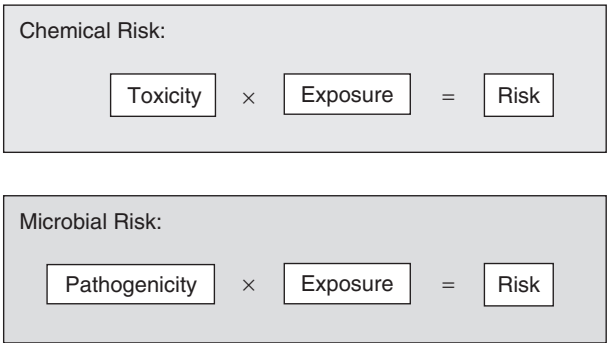



**FIGURE 1** Comparing biological and chemical risks from contaminants of interest.

biological agent with its pathogenic potential. EPA is compiling virulence factors for contaminants of interest. The data compilation effort includes

- associated microorganisms;
- genetic sequences;
- accessory factors (i.e. genes and/or proteins);
- environmental conditions for genetic expression;
- modes of action;
- structural analysis, when applicable;
- genetic recombination potentials;
- detection assays.

The pathogenicity assessment considers that virulence factors usually act in concert and that microbes exhibit adaptability to environmental pressures.

Accurate exposure pathway analysis is important to the pathogenicity assessment because microbial modes of action are dependent on the portal of entry into the host. For example, a traditional foodborne organism that causes a short-term gastrointestinal disease may be lethal if the organism gains entry to the bloodstream, via a break in the skin. It is also possible that an inhalational pathogen may not cause disease through an ingestion pathway. On the contrary, some pathogens cause disease no matter the portal of entry. *Bacillus anthracis*, for example, causes disease through all three exposure pathways: inhalational, gastrointestinal, and dermal anthrax. The pathogenicity assessment step evaluates the microbe's potential impact upon entry into each portal, which determines the significance of exposure pathways identified in the exposure assessment.

## 4 SHARING INFORMATION ON RESEARCH RESULTS

EPA's efforts to collaborate with its water sector partners means that frequent and effective communication is paramount to water sector security. Although easily accessible information must be available to sector partners, precautions must also be taken to ensure

that sensitive information on asset vulnerabilities and threat agents is not available for use by terrorists. There are many ways to share information on the results of data gathering and information development. Much of EPA's research results are provided using state-of-the-art information delivery techniques such as websites and electronic downloads. In some instances, the information developed is sensitive and can only be shared with a more limited set of customers or information users. The relatively small amount of information is shared in this fashion.

*The Water Information Sharing and Analysis Center (WaterISAC)* is a secure information system intended for use by drinking water and wastewater utilities. WaterISAC, managed by the Association of Metropolitan Water Agencies, was established to facilitate two-way communication between government agencies, law enforcement, research institutions, other ISACs, and the water utilities. It is specifically oriented to provide information on threat alerts and knowledge about threat agents and security systems. WaterISAC was established in response to PDD-63 and Executive Order 13231, which recommended that critical sectors establish information sharing and analysis centers. In addition to disseminating information, WaterISAC employs security analysts who scrutinize information for patterns, trends, and associations between seemingly unrelated events in order to provide early warning of potential dangers. This analysis provides a proactive and preventative element to water security [10].

Because WaterISAC is a privately established and operated venture, membership fees are required. Some smaller utilities experience difficulty in meeting the fee requirements of WaterISAC so, using a grant from EPA, WaterISAC established the Water Security Channel. Although password protected, the Security Channel does not have the highly sophisticated security of WaterISAC. It cannot provide all of the services and benefits of the ISAC, but it is free of charge and offers a library of federal advisories. WaterISAC and the Security Channel are instrumental in sharing information on a national level; however, more localized engagements are equally important. Regional, state, and local collaborations, consisting of organizations that will be required to work together during emergencies, can help promote an understanding of roles and responsibilities, and establish relationships that will help ensure effective response in times of emergency.

*Water Security Information Collaboratives* are groups of organizations and agencies formed to share information and address common issues regarding security. These collaboratives can take many forms, from ad hoc groups that meet only as needed to formal organizations complete with charters, mission statements, operating budgets, and regularly scheduled meetings. The principal benefit of a collaborative is enhanced drinking water and wastewater security and public health protection. Among the many other benefits, a collaborative provides is the opportunity for utility officials to develop working relationships with the people on whom they will rely during an emergency. Another benefit is the opportunity to share information from a variety of sources. For example, the water utility may subscribe to WaterISAC, from which it receives early warnings of potential threats, as well as information about security. State water regulatory agencies can provide expertise, resources, and information. Local law enforcement officials obtain updates from the Department of Homeland Security and regional offices of the Federal Bureau of Investigation (FBI). Public health agencies receive information from the CDC and are part of new disease surveillance programs being implemented around the country.

A focused effort to share information can ensure that utilities have a more comprehensive picture of the current security condition. Other benefits of collaboratives include the following:

- improved detection of, response to, and recovery from security crisis events;
- enhanced working knowledge and understanding of different professional disciplines;
- more effective use of different skills and resources;
- increased effectiveness in educating consumers and responding to questions from the media and public;
- improved intergovernmental communication;
- better understanding of various organizational perspectives and enhanced ability to resolve conflicts in a noncrisis environment;
- heightened sense of trust and community among organizations;
- identification and elimination of obstacles that prevent full cooperation;
- joint project development;
- increased efficiency through resource and information sharing;
- multiple communication links;
- enhanced problem-solving and team-building capabilities; and
- identification and coordination of interorganizational dependencies.

EPA has produced a guide to help the water sector establish security collaboratives. The guide includes case studies of three successful collaboratives [10].

## APPENDIX A: CONTAMINANTS OF INTEREST

A great deal can be done to prepare for intentional destructive acts against a drinking water or wastewater system without consideration of specific contaminants. Improved cyber and physical security and effective monitoring of general water quality all play a role in protecting water infrastructure. Following suspicion of tampering or an unexplained change in general water quality, a utility must quickly and confidently identify and characterize contaminants that may have entered the system. To successfully prepare for an intentional contamination event, utilities, researchers, responders, and public health professionals need to be knowledgeable of the range of contaminants that could be used to attack a drinking water or wastewater system.

Many organizations have compiled lists of the potential contaminants of interest that could damage drinking water or wastewater systems. These lists vary somewhat based on organizational responsibilities or interests, yet there are common contaminants among most of the lists. Contaminants of interest can be grouped into several categories: biological agents, chemical agents, toxic industrial chemicals, and radionuclides. This appendix provides a description of the contaminants of interest associated with water infrastructure.

## A.1 BIOLOGICAL CONTAMINANTS OF INTEREST

There are two primary types of biological agents that are contaminants of interest:

*Pathogens*, which may be bacteria, viruses, or protozoa, are replicating disease-causing organisms. Pathogens are infectious meaning that they will cause disease in a large number of exposed individuals. An example of a highly infectious pathogen is *B. anthracis*, the organism that causes the disease anthrax. Although highly infectious, *B. anthracis* is not communicable from human to human and is therefore not contagious. Pathogens capable of inflicting the greatest damage are both infectious and contagious. *Variola*, the pathogen that causes the disease smallpox, is both infectious and contagious.

*Biotoxins*, poisonous substances produced by living things, are common in nature. In many ways an attack using a biotoxin is more like a chemical attack than a biological attack, but because they are produced by living organisms, they are included in this section. Examples of biotoxins include venoms produced by insects and snakes. Biotoxins cause disease either on contact or by entering tissue and interacting with proteins. Reactions to biotoxins may be minor such as a bee sting or extremely lethal such as the reaction to ricin or botulism toxin.

A review by Burrows and Renner [11] discussed a variety of biological agents that might be used to intentionally contaminate water systems.

1. *Bacillus anthracis.* It is a spore-forming bacterium that causes the disease anthrax. The bacterium may occur in spore or vegetative form. Anthrax occurs in three forms: pulmonary, cutaneous, and intestinal. *B. anthracis* spores are very persistent and can survive in the environment for decades. While in its vegetative state *B. anthracis* is readily susceptible to inactivation by chlorine, the spore form requires exposure to 5–10% bleach or formaldehyde solution for inactivation. Although spores of *B. anthracis* may be physically removed from water through filtration systems capable of removing particles $<1\,\mu m$, significant hazards would be associated with handling of the contaminated filter components [11].
2. *Brucella melitensis and Brucella suis.* These are bacteria responsible for the disease brucellosis, which is highly infectious in cattle, pigs, and sheep. In humans, the infection is referred to as *Malta fever* or *undulant*. The illness is incapacitating, causing fever, aches, and pains, but the rate of fatality is relatively low. Brucellosis is known to have been contracted through the consumption of contaminated milk; thus, transmission through water is a concern. *B. suis* has been weaponized as an aerosol. *B. melitensis* is persistent in water for 20–72 days but can be inactivated by 1% sodium hypochlorite [11].
3. *Vibrio cholerae.* It is a bacterium, which causes acute, highly infectious cholera in humans and is transmitted through contaminated food or water. *V. cholerae* has been used throughout history to purposefully contaminate food and water. Symptoms of cholera are acute diarrhea resulting in dehydration. Without treatment, victims may die in a matter of hours of the onset of symptoms. *V. cholerae* may survive for weeks in water but is sensitive to heat, sunlight, and drying, and is easily killed by chlorine [11].
4. *Clostridium perfringens.* It is a common and highly persistent bacterium found in sewage. It causes food poisoning, which is associated with consumption of contaminated and undercooked meats. Symptoms include diarrhea, but unlike cholera, food poisoning is rarely fatal. *C. perfringens* is possibly transmissible through

water, which is of concern due to its insensitivity to chlorine. Aerosolization is another possible route of concern [11].

5. *Burkholderia mallei.* It is a bacterium that commonly results in the disease glanders in equines, although it can also occur in humans. The disease has not been seen in humans since 1945, but the bacteria are of concern for weaponization because it takes relatively few organisms to result in infection [12]. The symptoms of glanders depend upon the route of infection. The types of infection include localized, pus-forming cutaneous infections, pulmonary infections, bloodstream infections, and chronic suppurative infections of the skin. Generalized symptoms of glanders include fever, muscle aches, chest pain, muscle tightness, and headache. Additional symptoms have included excessive tearing of the eyes, light sensitivity, and diarrhea. Bloodstream infections can be fatal in a week to 10 days [12].
6. *Burkholderia pseudomallei.* This bacterium causes the disease melioidosis, which is clinically and pathologically similar to glanders, but the ecology and epidemiology of melioidosis are different. Melioidosis is predominately a disease of tropical climates, especially in Southeast Asia where it is endemic. The bacteria causing melioidosis are found in contaminated water and soil, and are spread to humans and animals through direct contact with the contaminated source. Glanders is contracted by humans from infected domestic animals [13].
7. *Yersinia pestis.* It is the bacterial cause of plague, a disease that has resulted in infamous devastation throughout history. Plague may occur in three forms: pneumonic plague, bubonic plague, and septicemic plague. Pneumonic plague can spread from person to person through the air. Bubonic plague is the most common form of plague. It occurs when an infected flea bites a person or when materials contaminated with *Y. pestis* enter through a break in a person's skin. Bubonic plague does not spread from person to person. Septicemic plague does not spread from person to person.[14]. *Y. pesitis* has been used in the intentional contamination of food and water sources. The bacteria can survive in water for several days. It is inactivated by heating to 55–72°C or by 1% sodium hypochlorite [11]. It could be killed after several hours of exposure to direct sunlight.
8. *Chlamydia psittaci.* It is a rickettsia bacterium that causes the disease psittacosis through inhalation of contaminated bird droppings. The disease results in pneumonia, with accompanying fever, chills, headache, muscle aches, and a dry cough [11]. Psittacosis is not transmissible from human to human. *C. psittaci* is stable in seawater up to 24 hours and thus may be able to survive in fresh water. It is inactivated by 1% sodium hypochlorite [11].
9. *Coxiella burnetii.* It is a rickettsia bacterium, which causes Q fever in humans. Q fever may be acute or chronic. Only about one-half of all people infected with *C. burnetii* have symptoms. Most acute cases of Q fever begin with sudden onset of one or more of the following: high fevers (up to 105°F), severe headache, fatigue, muscle pain, confusion, sore throat, chills, sweats, nonproductive cough, nausea, vomiting, diarrhea, abdominal pain, and chest pain. Fever usually lasts for one to two weeks. Weight loss can occur and persist for some time. Thirty to fifty percent of patients with a symptomatic infection will develop pneumonia. In addition, a majority of patients have abnormal results on liver function tests and some will develop hepatitis. In general, most patients will recover to good health

within several months without any treatment. Only 1–2% of people with acute Q fever die of the disease [15].

10. *Salmonella typhi.* This bacterium causes the life-threatening disease typhoid fever in humans. *S. typhi* infects only humans. Persons with typhoid fever carry the bacteria in their bloodstream and intestinal tract. In addition, a small number of persons, called *carriers*, recover from typhoid fever but continue to carry the bacteria. Both ill persons and carriers shed *S. typhi* in their feces [16].
11. *Shigella spp.* The Shigella bacterium causes dysentery, or shigellosis. It is characterized by diarrhea, abdominal pain, and bloody stools. The bacteria are transmitted through a fecal–oral route and are commonly seen in countries with poor sanitation. The disease is spread by those with active infections and by asymptomatic carriers. Shigellosis outbreaks are not uncommon, often associated with insufficiently treated recreational waters. *Shigella* are 99% inactivated by 0.05 mg/l chlorine and ultraviolet radiation [11].
12. *Francisella tularensis.* This bacterium causes the potentially serious disease tularemia. *F. tularensis* has been weaponized as an aerosol and is of concern as an agent for intentional contamination of water [11]. Symptoms may vary depending on the route of exposure but may include sudden fever, chills, headaches, diarrhea, muscle aches, joint pain, dry cough, pneumonia, ulcers, swollen glands, painful eyes, and progressive weakness. Tularemia is treatable with antibiotics [17]. *F. tularensis* is a hardy microbe that can thrive and multiply in water and mud. It is sensitive to heat but resistant to freezing. Studies on inactivation with chlorine have yielded mixed results [11].
13. *Rickettsia prowazekii.* It is a rickettsial bacterium, which causes epidemic typhus and Brill–Zinsser disease. Brill–Zinsser disease is a mild form of epidemic typhus. It occurs when the disease reactivates in a person who was previously infected. It is more common in the elderly [18]. *R. prowazekii* may be aerosolized, although there is no history of its use as a weapon or as an agent for intentional contamination of water supplies [11]. *R. prowazekii* is heat sensitive (50°C) and is inactivated by 1% sodium hypochlorite [11].
14. *Enteric viruses.* These are commonly transmitted by the fecal–oral route and although not documented as having been weaponized, they may be potable water threats. Symptoms of enteric viral infections include vomiting, abdominal distress, diarrhea, and dehydration. Fatality is rare among healthy adults. Enteric viruses may persist for 8–32 days in surface waters and >64 days in tap water. Enteric viruses are sensitive to chlorine and may be treatable through common municipal water treatment practices [11].
15. *Viral Hemorrhagic Fevers (VHF).* These result in a number of viral illnesses, including Ebola, Congo fever, Lassa fever, Marburg fever, and others that result from exposure to several different viral families. There is some evidence that these viruses have been weaponized, but no indication of intentional contamination of water sources has been documented [11]. Specific signs and symptoms vary by type of VHF, but initial signs and symptoms often include marked fever, fatigue, dizziness, muscle aches, loss of strength, and exhaustion. Patients with severe cases of VHF often show signs of bleeding under the skin, in internal organs, or from body orifices such as the mouth, eyes, or ears. Some types of VHF are associated

with renal (kidney) failure [19]. VHFs are sensitive to heat in excess of 56°C and are inactivated by UV light, 1–2% sodium hypochlorite, and/or 1% iodine [11].

16. *Variola major.* This is a viral disease more commonly known as *smallpox*. It is known to have been weaponized as an aerosol. Its use as an agent to contaminate water is not documented [11]. Before 1980, the smallpox vaccine was administered to the general public. Through the immunization program the disease was eradicated. Variola major virus supplies are now limited to research laboratories. It is unknown whether Variola virus is transmissible through water, but it can be inactivated by 1% sodium hypochlorite [11].
17. *Cryptosporidium parvum.* It is a protozoan, which is a common water contaminant associated with livestock waste. Although not previously used as a weapon, it is highly infectious, easily obtained, and readily transmissible in water and thus a concern for use as an agent of intentional contamination [11]. Crypto, as the illness is commonly called, is easily spread through the fecal–oral route. It is one of the most common waterborne illnesses associated with both contaminated drinking and recreational waters. The parasite lives in the host intestine and is discharged through the feces. A thick outer shell (oocyst) protects the protozoan and allows it to be persistent outside the host. Crypto can be transmitted by swallowing contaminated water or particles that have come into contact with contaminated surfaces. Crypto may be asymptomatic in some people, while others will suffer intestinal cramping, diarrhea, vomiting, fever, and aches. It is generally not fatal in healthy populations [20]. *C. parvum* oocysts are stable in water for days or more, but are heat sensitive and can be inactivated by boiling. The oocysts are highly resistant to chlorine-based disinfection and to chlorine dioxide. UV light systems of an advanced design have achieved $>4$ $\log_{10}$ inactivation of *C. parvum* oocysts. *Cryptosporidium* is an emerging pathogen for which disinfection regimens are still being developed [11].
18. *Aflatoxins.* These are naturally occurring biotoxins produced by many species of *Aspergillus*, a fungus, most notably *Aspergillus flavus* and *Aspergillus parasiticus*. Aflatoxins are toxic and carcinogenic. Aflatoxins have been weaponized although there is no documentation of their use as a water contaminant. Aflatoxins produce acute necrosis, cirrhosis, and carcinoma of the liver in a number of animal species. No animal species is resistant to the acute toxic effects of aflatoxins; hence, it is logical to assume that humans may be similarly affected. For most species, the lethal dose of aflatoxin ranges from 0.5 to 10 mg/kg body weight. The symptoms described are produced by an average intake of 2–6 mg/day of aflatoxins. Aflatoxins have limited water solubility and are probably heat stable. They are probably chlorine tolerant under normal disinfection conditions, but this needs to be determined [11].
19. *Cyanobacterial toxins (Microcystins, Anatoxin A).* These are powerful toxins produced during cyanobacterial blooms. Cyanobacteria have potential for weaponization through aerosolization but may also impact water supplies. The symptom of Anatoxin A poisoning is acute respiratory distress, whereas Microcystins are a liver toxin. These biotoxins are known, respectively, as the *fast* and *very fast death factors*. Alum flocculation, filtration, and chlorination are ineffective in the removal of cyanobacterial toxins, water purifiers containing carbon, ion exchange resin, and silver may be partially effective, whereas reverse osmosis was completely effective [11].

20. *Botulinum toxins.* These are produced by the bacteria *Clostridium botulinum*, which are commonly found in soils. Botulinium toxins have been weaponized as aerosols. Because of the quantities needed, it is unlikely that they would be used to contaminate a large water source, but they have potential to contaminated smaller supplies. The most common and lethal exposure route for botulinium toxin is ingestion, although dermal forms are on the rise due to intravenous drug use. Symptoms include double vision, blurred vision, drooping eyelids, slurred speech, difficult swallowing, dry mouth, and muscle weakness. If untreated, paralysis of the arms, legs, trunk, and respiratory muscles may occur. Death results from suffocation. Botulism toxins are inactivated by sunlight and exposure to air, heat, and chlorine. The toxins can be removed from water using reverse osmosis and possibly charcoal filtration [11].
21. *Ricin.* It is derived from castor beans and has been used throughout history as an assassin's poison. Ricin is easily produced in small quantities. Ricin poisoning can occur through inhalation, ingestion, or dermal contact, with inhalation and ingestion being the most serious. Inhalation results in severe respiratory distress, fever, and nausea. Ingestion results in vomiting, diarrhea, with possible liver, kidney, and spleen failure. There is no antitoxin for ricin [21]. Ricin can be inactivated by relatively high levels of chlorine (100 mg/l). It is removed from water by reverse osmosis and may possibly be removed by carbon filtration [11].
22. *Saxitoxin.* This toxin is the cause of paralytic shellfish poisoning and is produced by the marine dinoflagellate *Gonyaulax*, among others. Paralytic shellfish poisoning is typically encountered through ingestion of shellfish that have fed on *Gonyaula*, whose toxin accumulated in the fish. There is indication, however, that saxitoxins have also been isolated for use as an intentional poison. Saxitoxins are water soluble but can be inactivated by a strong chlorine solution (100 mg/l). Almost completely can be removed by reverse osmosis, whereas only partially removed by charcoal filtration [11].
23. *Staphylococcal enterotoxins.* These are toxins produced by bacteria such as *Staphylococcus aureus*. Staphylococcal enterotoxins have been weaponized and are of concern from both an ingestion and inhalation route. Ingestion results in gastrointestinal pain, vomiting, and diarrhea. Inhalation results in respiratory distress and fever. Poisoning is not fatal in healthy populations, but is incapacitating for a period of weeks. The toxin is heat sensitive and can be removed from water by carbon filtration [11].
24. *Mycotoxins: T-2.* It is isolated from cereal grains infected with the fungi *Fusarium*. Ingestion of mycotoxin could be life threatening. Unconfirmed and controversial findings suggest that mycotoxins were used as biological warfare agents in Laos, Cambodia, Afghanistan, and Iraq, thus weaponization is possible. Topical exposure causes blistering and skin necrosis. Sublethal effects of ingestion include lightheadedness, nausea, vomiting, and diarrhea.

    Mycotoxins are stable in water for a week, possibly longer, and are resistant to chlorine and iodine. The toxin is removed from water by reverse osmosis. Treatment by charcoal filtration should be effective [11].

## A.2 CHEMICAL AGENTS OF INTEREST

Included in this section is general information on chemical agents that have been used or considered for use in warfare. Chemical warfare agents are generally categorized into three groups: choking agents, nerve agents, and tissue-damaging (blistering) agents.

### A.2.1 Choking Agents

The most often considered choking agents are chlorine and phosgene. Exposure to these choking agents occurs most commonly through inhalation. The agents react with the water in the body to form hydrochloric acid: a strong acid that causes irritation and burning. Additional cell damage occurs through acylation of nucleophiles and lipid oxidation, by which free radicals "steal" electrons from the lipids (fats) in cell nucleus membranes. Chlorine reacts with water quickly, thus symptoms of chlorine exposure occur quickly. Phosgene reacts more slowly, thus symptoms could be delayed up to 48 hours. Symptoms of exposure to choking agents include

- coughing
- burning sensation in the throat and eyes
- watery eyes
- blurred vision
- difficulty breathing or shortness of breath
- nausea and vomiting.

Skin contact can result in lesions similar to those from frostbite or burns. Following exposure to high concentrations of phosgene, a person may develop fluid in the lungs (pulmonary edema) within 2–6 hours [22]. Phosgene has an odor similar to that of freshly mown hay and may be less noticeable or offensive, thus less likely to discourage consumption. Hydrolysis of phosgene, however, occurs quickly, thus it would not be a persistent contaminant in water [23].

### A.2.2 Nerve Agents

Nerve agents derive their name from their mode of action in the human body. They are organophosphorus compounds and are divided into two chemical families: the "G-agents" (e.g. tabun, sarin, and soman), named after the Germans who first created them, and the "V-agents", or venomous agents, (e.g. VA, VG, and VX). The V-agents were synthesized post-WWII, while the G-agents were manufactured during the war. Nerve agents can be dispersed as liquids or in aerosol form, allowing them to be inhaled, ingested, or absorbed through the skin. The most important chemical reactions involving nerve agents, particularly with respect to contaminated water treatment, take place directly at the phosphorus atom. The P–X bond is easily broken by nucleophilic reagents, such as water or hydroxyl ions (alkali). In aqueous solution at neutral pH, the nerve agents decompose slowly, whereas the reaction is greatly accelerated following the addition of alkali. The result is a nontoxic phosphoric acid.

The formation of the nontoxic phosphoric acid is also accelerated by a rise in temperature or by a catalyst (e.g. hypochlorite ions from bleaching powder). This hydrolysis forms the basis of most decontamination procedures using decomposition. In general, an area exposed to G-agents gets decontaminated through natural processes within a few days. However, V-agents may remain on the ground for several weeks because of their greater stability with respect to water and their much lower volatility. At pH levels between 7 and 10, VX is transformed into an extremely nonvolatile product of hydrolysis, which is incapable of penetrating skin [24].

### A.2.3 Blister Agents

Blister agents, or vesicants, are cytotoxic alkylating compounds. The most widely known of the blister agents is "mustard" or "mustard gas" (military designator: H). Other blister agents are sulfur mustard (HD), nitrogen mustard (HN), Lewisite (L), an arsenic containing vesicant, and phosgene oxime (CX). Phosgene oxime is a halogenated oxime with very different properties from those of the other agents.

**BOX A.1 EXAMPLES OF VESICANT OR BLISTER AGENTS WITH MILITARY DESIGNATORS IN PARENTHESES**

1. mustard or mustard gas (H);
2. sulfur mustard (HD), characterized by delayed action;
3. sulfur mustard with agent T (HT), the latter is bis-2-(2)-chloroethylthioethyl ether, similar to HD in structure;
4. nitrogen mustard (HN);
5. lewisite (L), similar to sulfur mustard in action, except immediate effects occur within minutes;
6. mixture of mustard and lewisite (HL), the combination of sulfur mustard (37%) with lewisite (63%) gives it a garlic odor;
7. phenyldichloroarsine (PD), like lewisite, is an organic dichloroarsine
8. phosgene oxime (CX), a pulmonary toxin with vesicant effects [25].

The mustard gases and lewisite are highly insoluble. Sulfur mustard quickly degrades to less toxic chemicals in agitated water [26], such as would occur in a distribution system. The rate of degradation of the mustard gases in water increases with heating. Similarly, degradation of nitrogen mustards in water with 90–95% hydrolysis is expected within 24 hours [27]. Although the persistence of lewisite in the environment is not well studied, it is known to lose its blistering properties in water. Phosgene oxime, unlike the other blister agents, is highly (70%) soluble in water. Although produced, it has never

been used in warfare, thus limited information is available. It is degraded by bacterial action in water over a few days [28].

## A.3 INDUSTRIAL CHEMICALS AND MATERIALS OF INTEREST

The following chemical information is from EPA's Planning for and Responding to Drinking Water Contamination Threats and Incidents [29]. The table includes information on chemical contaminants, both inorganic and organic, that potentially have an adverse impact if introduced into the drinking water supply. This is not an exhaustive list of chemicals, and there may be many others that could be used to contaminate a water supply. Additional information is provided for classes and/or constituents that may be of concern for terrorist use. These constituents are highlighted in Table A.1.

### A.3.1 Heavy Metals

Living organisms require trace amounts of some heavy metals, including iron, cobalt, copper, manganese, molybdenum, vanadium, strontium, and zinc, but excessive levels can be detrimental. Other heavy metals such as mercury, lead, and cadmium (with one exception for the latter) are toxic metals—they have no known vital or beneficial effect on organisms, and their accumulation over time in the bodies of mammals can cause serious illness. Toxic metals are metals that form poisonous soluble compounds and have no beneficial biological role. Often heavy metals are considered synonymous with toxic metals, but lighter metals also have toxicity. Toxic metals imitate the action of an essential element in the body, distorting the metabolic process to cause illness. The toxicity is a function of solubility, so that as insoluble salts or in the metallic form, toxic metals may have negligible toxicity [30]. Lead, osmium, and mercury are the toxic metals of greatest concern with respect to terrorist attacks. There are several methods for removing heavy metals from water:

- ion exchange
- specialized sorbents
- novel membranes
- precipitation
- electrokinetic processes
- phytoremediation [31].

### A.3.2 Arsenite Compounds

Arsenic (As) exists in the soil environment as arsenate, As(V), or as arsenite, As(III). Although arsenate is more common, arsenite is more toxic. Arsenite compounds are 4–10 times more soluble than arsenate compounds. Arsenic compounds occur in water as a result of both natural processes, such as weathering of arsenic minerals, and anthropogenic activities, including mining, industrial waste discharge, and application of arsenic herbicides and pesticides. Several treatment options are available for the removal of arsenic

**TABLE A.1 Chemical Contaminants, Their Availabilities, and Restrictions**

| Class | Examples (Not Exhaustive) | Sources | Limited Access? |
|---|---|---|---|
| | Inorganic chemical contaminants | | |
| Corrosives and caustics | Toilet bowl cleaners (hydrochloric acid), tree-root dissolvers (sulfuric acid), and drain cleaners (sodium hydroxide) | Retail and industry | No |
| Cyanide salts or cyanogenics | Sodium cyanide, potassium cyanide, amygdalin, cyanogen chloride, and ferricyanide salts | Supplier and industry (especially electroplating) | Yes |
| Metals | Mercury, lead, osmium, their salts, organic compounds, and complexes (even those of iron, cobalt, copper are toxic at high doses) | Industry, supplier, and laboratory | Yes[a] |
| Nonmetal oxyanions, organo-nonmetals | Arsenate, arsenite, selenite salts, organoarsenic, and organoselenium compounds | Some retail, industry, supplier, and laboratory | Yes[b] |
| | Organic chemical contaminants | | |
| Fluorinated organics | Sodium trifluoroacetate (a rat poison), fluoroalcohols, and fluorinated surfactants | Supplier, industry, and laboratory | Yes |
| Hydrocarbons and their oxygenated and/or halogenated derivatives | Paint thinners, gasoline, kerosene, ketones (e.g. methyl isobutyl ketone), alcohols (e.g. methanol), ethers (e.g. methyl *tert*-butyl ether, MTBE), and halohydrocarbons (e.g. dichloromethane, tetrachloroethene) | Retail, industry, laboratory, and supplier | No |
| Insecticides | Organophosphates (e.g. malathion), chlorinated organics (e.g. dichloro-diphenyl-trichloro-ethane (DDT)), carbamates (e.g. Aldicarb), and some alkaloids (e.g. nicotine) | Retail, industry, and supplier (varies with compound) | Yes |
| Malodorous, noxious, foul-tasting, and/or lachrymatory chemicals | Thiols (e.g. mercaptoacetic acid and mercaptoethanol), amines (e.g. cadaverine and putrescine), and inorganic esters (e.g. trimethylphosphite, dimethylsulfate, and acrolein) | Laboratory, supplier, police supply, and military depot | Yes |

| | | | |
|---|---|---|---|
| Organics, water-miscible | Acetone, methanol, ethylene glycol (antifreeze), phenols, and detergents | Retail, industry, supplier, and laboratory | No |
| Pesticides other than insecticides | Herbicides (e.g. chlorophenoxy or atrazine derivatives) and rodenticides (e.g. superwarfarins, zinc phosphide, $\alpha$-naphthyl thiourea) | Retail, industry, agriculture, and laboratory | Yes |
| Pharmaceuticals | Cardiac glycosides, some alkaloids (e.g. vincristine), antineoplastic chemotherapies (e.g. aminopterin), and anticoagulants (e.g. warfarin). Includes illicit drugs such as lysergic acid diethylamide (LSD), phencyclidine (PCP), and heroin | Laboratory, supplier, pharmacy, and some from a natural source | Yes |

[a]Availability may be commercially limited for the more toxic metals, especially the heavy metals, which can be quite expensive. Iron and copper are readily available, but not usually in soluble (bioavailable) forms.

[b]Availability of arsenicals and selenium compounds in the retail sector has been reduced owing to environmental regulations, but such products can occasionally be found as part of older inventories of merchandise, especially in small-town hardware stores. Supplies of such materials may generally be too small to cause concern.

from water: zero valent iron has been found to have the ability to simultaneously remove As(V) and As(III) compounds in water [32]. Dried water hyacinth plant roots prepared to a fine powder can remove more than 93% of As(III) and 95% of As(V) from a solution containing 200 μg of arsenic per litre within 60 minutes of exposure [33]. The use of titanium oxide ($TiO_2$) photocatalysis is attractive for the treatment of arsenic contaminated water [34].

### A.3.3 Carbamate and Organophosphate Pesticides

The word "organophosphates" (OPs) refers to a group of insecticides or nerve agents derived from phosphoric acid esters that act as inhibitors of the enzyme cholinesterase. The pesticide group carbamates (CMs) also act on this enzyme. CM and OP pesticides are widely used in homes, gardens, and agriculture. They are pesticides that can bind, or inhibit, acetylcholinesterase, making it unable to breakdown the neurotransmitter acetylcholine, resulting in paralysis and eventually death. Methods for removing OP and/or CM pesticides from water/ground water include the following:

- Bioremediation/biodegradation (live microbes—example carbofuran-metabolizing *Pseudomonas* sp.) [35].
- Enzymatic bioremediation (alternative to live microbes).
- Phytoremediation: for moderately water soluble organic contaminates, it may be possible to use plant species that can translocate and metabolize a contaminant within their shoots. For highly lipophilic compounds, a phytoremediation strategy would best focus on stimulation of biodegradation within the root zone of plants.
- Natural attenuation.
- Sulfuric acid treatment [36].
- High-performance liquid chromatography [37].

### A.3.4 Herbicides

Modern agriculture production practices rely heavily on the use of herbicides to control weed populations. Atrazine and simazine are widely used herbicides for the control of broadleaf weeds in corn, sorghum, sugarcane, and other crops. Because of their widespread use for over 50 years, these s-triazine herbicides are often detected in ground water, sediments, and soils at levels exceeding the maximal concentrations set by the EPA. Pesticides impact drinking water through leaching to ground water and discharge to surface water. Surface water discharge includes overland transport of storm water runoff and contributions from tile drains. Herbicides may be removed from water through the following treatment processes:

- bioremediation/biodegradation (live microbes/*in situ* treatment)
- carbon adsorption
- photodecomposition (sunlight breakdown) [38]

- air stripping
- reverse osmosis or ultrafiltration.

### A.3.5 Rodenticides

Rodenticides are a category of chemicals used in pest control intended to kill rodents. There are three common types of rodenticides: anticoagulants, metal phosphides, and hypercalcemia. Fatal internal bleeding is caused by doses of anticoagulants such as brodifacoum, coumatetralyl, and warfarin. Metal phosphides have been used as a means of killing rodents and are considered single-dose, fast-acting rodenticides (death occurs commonly within 1–3 days after single-bait ingestion). The acid in the digestive system of the rodent reacts with the phosphide to generate the toxic phosphine gas. Hypercalcemia such as calciferols (vitamins D), cholecalciferol (vitamin $D_3$), and ergocalciferol (vitamin $D_2$) are used as rodenticides. They are toxic to rodents and if the dose of the toxin is high enough, it leads to death. Treatment methods of rodenticides typically include

- bioremediation/biodegradation (live microbes/*in situ* treatment) [39]
- carbon adsorption
- air stripping
- reverse osmosis or ultrafiltration.

## A.4 RADIOACTIVE CONTAMINANTS OF INTEREST

Terrorist organizations may use radioactive substances in a number of ways, as part of radiological dispersion devices (RDD) and improvised nuclear devices (IND) radioactive substances may also be directly injected into a water supply. Of these modes of attack, the IND has the potential to result in the most destruction. An IND requires nuclear material such as highly enriched uranium or plutonium and through detonation causes an explosive chain reaction. An RDD, by contrast, does not result in the generation of radiation but disperses radiological particles. Most damage would result from the initial blast; however, radiological particles could contaminate buildings, outdoor areas, and water supplies. An RDD attack is considered more probable than an IND attack because little technical knowledge is needed to construct the devices and the materials are more readily available. The probability of direct injection of radionuclides into water supplies is low due to the relative difficulty in obtaining radiological agents compared with chemical or biological agents. There are, however, some radionuclides that are toxic in very low doses and are therefore discussed in this article.

### A.4.1 Cesium 137

It is produced when uranium or plutonium absorbs neutrons and undergoes fission. Examples of the uses of the fission process are nuclear reactors and nuclear weapons. The

splitting of uranium and plutonium atoms creates numerous fission products. Cesium-137 is one of the more well known of these products [40]. As cesium-137 undergoes radioactive decay, both $\beta$ particles and $\gamma$ rays are emitted. Cesium-137 decays to barium-137, a short-lived decay product, which in turn decays to a nonradioactive form of barium. The major radiation dose, which associates with cesium-137, is actually from the barium-137. The half-life of cesium-137 is 30.17 years. Cesium is soluble and moves easily through the environment. Its persistence and solubility makes the cleanup of cesium-137 difficult [40].

### A.4.2 Strontium 90

It is another radioactive product of nuclear fission. It has a half-life of 29 years and thus will persist in the environment. It is mobile in the environment and is therefore a potential threat in water. Strontium-90 decays to yttrium-90, emitting $\beta$ particles in the process. Unlike $\gamma$ rays, which can easily penetrate the body, $\beta$ particles are significantly blocked by the dermis and therefore present the greatest risk to health when ingested or inhaled. Ingestion is the most common route of exposure to Strontium-90. In the body, Strontium-90 behaves much like calcium, concentrating in bone and bone marrow. Bone tumors and tumors of the blood-cell forming organs are the main health concern. These tumors result from exposure to the $\beta$ particles emitted during the radioactive decay of strontium-90 and yttrium-90 [41].

## REFERENCES

1. Presidential Decision Directive/PDD-63 (1998). *Critical Infrastructure Protection*, May 22, http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, 2008.
2. U.S. Environmental Protection Agency (2007). *Public Drinking Water Systems Programs.* http://www.epa.gov/safewater/pws/index.html, 2008.
3. National Drinking Water Advisory Council (NDWAC) (2005). *Recommendations of the National Drinking Water Advisory Council to the U.S. Environmental Protection Agency on Water Security Practices, Incentives, and Measures*. http://www.epa.gov/ogwdw/ndwac/pdfs/wswg/wswg_report_final_july2005.pdf, 2008.
4. Homeland Security Presidential Directive/HSPD-7 (2003). *Critical Infrastructure Identification, Prioritization, and Protection*. http://www.fas.org/irp/offdocs/pdd39.htm, 2008.
5. U.S. Environmental Protection Agency (2007). *Water: Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*. http://www.dhs.gov/xlibrary/assets/nipp-ssp-water.pdf, 2008.
6. U.S. Environmental Protection Agency (2004). *Water Security Research and Technical Support Action Plan.* EPA/600/R-04/063. http://www.epa.gov/NHSRC/pubs/600r04063.pdf, 2008.
7. U.S. Environmental Protection Agency (2007). *Energy and Water Distribution Interdependency Issues: Best Practices and Lessons Learned (Summary Report of the 2005 Energy and Water Distribution Exercise)*. EPA 600/R-07/042. http://www.epa.gov/NHSRC/pubs/600r07042.pdf, 2008.

8. U.S. Environmental Protection Agency (2008). *Standardized Analytical Methods for Environmental Restoration Following Homeland Security Events—Revision 4.* http://www.epa.gov/nhsrc/pubs/600r04126d.pdf, 2008.
9. U.S. Environmental Protection Agency (2007) *Effective Risk and Crisis Communication During Water Security Emergencies: Summary Report of EPA Sponsored Message Mapping Workshops*. EPA/600/R-07/027. Held in: Atlanta, GA, March 2–3, 2005; Washington, DC August 17–19, 2005; Alexandria, VA February 14–15, 2006. http://www.epa.gov/NHSRC/pubs/600r07027.pdf, 2008.
10. U.S. Environmental Protection Agency (2005). *Security Information Collaboratives: A Guide for Water Utilities.* EPA/625/R-05/002. http://www.epa.gov/NHSRC/pubs/625r05002.pdf, 2008.
11. Burrows, W. D. and Renner, S. E. (1999). Biological warfare agents as threats to potable water. *Environ. Health Perspect*. **107**: 975–984. http://www.ehponline.org/members/1999/107p975-984burrows/burrows-full.html, 2008.
12. Centers for Disease Control and Prevention, Division of Foodborne, Bacterial and Mycotic Diseases (2008). *Glanders (Burkholderia mallei)).* http://www.cdc.gov/nczved/dfbmd/disease_listing/glanders_gi.html, 2008.
13. Centers for Disease Control and Prevention, Division of Foodborne, Bacterial and Mycotic Diseases (2008). *Melioidosis*. http://www.cdc.gov/nczved/dfbmd/disease_listing/melioidosis_gi.html, 2008.
14. Centers for Disease Control and Prevention, Division of Vector-Borne Infectious Diseases. (2007). *CDC Plague Home Page.* http://www.cdc.gov/ncidod/dvbid/plague/, 2008.
15. Centers for Disease Control and Prevention, Division of Viral and Rickettsial Diseases (2003). *Q Fever.* http://www.cdc.gov/ncidod/dvrd/qfever, 2008.
16. Centers for Disease Control and Prevention, Division of Foodborne, Bacterial and Mycotic Diseases (2005). *Typhoid Fever.* http://www.cdc.gov/ncidod/dbmd/diseaseinfo/typhoidfever_g.htm, 2008.
17. Centers for Disease Control and Prevention, Division of Foodborne, Bacterial and Mycotic Diseases (2003). *Tularemia.* http://www.bt.cdc.gov/agent/tularemia/pdf/tularemiafacts.pdf, 2008.
18. Centers for Disease Control and Prevention, Division of Vector-Borne Infectious Diseases (2005). *Rocky Mountain Spotted Fever.* http://www.cdc.gov/ncidod/dvrd/rmsf/index.htm, 2008.
19. Centers for Disease Control and Prevention, Special Pathogens Branch (2004). *Viral Hemorrhagic Fevers.* http://www.cdc.gov/ncidod/dvrd/spb/mnpages/dispages/Fact_Sheets/Viral_Hemorrhagic_Fevers_Fact_Sheet.pdf, 2008.
20. Centers for Disease Control and Prevention, Division of Foodborne, Bacterial and Mycotic Diseases. (2008) *"Crypto"—Cryptosporidiosis.* http://www.cdc.gov/crypto, 2008.
21. Centers for Disease Control and Prevention, Emergency Preparedness and Response (2008). *Facts About Ricin*. http://www.bt.cdc.gov/agent/ricin/pdf/ricinfacts.pdf, 2008.
22. Centers for Disease Control and Prevention, Emergency Preparedness and Response (2005). *Facts About Phosgene.* http://www.bt.cdc.gov/agent/phosgene/basics/pdf/phosgene-facts.pdf, 2008.
23. Livingston, J., Soilleux, R. J., and Doust, C. E. (2007). *Investigation into the Fate of Phosgene Contained Within Chemical Munitions Dumped Into Beaufort's Dyke.* DSTL/TR23848. Defense Science and Technology Laboratory, Porton Down, Salisbury, Wiltshire, UK. http://www.dstl.gov.uk/conferences/cwd/2007/pres/eddy-doust.pdf, 2008.

24. Swedish National Defense Research Establishment (1992). *FOA Briefing Book on Chemical Weapons.* Stockholm, Sweden. Information available from the Organization for the Prohibition of Chemical Weapons. http://www.opcw.org/resp/html/nerve.html, 2008.

25. Centers for Disease Control and Prevention, Emergency Preparedness and Response (2005). *Vesicant/Blister Agent Poisoning.* http://www.bt.cdc.gov/agent/vesicants/pdf/vesicant-tsd.pdf, 2008.

26. Public Health Service, Agency for Toxic Substances and Disease Registry (ATSDR) (2007). http://www.atsdr.cdc.gov/toxprofiles/phs49.html#bookmark02, 2008.

27. Public Health Service, Agency for Toxic Substances and Disease Registry (ATSDR) (2003). http://www.bt.cdc.gov/agent/nitrogenmustard/erc555-77-1.asp, 2008.

28. Public Health Service, Agency for Toxic Substances and Disease Registry (ATSDR) (2008). http://www.atsdr.cdc.gov/tfacts167.html, 2008.

29. U.S. Environmental Protection Agency (2003). *Planning for and Responding to Drinking Water Contamination Threats and Incidents Response Protocol Toolbox Module 1: Water Utility Planning Guide.* http://www.epa.gov/ogwdw/watersecurity/pubs/guide_response_module1.pdf, 2008.

30. Dartmouth Toxic Metals Research Program (2008). http://www.dartmouth.edu/~toxmetal/TX.shtml, 2008.

31. SenGupta, A. K. (2002). *Environmental Separation of Heavy Metals: Engineered Processes.* http://www.amazon.com/gp/reader/1566768845/ref=sib dp pt/105-0102840-4165235#readerlink, 2008.

32. Sun, H., Wang, L., Zhang, R., Sui, J., and Xu, G. (2006). Treatment of groundwater polluted by arsenic compounds by zero valent iron. *J. Hazard. Mater.* **129**(1–3), 297–303.

33. Al Rmalli, S. W., Harrington, C. F., Ayub, M., and Haris, P. I. (2005). A biomaterial based approach for arsenic removal from water. *J. Environ. Monit.* **7**, 279–282.

34. Xu, T. and O'Shea, K. E. (2005). Mechanistic evaluation of $TiO_2$ photocatalytic oxidation of arsenite. *J. Phys. Chem. A.* **109**(40), 9070–9075. http://pubs.acs.org/cgi-bin/abstract.cgi/jpcafh/2005/109/i40/abs/jp054021x.html, 2008.

35. Chaudry, G. R. and Wheeler, W. B. (1988). Biodegradation of carbamates. *Water Sci. Technol.* **20**(11-12). http://md1.csa.com/partners/viewrecord.php?requester=gs&collection=ENV&recid=1971837&q=groundwater+treatment+carbamates&uid=791441435&setcookie=yes, 2008.

36. Yoon, H. R., Lee, E. J., Park, M. K., and Park, J. H. (1998). Sulfuric acid pretreatment for the simultaneous GC screening of organochlorine and organophosphorus pesticides in herbal essential oils. *Chromatographia* **47**(9-10), 587–592. http://www.springerlink.com/content/ek8m444258u82562, 2008.

37. de Kok, A., Hiemstra, M., and Vreeker, C. P. (1987). Improved cleanup method for the multiresidue analysis of N-methylcarbamates in grains, fruits and vegetables by means of HPLC with post column reaction and fluorescence detection. *Chromatographia* **24**(1), 496–476. http://www.springerlink.com/content/l368416715436j70, 2008.

38. Nyer, E. K. (1993). *Practical Techniques for Groundwater and Soil Remediation,* CRC Press, Boca Raton.

39. Painter, J. A., Molbak, K., Sonne-Hansen, J., Barrett, T., Wells, J. G., and Tauxe, R. V. (2004). *Salmonella*-based Rodenticides and Public Health. *Emerg. Infect. Dis.* **10**(6), 977–1186. http://www.cdc.gov/ncidod/eid/vol10no6/pdfs/Vol10No6.pdf, 2008.

40. U.S. Environmental Protection Agency (2008). *Radiation Protection: Cesium*. http://www.epa.gov/rpdweb00/radionuclides/cesium.html, 2008.

41. Argonne National Laboratory (2006). *Human Health Fact Sheet*. http://www.ead.anl.gov/pub/doc/Strontium.pdf, 2008.

# DRINKING WATER SUPPLY, TREATMENT, AND DISTRIBUTION PRACTICE IN THE UNITED STATES*

YAKIR J. HASIT
*CH2M HILL, Philadelphia, Pennsylvania*
FORREST GIST
*CH2M HILL, Portland, Oregon*
REX HESNER
*CH2M HILL, Oakland, California*
KEN THOMPSON
*CH2M HILL, Englewood, Colorado*

## 1 RISK MITIGATION

To mitigate risks, United States (US) water systems typically use one or more of the following general approaches:

- adding physical protection systems (PPSs), equipment, or hardware;
- developing security policies/procedures;
- modifying management and staffing practices.

If utilities cannot mitigate risks through one or more of these means, then the other options they have used are to accept the risk as a cost of doing business or to reduce the risk by buying insurance.

## 2 PHYSICAL PROTECTION SYSTEMS

PPSs have included perimeter hardening improvements, such as fences or gates, and electronic security systems, such as card access or camera surveillance systems. However, not all security systems that have been installed have been effective. An effective PPS must include elements of deterrence, detection/assessment, delay, and response. These elements are described below.

*This article gives an overview of current security practices observed at public water systems in the United States. It covers risk mitigation, cyber security and contamination warning systems.

### 2.1 Deterrence

Deterrence is the capability to discourage an adversary from attempting to perform a malevolent act against a facility. Deterrence can be accomplished in one or more ways, including:

- well-maintained fencing or walls that present an imposing presence;
- presence of signage that indicates prosecution if trespassing occurs;
- good lighting;
- visual observation by persons or passing vehicles;
- high visibility of security guards.

Deterrence is difficult to quantify for high consequence, low frequency events such as a major bomb attack or large scale assault. It may be impossible to determine if the absence of a major attack is because of the deterrent effect of an effective PPS or whether no adversary would contemplate an attack even if a facility had been left completely unprotected.

### 2.2 Detection/Assessment

In the event that an adversary is not deterred and does attempt to enter a facility to carry out theft, sabotage, or other malicious activity, the next best option for the PPS is to defeat the adversary's attempt. This requires the detection of the intrusion attempt and holding back the intruder while there is still sufficient time to take an appropriate response. For high consequence events, an appropriate response requires the arrival of law enforcement personnel capable of stopping the adversary before the adversary has completed the malevolent act. In the case of low consequence events such as minor theft or vandalism, it may be adequate to allow the malevolent act to occur as long as the system obtains a video record of sufficient quality to allow subsequent identification and prosecution of the criminal.

*2.2.1 Detection/Assessment Systems.* The first line of defense is the discovery of an adversary attack. This involves the following events depicted in Figure 1:

- An abnormal occurrence is detected (through either a sensor or personnel) and an alarm is initiated.
- The sensor and assessment subsystems report and display information.
- Someone assesses this information and determines whether the alarm is valid.

An effective assessment system provides two types of information associated with detection: (i) whether the alarm is a valid or a nuisance alarm and (ii) the cause of the


**FIGURE 1** Detection sequence diagram.

alarm (that is, what, who, where, how many) so that the appropriate response may be initiated.

The effectiveness of the detection function is measured by the probability of sensing adversary action and the time required for reporting and assessing the alarm.

Examples of detection and assessment system components used by US water systems include the following:

- *Observation by personnel*, including neighbors, staff workforce, or security guards/law enforcement personnel.
- *Intrusion detection sensors*, such as fence disturbance, door position, glass-breakage, buried line, microwave, active-and-passive infrared, and video motion analytic systems.
- *Timely assessment*, preferably using closed-circuit television (CCTV) with instant playback of pre- and post-alarm images of the area associated with the intrusion alarm. Personnel may also be used for assessment, but that option is frequently much more expensive to provide reliable timely detection on par with CCTV.
- *Access control* using photo badges, card readers, personal identification numbers (PINs), and possibly biometrics such as a hand-geometry reading. The entry points used by the workforce represent places where an adversary could gain entry, bypassing the other elements of the PPS detection system; the ability of the access control system to identify unauthorized entry attempts is a component of the detection and assessment system.

***2.2.2 Delay Systems.*** Delay is the function of slowing the adversary on his or her way to the target. It is important to note that delay devices placed before any opportunity for detection are of little value. An intruder not faced with detection has all the time required to climb a fence or cut a lock. When the penetration has been detected and a response initiated, any delay facing the adversary gives the response force more time to successfully interrupt the threat.

Following are examples of delay system components used by US water systems:

- *Locks*, which must be shielded so that they cannot be easily defeated. This includes strengthening of door jambs to prevent mechanical spreading, and placement of metal guards to prevent prying of the latch.
- *Long distances* to be traversed, especially if traversing must be accomplished without a vehicle.
- *Barriers* of various types such as fences, walls, doors, and sturdy metal screens over windows.
- *Activated delays* such as pop-up vehicle barriers, automated lockdown of doors, and smoke or aqueous foam dispensers.

***2.2.3 Response Systems.*** Response is the time required by the security force (e.g., police or other law enforcement officers) to prevent adversarial success. Response includes both interrupting and stopping the adversary. The measure of response effectiveness is the time between receiving a communication of adversarial action and interrupting it with sufficient capability to stop the adversary. The effectiveness measures include the probability of accurate communication, the time required to communicate,

and the response force engagement effectiveness. An effective security system must be able to detect the adversary early enough that the adversary has not had time to cause the undesired event, delay the adversary long enough for the response to arrive, and stop the adversary before his or her mission is accomplished. If the design basis threat (DBT) includes a potential terrorist threat, any response force must be armed and have sufficient numbers to have a capability to stop the threat. DBT is defined as the adversary against which a utility must be protected. Determining the DBT requires consideration of the threat type, tactics, mode of operations, capabilities, threat level, and likelihood of occurrence. (*Source: ASCE/AWWA Draft American National Standard for Trial Use, Guidelines for the Physical Security of Water Utilities, December 2006).*

The PPS must perform the functions of detection, delay, and response in a period of time that is less than the time required for an adversary to complete his or her tasks. This relationship is shown in Figure 2. Security master plans developed for US utilities typically utilize the analysis described below.

As seen on this diagram, the adversary faces certain tasks (which equate to time) to get to the target area. In this example, the adversary must climb a fence, run to the transformers, open the drain valves, set the ignition sources, and leave before the fires occur. This total time is shown as the "adversary task time."

The "system delay" is the total delay time that the present security system provides from the time of first detection. "PPS time required" is the total time that the present system provides for detection, assessment, and response.

Because the system delay after detection time is greater than the time required to detect and respond to the intrusion, the PPS will be successful in interrupting the adversary.

Figure 3 shows what would happen if the first detection opportunity (perhaps a fence motion sensor) were moved to the transformer area. The adversary has a reduced remaining task time because he or she has already climbed the utility area fence before detection. Because the first alarm is now at the transformer area and the time required for detection and response will remain the same, the two boxes representing these functions must be

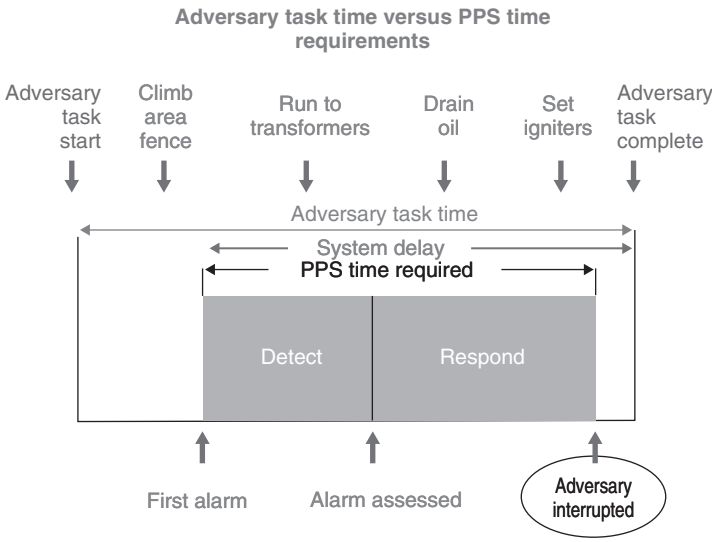



**FIGURE 2** Adversary task time versus PPS time requirements for a successful PPS.

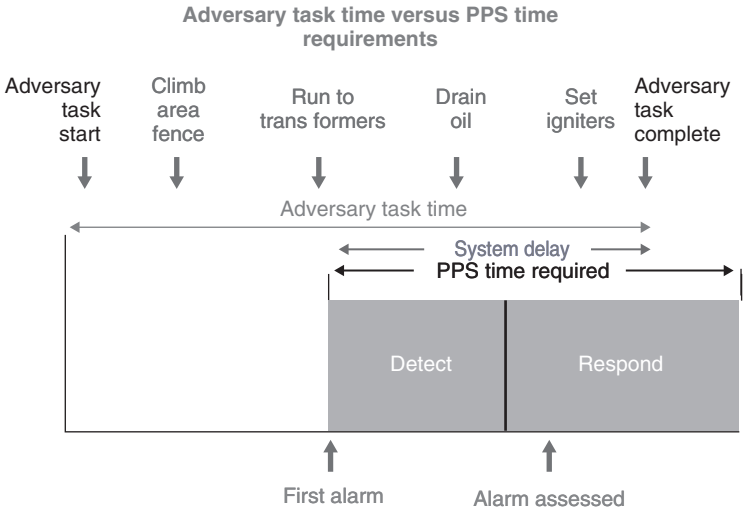



**FIGURE 3** Adversary task time versus PPS time requirements for an unsuccessful PPS.

shifted to the right on the timeline as shown. The PPS is now ineffective against the same adversary, because the adversary completes the effort before the response.

## 3 METHODOLOGIES FOR IDENTIFYING PHYSICAL PROTECTION SYSTEMS

To effectively identify appropriate physical protection measures and systems, a systematic methodology is necessary. Because it is rarely feasible to provide all assets or facilities with the same level of protection, it is necessary to identify those assets that are critical for the system to continue functioning and then prioritize security upgrades and/or modify policies and operational procedures to mitigate identified risks. This way, a balanced security program can be developed with the most appropriate resources allocated where they are most needed.

### 3.1 American Society for Industrial Security

The American Society of Industrial Security (ASIS) has developed the following methodology for identifying and evaluating PPSs, illustrated in Figure 4. This approach is used in security master plans developed for some US water utilities.

1. *Identify assets.* Determine the groups, core business organizations, equipment, buildings, vehicles, or other assets at risk.
2. *Specify loss events.* Identify loss events or vulnerabilities. These might include damage or destruction of equipment, harm or assault to employees, etc.
3. *Frequency of events.* Review and determine the probability of loss risk and frequency of events based upon consideration of prior incidents, trends, warnings, etc.

4. *Impact of events.* Evaluate the costs associated with the loss of tangible (direct costs, such as financial) or intangible (indirect costs, such as psychological) assets of an organization.
5. *Options to mitigate.* Identify options available to prevent or reduce losses through security improvements, such as hardware, procedures, and policies.
6. *Feasibility of options.* Study the feasibility of implementing mitigation options that do not interfere with the key operations or profits of the business.
7. *Cost/benefit analysis.* Identify costs associated with the suggested mitigation options.

## 3.2 Additional Recommendations

***3.2.1 Start from Inside and Work Out.*** In addition to the ASIS methodology presented in Figure 4, CH2M HILL recommends that, when identifying potential delay measures for physical protection, utilities should begin at the interior of the facility at the critical assets and work outwards. Delay measures such as hardened walls, locks and barriers can be enhanced protection at a reduced cost if they are close to the asset being protected. For example, if an asset such as a generator needs to be protected from damage, it is more cost effective to provide protective fencing around the asset (the generator) instead of fencing an entire site.

***3.2.2 Balanced Layered Security.*** The most critical assets should be identified, and if possible, located or moved to the center core of the facility, with concentric rings

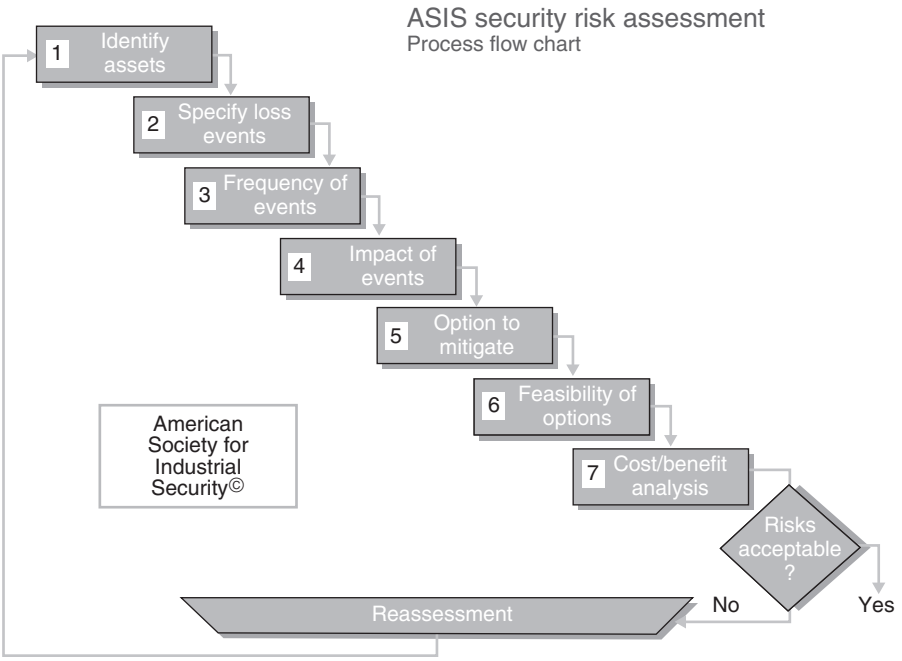



**FIGURE 4** ASIS general security risk assessment methodology. (Source: General Security Risk Assessment Guideline, 2003, American Society for Industrial Security.)

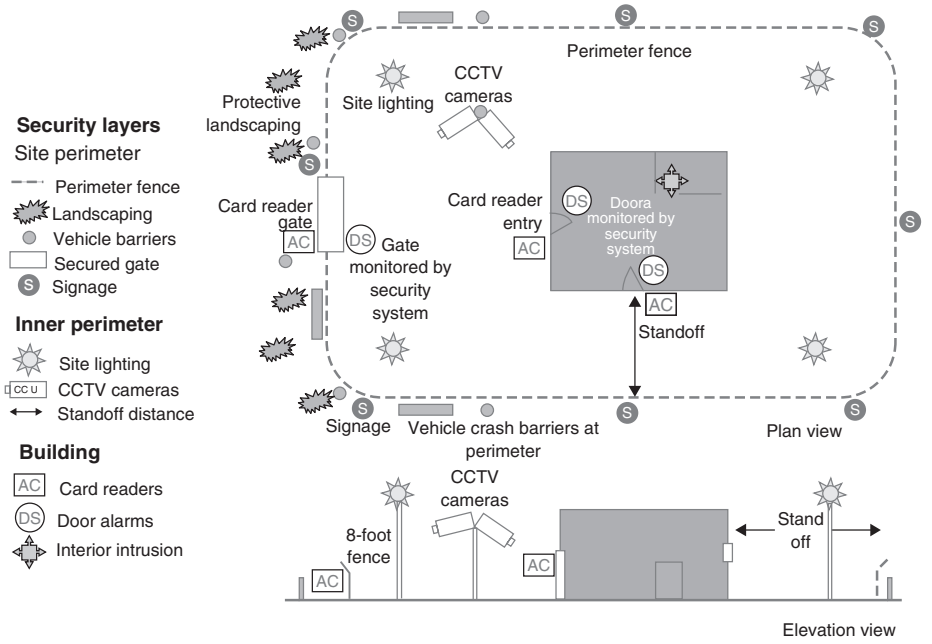



**FIGURE 5** Sample layered security recommendations for a facility.

of security protection provided around the asset as shown in Figure 5. Multiple layers of security will necessitate that the adversary must defeat each of these layers in order to carry out a successful attack. The use of multiple barriers requires more extensive preparation by the adversary and transportation of more breaching equipment, creates adversary uncertainty, and provides multiple opportunities for the adversary to fail in a successful breaching attempt.

### *3.2.3 Other Suggested Recommendations.*

- Utilities should implement a security procedure to identify when keys are not returned. This should include a policy to receive reports of lost keys on a regular basis and assess whether the locks should be re-keyed as a result of lost or stolen keys. Also, the work of security staff and lock technicians needs to be coordinated.
- In the case of an employee quitting or being terminated for cause, the vulnerability becomes higher and the utility should have a procedure in place to automatically secure facilities from access by this employee.
- Utility vehicles should be locked at all times, with keys removed from the vehicle and stored in a secure location. At service centers, the keys should be stored within the building and a sign-out procedure for vehicles should be implemented.
- Utilities should explore using shackle protection of their padlocks or consider hardening the padlock entry hinge. With time, an adversary could defeat the padlock system; hardening or protecting the padlock shackle will add more delay to the gate areas.

- Utilities should develop a policy for re-keying facilities on a regular periodic basis, such as every 5 years, or when a significant security breach or event occurs. To the broadest extent feasible, an electronic key system such as a card key or a pin-key product should be implemented.
- A corporate policy for dealing with temporary and contractor badges should be developed and adopted. The policy should include provisions for auto-expiration of visitor/contractor badges, limited access areas at facilities, limited available access time periods, and a requirement for mandatory two-person entry at critical areas. System auditing should be done on a periodic basis to identify outdated or missing temporary badges within the system.
- Utilities should develop a methodology for generating a variety of standard reports, including
  - card holders granted access through specified doors;
  - card holders attempting entry into unauthorized areas;
  - actions taken to acknowledge security alarms.
- Automatic reports should be defined and produced on a weekly basis for management review. Most card reader systems allow customized reports that can be automatically generated at scheduled intervals. These reports allow attempted breaches of security or other incidents be investigated properly and quickly.
- Some means of accurate intrusion detection, coupled with video assessment, should be provided at all critical facilities.
- It is critical that all perimeter doors be monitored for door forced-open alarm conditions. Balanced magnetic door contact switches interconnected to an intrusion alarm panel or to a monitoring system is a recommendation for all perimeter doors.

## 4 CYBER SECURITY

Cyber security is the protection of enterprise information systems from outside or inside attack. The reliance of a water utility on its automated systems can be substantial: the supervisory control and data acquisition (SCADA) system runs the plant, the financial system maintains fiscal equilibrium, and several other systems facilitate most business processes. In short, if the information systems do not work, the enterprise will not operate.

### 4.1 Cyber Security Vulnerabilities and Consequences

US water utilities have been vulnerable to cyber attacks from many points of entry. Gaining unauthorized entrance to an organization's information infrastructure is no longer the province of a small cadre of skilled intruders. The specific vulnerabilities of widely used platforms, like Microsoft Windows, are detailed on any number of websites. Inexpensive computers, anonymous Internet accessibility, and readily available hacking tools offer political and criminal organizations a potent tactical weapon.

The consequences of a compromised information system can have catastrophic repercussions to a utility. A penetrated financial system can result in lost revenue or stolen identity information from ratepayers, a sabotaged website has the potential to shake public trust, or interruption of the plant process because of SCADA malfunction can lead to service interruptions or water quality issues for the community. Effective cyber security

requires a balanced, planned approach that imposes standards across a broad range of technologies and personnel management.

### 4.2 Cyber Security Threats

There is no shortage of potential intruders to the enterprise from the Internet. For the purposes of the following cyber security discussions, intruders that have targeted water utility systems are as follows:

- *Outside attackers.* The primary goal of this group is unauthorized entry; their motivation is thrill-seeking, criminal opportunity, or political goals.
- *Inside attackers.* The primary goal of an inside attacker is to disrupt enterprise operations; their motivation is personal gain or vengeance.

The primary defense against outside attackers is both a robust anti-intrusion system, and security training for employees. A classic "low-tech" intrusion tactic called *social engineering*, where outsiders trick employees into revealing their user names and passwords over the telephone. The most effective deterrence against insider attack is a clearly articulated security policy, accompanying procedures, and noncompliance consequences.

### 4.3 Deterring Cyber Attack from the Outside

Cyber security addresses the need to ensure continuous functioning of the information systems serving the utility. Of special concern to water utilities is the SCADA system, whose distributed components autonomously maintain continuous operation of the various processes. Figure 6 gives an overview of the multiple vulnerability points of a typical SCADA system.

Cyber intruders have gained access to an enterprise network via one of three broad avenues:

- Internet
- Telephone system
- Wireless (including radio)

The following discussion outlines methods of preventing unauthorized entry from each avenue.

***4.3.1 Internet Intrusion.*** The outside hacker/attacker is most easily deterred at the firewall to the Internet. If no entry point is penetrable, the hacker will likely move on and choose an easier target. Internet access to the enterprise, however, is not always under the control of water utility Information Technology (IT) staff. In the cases of water departments in municipalities, it is common for the umbrella municipality to administer all security aspects of the Internet gateway.

No matter who administrates the Internet gateway, it is important for the utility to understand the standards that were used in developing security solutions. The Payment Card Industry (PCI) or Criminal Justice Information System (CJIS), for example, provide detailed configuration compliance requirements before allowing credit card payments or

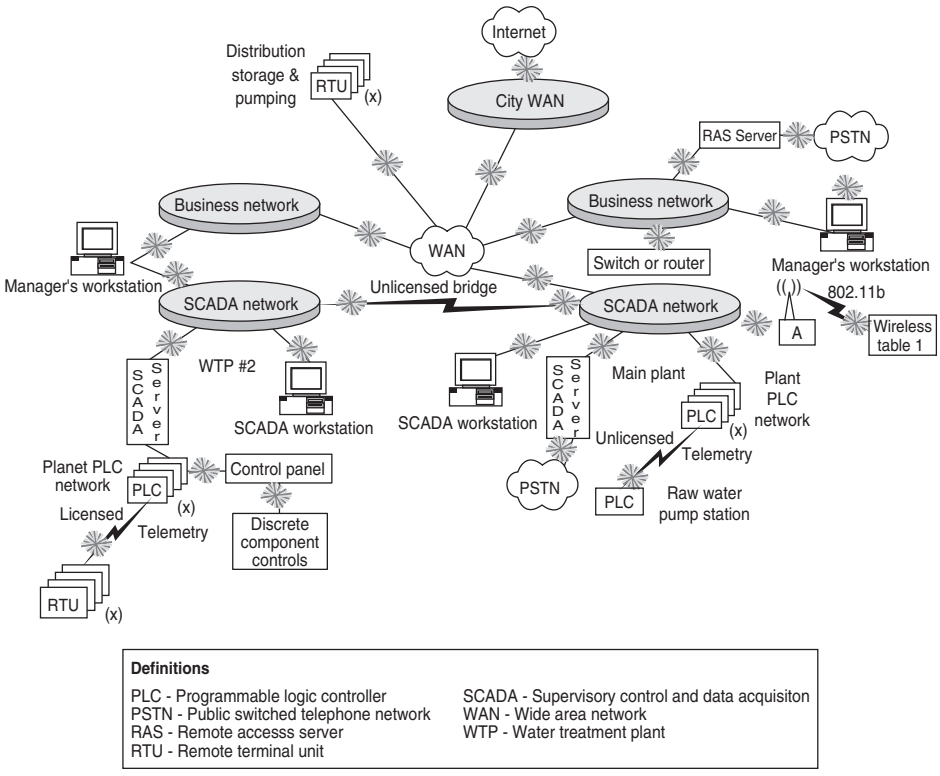



**FIGURE 6** Overview of SCADA system vulnerabilities.

storage of sensitive court documents. The National Institute of Standards and Technology (NIST) is currently the leading authority on providing SCADA system security guidelines (www.nist.gov); the SANS (SysAdmin, Audit, Network, Security) Institute (www.sans.org) provides similar guidelines for the business network.

Important internet intrusion prevention design elements include the following:

- *Intrusion prevention.* Install and monitor firewalls that employ "stateful packet inspection." For additional security, implement stateful packet inspection firewalls in combination with a "proxy server" firewall to provide a layered security approach. Conduct periodic penetration tests on the Internet firewall to uncover "open ports" commonly used by hackers.
- *Intrusion detection.* Install an Intrusion Detection System (IDS) at the Internet gateway and regularly audit IDS logs for evidence of unauthorized entry. An IDS can provide valuable information about intrusion attempts.
- *Access control.* Restrict general user access to critical applications via configuration of switches, routers, or internal firewalls. For example, segregate financial servers by locating them on a separate network segment with tightly restricted user access.

- *VPN access.* Employ a virtual private network (VPN) solution to ensure secure access to assets inside the enterprise from the Internet.
- *Hardened operating systems and applications.* Conduct server and workstation software audits to ensure the operating systems are "hardened" with the most current upgrades and security-related patches.

***4.3.2 Telephone System Intrusion.*** The most common method of telephone system intrusion is via dial-up modem. Many SCADA systems employ a modem to facilitate system maintenance by the vendor or utility IT staff. Traditionally, these modem connections have little or no security; they are an attractive target for "war-dialing," a common technique used by telephone hackers.

In addition, modems can be found attached to remote access servers (RAS) on the business network to facilitate employee dial-in. Finally, some employees occasionally install a personal modem to their workstation so they can access work from home. This last type of modem is difficult to track down and usually has no provisions for security. Design elements to reduce risk from the telephone system are as follows:

- *Modems.* Create policies designed to prevent the installation of unauthorized modems on enterprise equipment. Commercial phone-scanning software can usually identify modem connections not sanctioned by the utility. Turn off SCADA modems unless needed for remote troubleshooting or application updating by an authorized vendor representative. Configure modems to allow dial-up access from a restricted set of phone numbers. Use a timer to turn off modems after a preset period of time if not in use.
- *Telephone lines.* Telephone lines are sometimes used to connect to remote terminal units (RTUs) from the field. Consideration should be given to encrypting commands to prevent interference from attackers "tapping" into leased or owned phone lines.

***4.3.3 Wireless Intrusion.*** The explosion of wireless networking (or Wi-Fi) at home and in the workplace has created an enormous security risk for water utility network administrators. Many wireless installations in the workplace can exist without the knowledge of the IT group. These installations generally have little or no security and can be accessed by anyone within a large signal range.

- *Wi-Fi.* Configure authorized Wi-Fi access points to appropriate security and encryption levels. Minimize reception area by antenna type and placement. Use wireless detection software and hardware to identify unauthorized installations.

Many utilities rely on unlicensed radio transmission via 900 MHz radios to interact with remote SCADA components in the field. RTUs in the field exchange, monitor, and control information in "plain text." These unencrypted broadcasts can be intercepted and retransmitted with different—potentially harmful—information. Utilities should evaluate the following areas:

- *Unlicensed radio (900 MHz).* Encrypt radio traffic between RTUs (or programmable logic controllers (PLCs) with radio units) to master unit with scrambler/descrambler devices. As an alternative, modify or replace radios to take advance of more secure spread spectrum frequency-hopping transmissions.

- *Remote terminal units.* Provide hardened lockable enclosures for all remote control system units. Many of these units are in isolated areas with few protective measures to deter vandalism.

### 4.4 Deterring Cyber Attack from the Inside

The key to deterring inside attacks is a cyber security plan that seeks to minimize inadvertent or intentional damage to the SCADA system by employees and contractors. At the core of any security plan is an enforceable security policy and accompanying procedures that promote operational accountability and auditability. Several SCADA-specific security practices are as follows:

- *Separate the SCADA and business networks.* Isolate the SCADA network via firewalls or other networking devices that restrict network traffic to and from the business network. Figure 7 offers a simplified view of a SCADA network separated from the business network by a firewall.

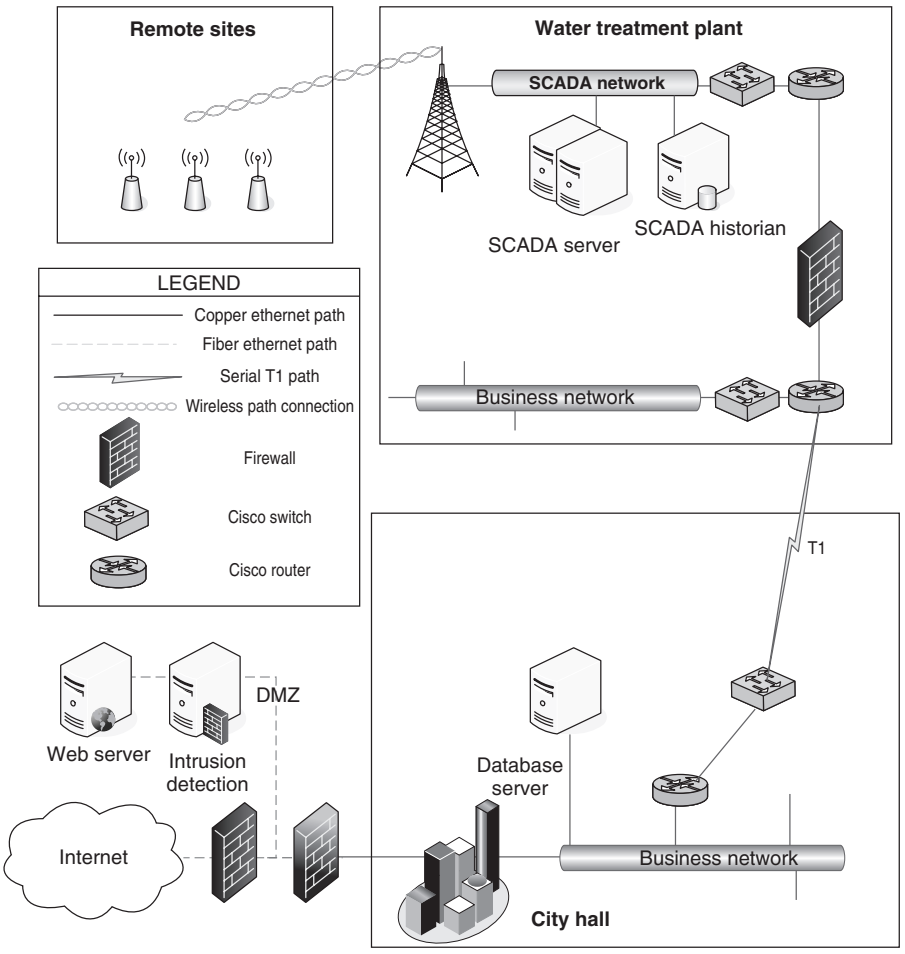



**FIGURE 7** Sample SCADA network separation diagram.

- *SCADA-specific policies.* Develop and post SCADA cyber security policies in control rooms. Immediately remove user accounts from the SCADA system upon termination of employees.
- *SCADA system passwords.* Require individual logon credentials to access the SCADA system. Enforce appropriate password-strength rules for user access (i.e., more "complex" passwords for administrators). Require a password to make software programming changes to RTUs/PLCs.
- *SCADA security guidelines.* Configure SCADA logon privileges to match responsibility levels. Maintain SCADA log files that associate user log-on credentials with actions and changes such as set points made to SCADA systems. Program set point ranges to reject potentially harmful out-of-range adjustments.
- *Physical security for SCADA.* Monitor access to the control room (and network/server room) with an entry system that stores information about who has entered and departed. Backup SCADA servers and programming workstations to tape every night and store appropriate tapes off site. Maintain SCADA infrastructure in environmentally appropriate facilities (with separate heating, ventilating, and air conditioning (HVAC), power redundancy, etc.).

## 5 CONTAMINATION WARNING SYSTEMS

After performing vulnerability assessments in 2002 and 2003, water utilities began to focus on the possible intentional or accidental contamination of their source and finished waters, a topic not addressed in the vulnerability assessments. Source waters can be easily contaminated due to unintended causes (agricultural runoff, accidental spills, etc.); however, treatment processes can reduce or eliminate the risk posed to consumers. On the other hand, the ease by which a distribution system can be contaminated accidentally (e.g. cross connections), or intentionally due to multiple points of access is of great concern to utilities. The large majority of utilities have realized that due to the novelty of the threat, the difficulty of detecting contamination, and the uncertainty of its consequences, they were not well prepared to cope with such incidents. To reduce the risks, significant work started in the area of contamination warning systems (CWSs) so that utilities can provide the appropriate response to protect the health and safety of the public and their employees. In addition to detecting contamination, the water quality monitoring also provides the dual benefit of operational insight, resulting in improved operations.

As a response to such industry concerns, various agencies (particularly the US Environmental Protection Agency (EPA)), professional associations, and utilities have undertaken various initiatives and projects on contamination detection. This interest has been reflected by the numerous conferences, seminars, and workshops given on the subject. Significant sources of information on the subject are the *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System* (Pikus, 2004) published by the American Society of Civil Engineers (ASCE), and several publications released under EPA's Water Security Initiative (formerly WaterSentinel). These publications include *WaterSentinel System Architecture*, Draft, Version 1.0 (EPA December 2005), *Water Security Initiative; Interim Guidance on Planning for Contamination Warning System Deployment* (EPA 817-R-07-002, May 2007), *WaterSentinel Online Water Quality Monitoring as an Indicator of Drinking Water Contamination* (EPA December 2005), *WaterSentinel Consequence Management Strategy*, Draft Version 1.0

(EPA December 2005) and *Overview of Event Detection Systems for WaterSentinel* (EPA December 2005). Furthermore, EPA's Threat Ensemble Vulnerability Assessment (TEVA) Research Program has released several papers on evaluating the impact of contamination on distribution system customers and locating sensors on distribution systems (http://www.epa.gov/nhsrc/news/news073007.html#sensor, accessed October 19, 2007). The material presented here has been primarily based on these documents.

According to the *Water Sentinel System Architecture* document, a CWS is "a proactive approach to managing threat warnings that uses advanced monitoring technologies/strategies and enhanced surveillance activities to collect, integrate, analyze, and communicate information to provide a timely warning of potential water contamination incidents and initiate response actions to minimize public health and economic impacts." This definition of CWS also includes information sources such as public health agencies, consumer complaints, physical security alerts, and laboratory analyses. A representation of such a comprehensive CWS is illustrated in Figure 8. In this article, CWS is limited to identifying contaminants through the use of online water quality monitoring instruments.

Pikus lists the following objectives of a CWS:

- to provide a reliable early warning of a contamination event so that steps can be taken to reduce its effects by limiting exposure of the at-risk population;
- to indicate the location and travel of the contaminant to facilitate implementation of the appropriate responses;
- insofar as possible, to identify the contaminant and determine its concentration so that the most appropriate response can be mounted, and to alert and inform the medical community about the potential need for treatment;

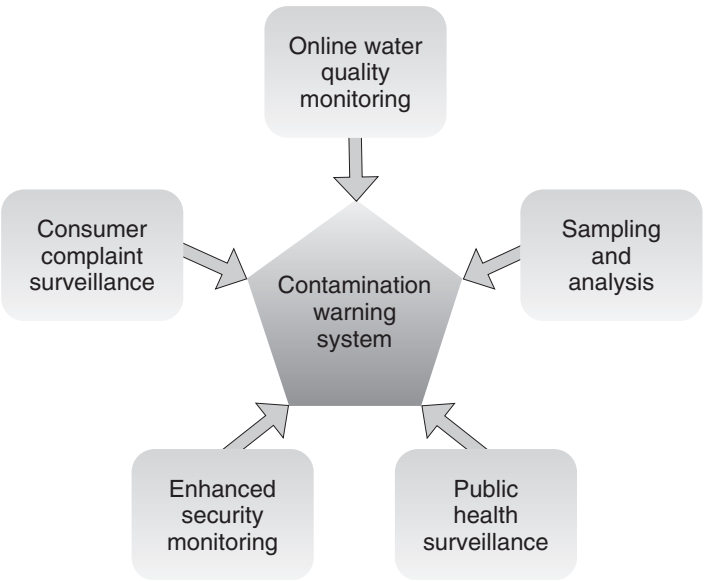



**FIGURE 8** Conceptual diagram of a comprehensive CWS. (Source: US EPA Water Security Initiative, Request for Applications for Contamination Warning System Demonstration Pilots Presentation, June 18, 2007.)

- to provide information on the "normal" operating characteristics of the water-supply or wastewater system;
- to support or supplement the existing regulatory surveillance activities.

To meet these objectives, the development of a CWS should include the following elements:

- types of contaminants to be monitored;
- online monitoring instruments and sensors (current industry practice assumes that monitoring should be continuous in order to spot any contamination events.);
- contaminant fate and transport models that are applicable under given hydraulic and water chemistry conditions;
- monitoring locations;
- communications links and protocols for the necessary collection, transfer, and analysis of data;
- integration with existing SCADA system;
- tools and guidance for the proper interpretation of data (that is, event detection systems).

### 5.1 Type of Contaminants

The need to know what the potential contaminants might be is to give utilities a sense of the potential threats to their systems, to provide the public health community a sense of the illnesses and medical emergencies that might occur, and to determine the monitoring instruments that might be better suited for each utility.

There are three major categories of contaminants:

- chemical (including biotoxins);
- biological (pathogens);
- radioactive materials.

Unfortunately, the number of potential contaminants is very large and unwieldy for the utilities to work with. EPA provided the following list of contaminant categories and identified which contaminant categories can be identified by which method (Table 1).

### 5.2 Monitoring Instruments

Given the extent of water distribution systems and the unlimited number of potential contamination insertion points, utilities might need a relatively large number of monitoring instruments in their systems to feel confident that they can detect any contamination on time. However, currently there are no affordable and practical continuous monitoring instruments that can identify all contaminants.

On the other hand, most known contaminants in water affect, to varying degrees, some measurable properties of the water, indicating their presence through changes in these properties. As a result these properties, or parameters, are called "surrogate" parameters, and they can be measured by commercially available and relatively affordable instruments. The effectiveness of these instruments, however, needs further scrutiny because

**TABLE 1 Contaminant Categories and Detection Strategies**

| Class | Description | Water Quality | Consumer Calls | 911 Calls/EMS | Hospital Data |
|---|---|---|---|---|---|
| 1 | Petroleum products | √ | √ | | |
| 2 | Pesticides (with odor or taste) | √ | √ | √ | |
| 3 | Inorganic compounds | √ | √ | √ | |
| 4 | Metals | √ | √ | √ | |
| 5 | Pesticides (odorless) | √ | √ | √ | |
| 6 | Chemical warfare agents | √ | | √ | |
| 7 | Radionuclides | √ | | √ | |
| 8 | Bacterial toxins | √ | | | √ |
| 9 | Plant toxins | √ | | | √ |
| 10 | Pathogens causing diseases with unique symptoms | √ | | | √ |
| 11 | Pathogens causing diseases with common symptoms | √ | | | √ |
| 12 | Persistent chlorinated organic compounds | √ | | | |

*Source: US EPA Water Security Initiative, Request for Applications for Contamination Warning System Demonstration Pilots Presentation, June 18, 2007*.

their sensitivity might not be sufficient to detect minor (but still real) changes in water quality due to contamination. Furthermore, changes in water quality also occur due to the dynamic nature of distribution systems (operational changes, source water blending, etc.).

Recommended surrogate parameters are:

- residual chlorine;
- turbidity;
- TOC;
- pH;
- conductivity;
- oxidation reduction potential (ORP);
- ammonia, chloride, and nitrate.

System pressure and temperature are also monitored.

Instruments that monitor these parameters are currently being employed in CWSs motelled at several US utilities. Once contamination is suspected, utilities need to collect additional samples and test them at a laboratory with specific contaminant detection capabilities for confirmation purposes.

### 5.3 Contaminant Fate and Transport Models

Contaminant fate and transport models are used to predict the change in the nature and concentration of the contaminants. These changes occur due to the various constituents in the water (e.g. chlorine residual), pipe characteristics (e.g., cement lining in iron

pipes, biofilm), the alkalinity of the water, and so on. Thus, these models support the interpretation of water quality changes, if they might be due to normal operational changes or due to contamination. In distribution systems, hydraulic/water quality network models are employed for this purpose.

### 5.4 Monitoring Locations

As mentioned above, a relatively large number of instruments might be needed to provide sufficient coverage to a distribution system. However, this is neither affordable nor practical. Thus, utilities must select an optimal number of locations that they can afford and sustain. There are some software packages that currently support the identification of sensor locations within distribution systems. EPA's TEVA program also supports this kind of applications. Pikus (2004) provides the following guidance in the selection of the instrument locations.

The local site conditions that a utility should consider include:

- easy access to the instrument site by authorized personnel;
- available space for the instruments and auxiliary equipment;
- suitability of candidate instruments for the sampling site and access to other utilities;
- physical security of the instrument site;
- hydraulic conditions at sampling sites;
- existing sampling sites for baseline or compliance monitoring.

System-wide and topological factors include:

- potential areas or points of entry of contamination;
- likely contaminants;
- contaminant transport time and concentration;
- proximity to vulnerable populations;
- relative water demand and associated flow characteristics.

### 5.5 Proper Interpretation of Data (Event Detection)

As discussed by Pikus, the purpose for analyzing the data obtained from monitoring instruments is to:

- identify the presence and location of significant contamination in the system;
- identify the contaminant or its class with sufficient specificity to allow appropriate responses;
- characterize the level of contamination at various parts of the system;
- determine time to consumption;
- eliminate false negatives and minimize false positives;
- assess public health risk;
- provide timely information to decision makers.

Data analysis, however, is a relatively complex task due to two primary sources of variability in the data:

1. Temporal variations, due to changing operational conditions in a water system, such as:
   - seasonal variations due to changes in the source water or demand (such as lawn irrigation in summers);
   - weekday variations due to changes in demands and operation practices (such as weekday vs. weekend use, utility maintenance activities, etc.);
   - diurnal variations due to changes in hourly demands by residential, commercial, or industrial customers.

   Typically, higher Cl residuals are observed when the water age is younger due to higher demand. In some cases, depending on the alkalinity of the water, cement-lined pipes affect the pH of the water in the distribution system, increasing pH with water age.
2. Instrument based variations which are introduced into the data due to the reliability of the instruments. Field instruments tend to require more maintenance and calibration than laboratory instruments and are less accurate. To increase the confidence in the sensors, it might be necessary to have duplicate instruments, but this is not a common practice due to increased maintenance needs and associated costs. More typical is taking duplicate samples for lab verification.

To address these issues, it is critical that a utility becomes very familiar with the quality of its water and its seasonal, weekday, diurnal and spatial variations. An illustration of temporal variations of chlorine residual at one utility is shown in Figure 9. This can be done by conducting a baseline water quality analysis, and then comparing monitoring instrument results with its baseline to determine whether there is potential contamination.

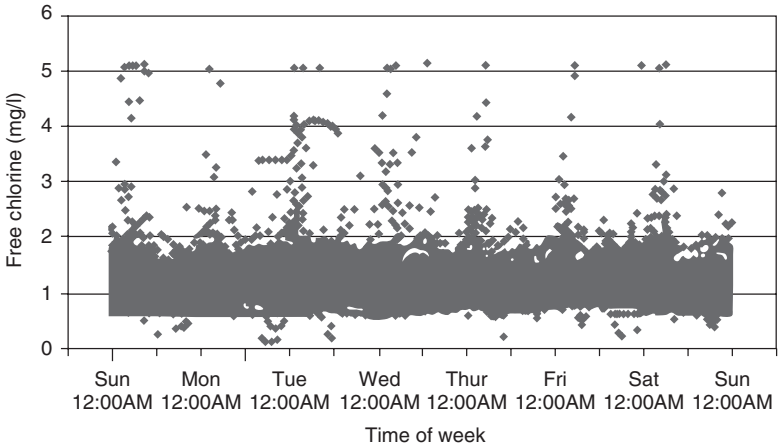



**FIGURE 9** Temporal variations in baseline Cl residual data.

**ACKNOWLEDGMENT**

The technical editor of this article was Jane Mailand from CH2M HILL.

# HOMELAND SECURITY AND WASTEWATER TREATMENT

MARC A. MILLS AND RICHARD C. BRENNER
*U.S. Environmental Protection Agency, Office of Research and Development, Cincinnati, Ohio*
JAMES F. KREISSL
*Environmental Consultant, Villa Hills, Kentucky*
MAKRAM T. SUIDAN
*University of Cincinnati, Cincinnati, Ohio*

## 1 INTRODUCTION

Wastewater results from mankind's use of water in all aspects of daily life, including personal hygiene, food preparation, commercial activity, industrial production, and recreation. Historically, increasing population density forced mankind to abandon localized disposal (cesspools, septic tanks, etc.) toward collection and conveyance of contaminated water away from population centers for the prevention of disease and protection of water supplies. The aggregate of these contaminated waters has over time come to be known as *wastewater* or *sewage*. Most commonly, this wastewater was directly discharged into local surface waters, such as streams, lakes, rivers, and oceans. Also, a limited amount of this water was used for irrigation.

Mankind's relationship to the environment has been documented as far back as 3750 BC in the form of archeological findings and ancient writings. The history of what we call "sewers" is most fascinating and is well documented in the literature. In the United States, the first sewerage system constructed in a major city is reported to have been in New York City in 1805 [1].

The long battle to separate mankind from its waste products has taken many turns owing to political decisions and cultural changes, but the agreement that the "great sewer construction period" in US cities occurred from the mid eighteenth century until 1915 when Baltimore completed its sewer system [1]. Most of these city sewer systems were

designed to dispose of both human wastes and stormwater to some distant point away from population centers.

Initially, the direct discharge of wastewater into local surface waters was not considered a serious human health or environmental concern [2]. This assessment was based solely on esthetic parameters such as color, odor, and clarity. As population density and per capita water use increased, combined with expanding industrial output, the impacts of these discharges became more pronounced, leading eventually to engineered wastewater management/treatment prior to discharge.

The practice of treating wastewater began with studies in London in the mid-nineteenth century and migrated to the United States soon after [1]. The number of municipalities and communities incorporating end-of-pipe treatment for their sewer systems grew phenomenally in the first half of the twentieth century. Initially, treatment approaches were primarily developed to reduce nuisance conditions (e.g. odors) in receiving waters and not for public health protection. Federal laws in the later part of the twentieth century were passed in response to the lack of state and local enforcement of pollution abatement laws and regulations. The results of passage and implementation of these federal laws have had a significant positive impact on the water quality of the majority of water bodies in the United States. The American Housing Survey of 2006 (US Census Bureau) estimated that nearly 80% of the US population is now served by municipal collection systems and treatment facilities.

The above historical scenario has evolved concurrently with newly developed scientific knowledge relating to the epidemiological basis of human exposure and disease. These advances in science served as the prelude to the passage of numerous federal and state laws that sought to minimize the now-quantifiable hazards to public health and, more recently, the environment.

## 2 DEVELOPMENT OF WASTEWATER SEWERAGE SYSTEMS

Stormwater conveyance has been documented as the major reason for the construction of most early sewers. Incorporation of human excretions into stormwater conveyance was initially strongly discouraged. The transition of combining the two wastes emanated primarily from England, which unfortunately passed this practice on to its colonies [1]. In the second half of the twentieth century, it became clear that "sanitary sewers" should be built to separate human wastes from stormwater; therefore, no new combined sewers have been installed in recent years. Separation of the two flows has become the norm in the United States. Conventional sewer design technology has not changed significantly for several decades and has often been applied inappropriately to smaller systems.

The governing principle of sanitary sewer design is that wastewater is conveyed from each service connection to the collector and then, it flows through the collector sewer by gravity. However, hydraulic design standards require that the pipe must slope sufficiently to maintain a velocity of 2 ft/s in order to convey the solids and prevent accumulations in the sewer that can lead to blockages. Thus, unless favorable ground slopes exist, the depth of cut to accommodate this requirement and, therefore, the cost per lineal foot become excessive. In the United States, this maximum depth is typically about 25 ft. In such cases, lift stations are required to pump the wastewater toward the ground surface in order to reestablish the necessary head for continued gravity flow. Design requirements

also dictate the insertion of manholes at regular (e.g. 250–300 ft) intervals to facilitate access to the sewer for inspection and cleaning.

After nearly 100 years, the above approach is still utilized in designing wastewater collection systems. For the past few decades, this type of system has been installed in suburbs outside of the densely populated urban areas for which they were originally conceived. This has resulted in increasingly expensive sewer systems that employ more sewer pipe length, manholes, and pump stations per service connection compared to strictly urban applications. This approach to sewer design, which can involve numerous connections below the groundwater table, tends to increase the infiltration of additional water requiring treatment. As a result, natural groundwater comingled with wastewater is treated and discharged into a surface water body that may be far removed from its original basin. Base flow in the surface waters of the original basin is thus reduced and wells in that basin can suffer reduced productivity. Examples of this effect can be found in Boston and other metropolitan areas [3].

Stormwater collection system designs are in a state of flux. In recent years, federal laws and regulations have forced cities to curtail unauthorized "non-point-source" (NPS) discharges into the waters of the United States. This has resulted in the emergence of numerous programs to minimize untreated discharges from combined and storm sewers. The impetus for these efforts has been the United States Environmental Protection Agency's (USEPA's) national surveys [4] that have determined that most of stream and lake water quality impairment in the United States is due to these and other NPS discharges, rather than from wastewater treatment plant (WWTP) effluents.

In recent years, considerable emphasis has been placed on prevention of runoff through on-site capture of rainwater and snowmelt. These efforts are aimed at reducing the volume and pollutant concentrations in conveyance systems. Although these sources are less concentrated in some pollutants than in municipal wastewater, they do contain most of the constituents displayed in Table 1 (from [5]) and are more concentrated in certain pollutants, such as metals and hydrocarbons. Best management practices are also being applied to provide end-of-pipe treatment for these formerly untreated contaminant sources.

## 3 DEVELOPMENT OF WASTEWATER TREATMENT SYSTEMS

### 3.1 Overview

Wastewater contains a number of physical, chemical, and microbiological pollutants. Some are objectionable only from an esthetic point of view, while others pose the potential for causing serious health problems and disease as well as damage to the environment. The major classes of contaminants found in residential or domestic wastewater are summarized in Table 1. Typical concentrations and per capita loadings of these contaminants for domestic wastewater are provided in Table 2 [5]. Industrial waste constituents of varying hazard potential and toxicity may receive some degree of pretreatment prior to being combined with the domestic wastewater component to form the mixed contaminated liquid flow known as *municipal wastewater*. Municipal WWTPs must contend with and treat all constituents present in the incoming flow, irrespective of the proportions and characteristics of the domestic and industrial contributions.

Table 2 clearly indicates that wastewater is laden with potential pathogens (bacterial and viral), putrescibles (organics that can result in oxygen deficiency and generation of odors), and nutrients (nitrogen and phosphorus that can stimulate nuisance organism

**TABLE 1 Wastewater Pollutants of Concern**

| Pollutant | Reason for Concern |
|---|---|
| Suspended solids | In surface waters, can result in the development of sludge deposits that smother benthic macroinvertebrates and fish eggs and may contribute to benthic enrichment, toxicity, and sediment oxygen demand. Excessive turbidity can block sunlight, harming aquatic life (e.g. block sunlight needed by plants) and contribute to decreased dissolved oxygen in the water column. In drinking water, turbidity is esthetically displeasing and interferes with disinfection |
| Biodegradable organics | Biological stabilization of organics in the water column can deplete dissolved oxygen in surface waters, creating anoxic conditions harmful to aquatic life. Oxygen-reducing conditions create taste and odor problems in drinking water and allow metals to leach from soil and rock in ground to surface waters |
| Pathogenic agents | Parasites, bacteria, and viruses can cause communicable diseases through direct/indirect body contact or ingestion of contaminated water or shellfish. A particular threat when partially treated sewage pools on ground surfaces or migrates to recreational waters. Transport distances of some pathogens in ground or surface waters can be significant |
| Nitrogen | An aquatic plant nutrient that can contribute to eutrophication and dissolved oxygen loss in surface waters, especially in lakes, estuaries, and coastal embayments. Algae and aquatic weeds can contribute trihalomethane (THM) precursors to the water column that may generate carcinogenic THMs in chlorinated drinking water. Excessive nitrate nitrogen in drinking water can cause methemoglobinemia in infants and pregnancy complications for humans. Livestock can also suffer health impacts from drinking water high in nitrogen |
| Phosphorus | An aquatic plant nutrient that can contribute to eutrophication of inland and coastal surface waters and reduction of dissolved oxygen |
| Toxic organics | Toxic organic compounds present in household chemicals and cleaning agents can interfere with certain biological processes in conventional and alternative on-site wastewater treatment systems (OWTSs) and can be persistent and bioaccumulative in the aquatic environment. They can cause damage to ecosystems and human health directly or through ingestion of contaminated aquatic organisms (e.g. fish and shellfish) |
| Heavy metals | Heavy metals (e.g. lead and mercury) in drinking water can cause human health problems. In the aquatic ecosystem, they can also be toxic to aquatic life and accumulate in fish that may be consumed by humans, resulting in metal toxicity health threats |

growth that degrade water quality). Thus, the practice of early sewer builders in separating urban populations from their waste products was based on factual elements that were not yet understood fully.

Early wastewater treatment practices concentrated on the removal of suspended materials, floatables, and garbage and debris [6]; [7]. The preliminary and primary treatment processes employed for achieving these limited objectives consisted of screening, sedimentation, and grease/oil removal [8]. This type of treatment removed visible objectionable materials without affecting the chemical and biological characteristics of the waste appreciably. However, the discharged wastewater still contained sufficient organic matter to cause significant adverse impacts on receiving waters. The remaining organic content of this wastewater was removed through aerobic biodegradation

**TABLE 2 Constituents of Typical Residential Wastewater**

| Constituent | Mass Loading (grams/person/day) | Concentration (mg/l) |
|---|---|---|
| Total solids (TS) | 115–200 | 500–880 |
| Volatile solids | 65–85 | 280–375 |
| Total suspended solids (TSS) | 35–75 | 155–330 |
| Volatile suspended solids | 25–60 | 110–265 |
| 5-day biochemical oxygen demand ($BOD_5$) | 35–65 | 155–286 |
| Chemical oxygen demand (COD) | 115–150 | 500–660 |
| Total nitrogen (TN) | 6–17 | 26–75 |
| Ammonia ($NH_4$) | 1–3 | 4–13 |
| Nitrites and nitrates ($NO_2$-N; $NO_3$-N) | <1 | <1 |
| Total phosphorus (TP) | 1–2 | 6–12 |
| Fats, oils, and grease | 12–18 | 70–105 |
| Volatile organic compounds (VOC) | 0.02–0.07 | 0.1–0.3 |
| Surfactants | 2–4 | 9–18 |
| Total coliforms (TC) | — | $10^8$–$10^{10}$ |
| Fecal coliforms (FC) | — | $10^6$–$10^8$ |

resulting in depletion of dissolved oxygen (DO) in the water body and concomitant fish kills and degradation of drinking water resources. Additionally, the recreational use of these water bodies became problematic due to increased incidence of water-borne diseases [9]. In retrospect, use of impacted surface waters for drinking water supply required more rigorous chlorination, which we now know results in the formation of carcinogenic chlorinated disinfection byproducts.

In the first half of the twentieth century, these observations and human health impacts underscored the need for more advanced wastewater treatment focused on reduction of dissolved organic matter. Biological oxidation rapidly emerged as the most viable technology to achieve this objective. Early biological treatment systems consisted of lagoons that afforded sufficient retention time for microorganisms to convert organic matter into carbon dioxide ($CO_2$), water, and new biomass [10]. Due to the large footprint required for lagoon-based treatment, its use was limited primarily to small flows and rural areas [10]. Application of biological treatment to large wastewater flows typical of high-density population centers led to the development of more efficiently engineered biological systems that emphasized the retention of large concentrations of biomass allowing more compact treatment systems. Numerous treatment processes, commonly referred to as *secondary treatment*, emerged. These secondary treatment processes were not only effective in reducing the dissolved organic content of wastewater, but were additionally capable of trapping a significant portion of suspended matter with the retained biomass. Prominent among these processes were the activated sludge (AS) and trickling filter systems. Typically, secondary treatment is used in conjunction with primary treatment where the two systems complement each other, yielding effluents low in suspended and dissolved organic matter. Wide application of these systems significantly improved the esthetic quality of the receiving waters of this country.

Primary settling is a separation process that results in the production of waste solids, while secondary treatment results in the production of excess biomass. These solids-bearing streams, commonly referred to as *primary and secondary sludge*,

respectively, require further treatment and disposal or reuse. Sludge handling and treatment generally consists of volume reduction, stabilization, dewatering, and final disposal via incineration or landfilling. Alternatively, treated sludge can be land applied for soil conditioning and nutrient enhancement.

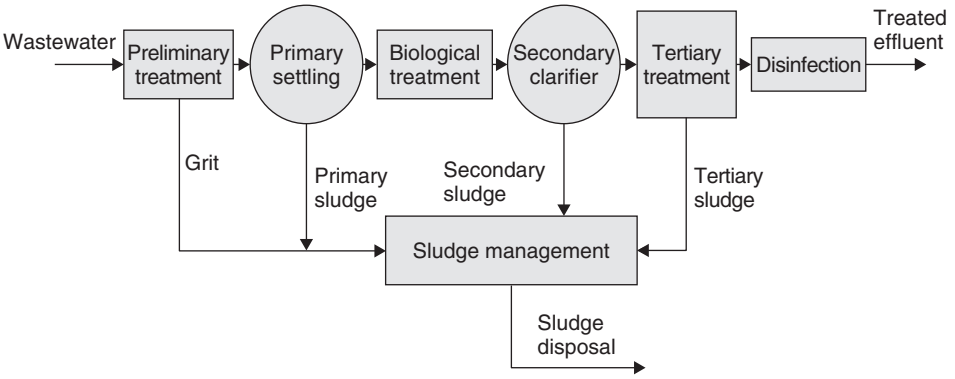
During the 1960s–1980s, USEPA instituted a Construction Grants Program to assist municipalities in upgrading existing primary treatment plants to secondary treatment. These upgraded treatment plants improved the receiving water quality across much of the United States with significant human health and environmental benefits as manifested in reduced enteric disease transmission, less fish kills and consumption advisories, less recreational contact hazards, more suitable water supply resources, and a general sense of environmental well being [8].

The significant improvements in receiving water quality realized as a result of widespread implementation of secondary treatment focused attention on remaining problems associated with the environmental impact of continued discharge of nutrients, such as nitrogen and phosphorus. The widespread use of soil-based wastewater systems in rural areas generally captured most of the phosphorus in the soil, but nitrogen was only partially removed (~20%) before incorporation into groundwater. Phosphorus (in freshwater) and nitrogen (in marine water) discharge continued to promote the excessive growth of algae (a process known as *eutrophication*), whereas the discharge of ammonia from most secondary plants resulted in oxygen depletion due to the oxidation of ammonia to nitrate in the receiving water. Excessive algal blooms are undesirable due to oxygen depletion in shallow waters and the production of esthetically displeasing taste and odor compounds in drinking water. As a result, additional treatment became necessary in many areas to manage the nutrients discharged in WWTP effluents [10].

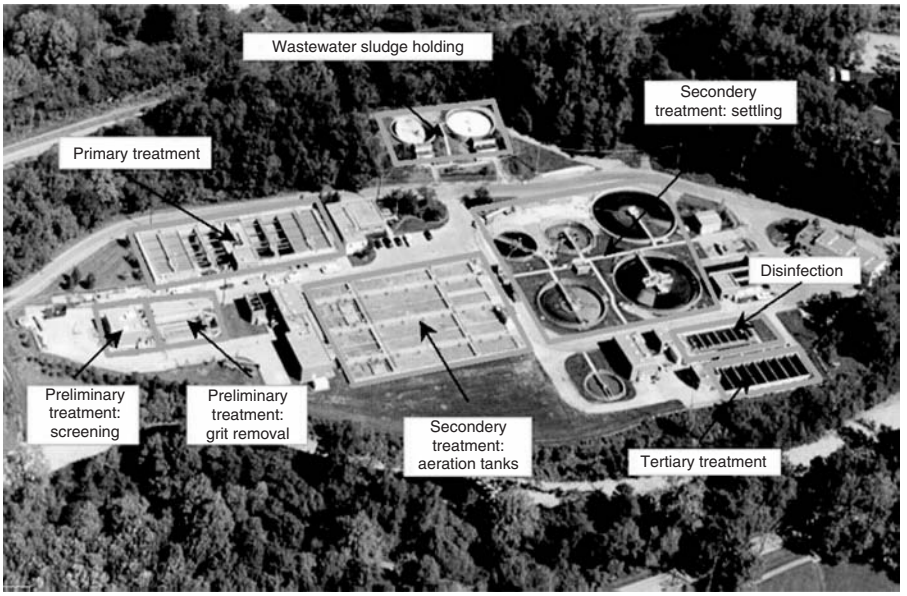
Collectively, the group of technologies designed to control nutrients and further reduce organics and solids in final effluents is referred to as *tertiary treatment*. Innovative treatment processes have been developed to further improve WWTP effluent quality. These include sand filtration for improved solid reduction, carbon adsorption for managing specific industrial pollutants and alternative disinfection processes, such as ozonation and ultraviolet (UV) inactivation, which do not form chlorinated byproducts, and some membrane separation technologies (e.g. reverse osmosis) facilitate more direct water reuse [11].

### 3.2 Description of Treatment Processes

Most of the modern large treatment plants are comprised of preliminary treatment units, primary settling or clarification, hereafter referred to as *primary clarification*, and secondary biological treatment consisting of a biological oxidation process followed by separation of solids, that is, secondary or final clarification. The liquid treatment sequence is sometimes followed by one or more tertiary treatment units needed to meet specific effluent discharge requirements or standards. The final step in the treatment sequence is usually effluent disinfection to reduce the pathogenic potential. Preliminary treatment, primary clarification, secondary biological treatment, and tertiary treatment processes (if used) result in a treated effluent and generate various waste sludge streams and debris that require subsequent treatment and/or disposal. A schematic diagram of a typical municipal WWTP is presented in Figure 1a. An aerial photograph of the Sycamore municipal WWTP, Cincinnati, Ohio is shown in Figure 1b. Following is a brief discussion of the treatment unit operations shown in Figure 1a.




(a)




(b)

**FIGURE 1** (a) Schematic diagram of a typical municipal wastewater treatment plant. (b) Aerial view of the Sycamore municipal WWTP, Cincinnati, Ohio.

***3.2.1 Preliminary Treatment.*** Depending on the topography and location of a WWTP, gravity flow collection systems commonly used for conveying wastewater to the plant normally result in the wastewater reaching the plant that is significantly below grade. This may necessitate the need for a lift pump to transfer the wastewater to the plant elevation. To protect the lift pump, screening devices are often employed to remove large objects from the wastewater. These may include dead animals, rags, tires, wood debris, and other large objects that may hamper proper functioning of the pumps [11].

Once at plant elevation, comminutors or grinders are often used to decrease the size of the remaining suspended materials in the wastewater. Comminution is typically followed by grit removal. Grit removal devices (grit chambers) are designed to separate high-density inert particles from low-density organic particles. This separation

is accomplished through the use of high superficial flow velocities that scour the high-surface area, low-density organic particles from the grit. Grit chambers are commonly of two designs, air lift vortex or high-velocity open channel design [10].

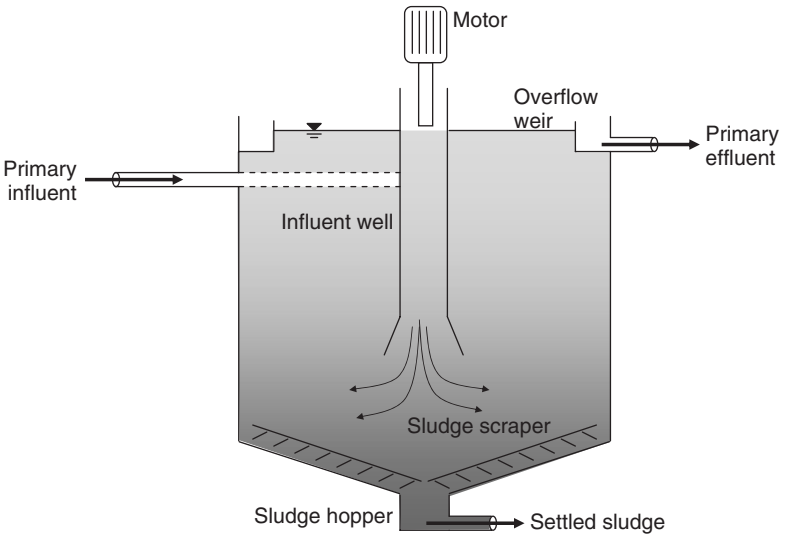
***3.2.2 Primary Clarification.*** The organic content remaining in wastewater after preliminary treatment is comprised of a suspended fraction and a dissolved fraction. Collectively, the organic content of wastewater is often quantified using surrogate measures such as biochemical oxidation demand (BOD) and/or chemical oxygen demand (COD). Both of these measurements represent an estimate of the oxygen required to mineralize the organic matter to $CO_2$ and water. Total suspended solids (TSS) refers to the *filterable portion* of the solids remaining in the wastewater. TSS comprises both organic and inorganic material. The ignitable fraction of the TSS is referred to as *volatile suspended solids* (VSS) and is used as a surrogate for solids of organic origin.

Primary clarification consists of a continuous flow tank that provides a quiescent zone and adequate retention time to remove 50–67% of TSS and 27–40% of BOD [10]. Solids thus removed are collected in a hopper at the bottom of the tank and can be withdrawn intermittently or continuously. The withdrawn material is referred to as *primary sludge*. Floatables present in the wastewater (i.e. grease, oil, and scum) are removed at the surface using skimming devices. Floatables are generally burned and primary sludge is routed to subsequent sludge management units. Primary clarifiers are commonly 10–16 ft deep and provide a hydraulic retention time (HRT) of 1.5–2.5 h [10]. A schematic diagram of a typical circular primary clarifier is portrayed in Figure 2a. A photograph of a rectangular primary clarifier at the Gest Street WWTP of the Metropolitan Sewage District of Greater Cincinnati, Ohio is shown in Figure 2b.

***3.2.3 Secondary Treatment.*** Secondary treatment is most often comprises two unit processes, a biological oxidation reactor followed by a solids separation unit (final clarifier). Within the biological reactor, most organic matter is transformed by biomass (bacteria and other microorganisms) to innocuous end products and new biomass. Excess biomass is commonly referred to as *waste secondary sludge*, and is managed either separately or in combination with primary sludge [11]. The most commonly employed secondary biological treatment processes are the AS and trickling filter (TF) systems.

*3.2.3.1 Activated Sludge.* AS systems rely on biomass sedimentation and recycle to maintain elevated levels of suspended biomass within a biological reactor called *aeration tank*. Mixing and oxygen transfer within the aeration tank are accomplished by either mechanical or diffused aeration devices. The sustained operation of AS systems requires the removal of excess biomass (waste AS) to maintain a manageable inventory of biomass (mixed liquor) within the secondary treatment system. The ratio of the biomass inventory within the AS system to the biomass wasted daily in the secondary sludge is referred to as the *solids residence time* (SRT). This parameter is typically maintained in the range of 5–15 days, whereas the aeration tank is usually designed to provide an HRT of 3–8 h [10]. Biomass recycle (return AS) and the concomitant decoupling of HRT and SRT in an AS system results in volume reduction in the biological reactor equivalent to the ratio of SRT/HRT.

The secondary clarifier in the AS system serves two functions, liquid–solid separation (clarification) and biomass concentration. Clarification takes place in the upper portion of the secondary clarifier, and its effectiveness depends on the nature of the biomass




(a)

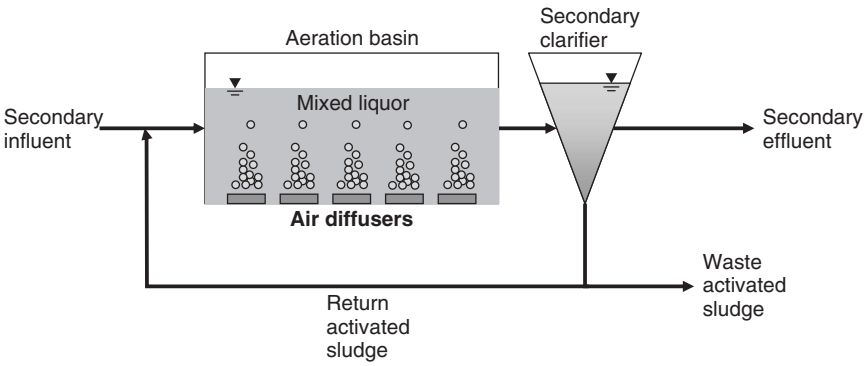

(b)

**FIGURE 2** (a) Schematic diagram of a typical circular primary clarifier. (b) Photograph of a rectangular primary clarifier in Gest Street WWTP at the Metropolitan Sewage District of Greater Cincinnati, Ohio.

solids and the discharge rate of the clarified wastewater flow per unit surface area of the tank (overflow rate). The lower portion of the secondary clarifier is devoted to the collection and thickening of settled biomass prior to its recycle to the aeration tank. The degree of thickening achieved in the clarifier hopper depends on the type of sludge collection and removal system utilized and biomass characteristics. Optimization of the thickening function of the clarifier allows a more compact aeration basin design. Excess

biomass produced in the aeration tank is commonly wasted from the secondary clarifier recycle stream. This wasting operation is necessary to maintain biomass SRT at levels that permit effective settling of these solids to the bottom of the clarifier. Skimming devices are used on the surface of these clarifiers to collect and transport floating particles to a waste trough. Secondary clarifiers for the AS system are typically 12–20 ft [10] in depth with an HRT of 2–3 h [11]. Successful operation of the AS treatment system is predicated on the ability of biomass to agglomerate into larger particles (flocs) that are amenable to settling and removal.

A schematic diagram of a typical diffused aeration AS system is shown in Figure 3a. A photograph showing the surface of AS aeration basins equipped with diffused aerators at the Gest Street plant of the Metropolitan Sewage District of Greater Cincinnati, Ohio is given in Figure 3b.




(a)

(b)

**FIGURE 3** (a) Schematic diagram of a typical diffused aeration activated sludge system. (b) Photograph of several activated sludge aeration basins (diffused aeration) in Gest Street WWTP at the Metropolitan Sewage District of Greater Cincinnati, Ohio.

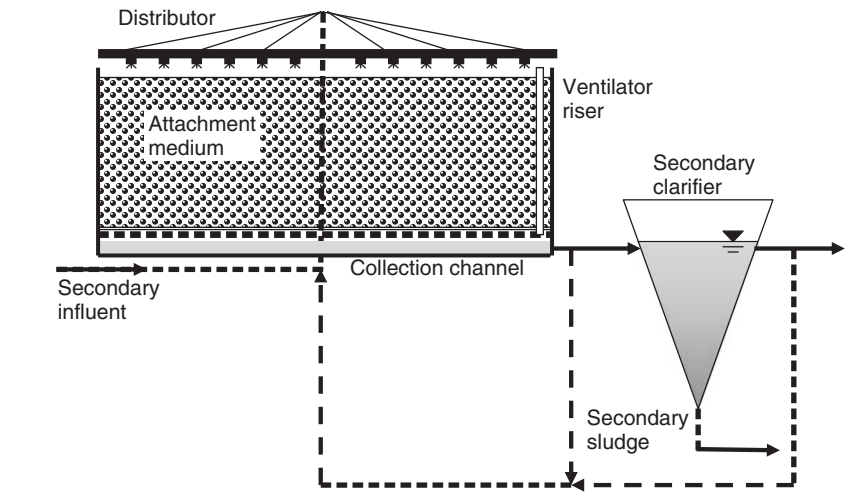
*3.2.3.2 Trickling Filtration.* TF systems are generally used as a simpler secondary treatment system for smaller municipalities. TF systems are comprised of two components, a TF bioreactor followed by a secondary clarifier. TFs rely on the application (or trickling) of a thin layer of primary effluent to the surface of a bed of artificial or natural inert filter media onto which attached biomass has developed (biofilm). The applied wastewater trickles by gravity flow down through the media for treatment. Successful operation of TF systems requires uniform distribution of wastewater across the filter surface and with depth. Application rates should not exceed the biofilm's soluble organic removal capacities for efficient treatment to occur. Attachment media options include natural materials (such as rock and redwood) and synthetic engineered materials (such as plastic and blast furnace slag) that optimize flow distribution and media porosity and maximize attachment surface area and oxygen transfer. Effluent recirculation is employed with rock media to effect more even flow distribution and media wetting and thereby promote improved removal efficiency. Effluent recirculation becomes less necessary when engineered or more open media are used [10].

The primary function of the secondary clarifier in a TF system is to clarify the treated wastewater for effluent discharge. In addition, biomass sloughed from the TF media, which represents the net biomass growth, settles to the bottom of the clarifier from where it is wasted for subsequent management. Secondary clarifiers following TF systems are designed with up to 15 ft depth [10] and an HRT of 1–1.5 h [11]. A schematic diagram of a typical TF system is presented in Figure 4a. Photographs of a typical rock media trickling filters are shown in Figure 4b.

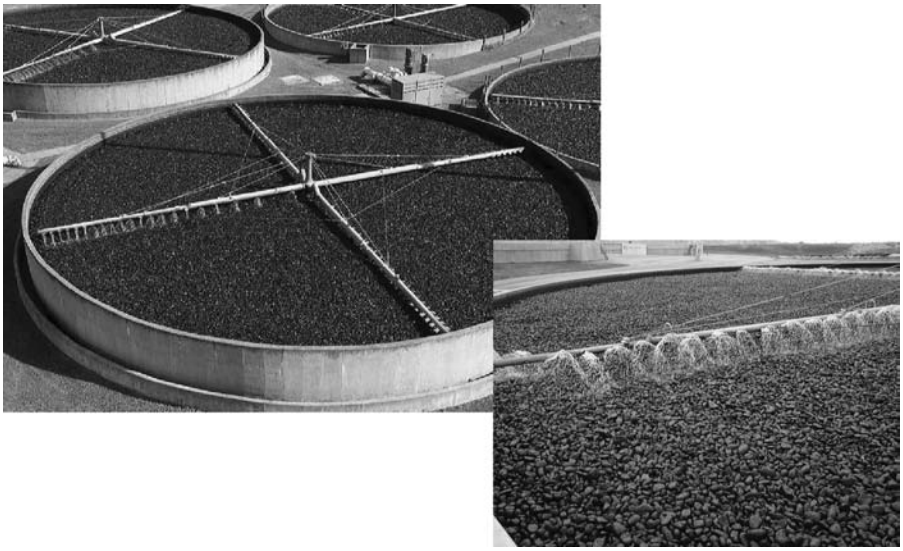
*3.2.3.3 Comparison of AS and TF Systems.* Although both AS and TF systems are regarded as secondary treatment processes, the two technologies differ significantly with respect to effluent quality, ease of operation, resiliency or susceptibility to upsets, and adaptability for nutrient control and tertiary treatment. In general, AS systems maximize soluble organic removal, while TF systems are well adapted to the removal of suspended particles and result in less turbid effluents [10]. With the interchange of biomass between aeration tank and clarifier, the secondary clarifier of an AS system requires considerable operator attention and staffing due to its sensitivity to varying wastewater characteristics and aeration basin operating conditions. Since biomass in a TF is retained within the bioreactor, management of the biomass inventory is less challenging than in AS systems. TFs operate at significantly higher SRTs than do AS systems, resulting in less biosolids production and, therefore, less biosolid disposal requirements. TFs are more resilient and less susceptible to chemical upsets (both natural and intentional) because the attached biomass, with its reduced impacted surface area and exposure time, is less vulnerable to toxic episodes. Furthermore, AS systems are more susceptible to extreme flow events that can lead to biomass washout from the final clarifier resulting in temporary process failure.

With their many possible flow and aeration configurations, AS systems can be designed to treat wastewater of differing characteristics. For example, selection of the sludge recycle reentry point can be tailored to optimize treatment of wastewater of differing organic contaminant strengths and distribution of organic matter between the suspended and soluble fractions.

***3.2.4 Nutrient Control.*** Many nutrients are found in municipal wastewater, those of most concern being ammonium nitrogen (ammonia) and phosphorus [10]. Ammonia




(a)



(b)

**FIGURE 4** (a) Schematic diagram of a typical trickling filter system. (b) Photographs of typical rock media trickling filters (adapted from http://industrial–landscape.com and www.centervilleut.net).

is a reduced form of nitrogen that can, with appropriate process control, be biologically oxidized to nitrate nitrogen (nitrate) in WWTPs. If not oxidized in the WWTP, ammonia will normally be oxidized over a longer period of time in receiving waters contributing to oxygen depletion. Single-stage secondary AS systems can under optimum operating conditions of organic loading, SRT, temperature, and DO achieve ammonia oxidation (nitrification). Alternately, nitrification can be achieved in specially designed second-stage AS or TF systems where the bulk of the organic content of the wastewater has been removed in a first-stage secondary treatment unit. Such second-stage units can

be designed for maximum nitrifying biomass retention to compensate for low oxidation rates associated with lower seasonal temperatures.

Effluent dominated receiving waters and health issues (i.e. blue baby syndrome) may require nitrate removal (denitrification) [6]. Denitrification is the process of reducing nitrate to nitrogen gas using either organic matter present in the wastewater or the addition of an organic substrate. When wastewater organic matter is to be used for denitrification, a portion of the aeration basin is reserved for this process, with the degree of nitrate removal achieved dictated by the wastewater recycle rate. Alternately, more complete denitrification is possible by passing the entire nitrified effluent through a dedicated biological unit process. Such a process can either be a variation of the AS system or one of several fixed film designs [10].

Phosphorus removal can be accomplished through biological or chemical control technologies, with chemical technologies being more prevalent at present. Chemical phosphorus control relies on the precipitation of orthophosphate as a metal salt (i.e. iron, aluminum, or calcium). Chemical precipitation agents can be added to the primary clarifier or the aeration basin or the recycle sludge flow of an AS system. For fixed film systems, precipitating chemicals are added to either the primary or secondary clarifiers, but not directly to the fixed film reactor in order to avoid coating of the biofilm.

***3.2.5 Tertiary Treatment.*** Depending on final effluent discharge standards and the possibility of water reuse (direct or indirect), many types of unit processes can be employed for the removal of trace residual organics and metals, dissolved salts, and residual particulate matter [11]. Such processes include, but are not limited to, ion exchange, reverse osmosis, carbon adsorption, chemical coagulation/flocculation, and various forms of filtration (e.g. sand filtration, dual media filters, and ultrafiltration) [11]; [10]. Of these processes, filtration is the most commonly practiced form of tertiary treatment. Filtration is primarily used to remove suspended and colloidal particles and associated organic matter. Such a polishing process enables municipal WWTPs to meet discharge standards of BOD and particulate matter that are not attainable using conventional biological treatment technologies alone.

***3.2.6 Disinfection.*** Prior to final discharge, treated wastewater is often subjected to one of several disinfection processes for pathogen control. This is particularly important when the effluent is discharged to receiving waters used for recreational purposes (swimming, skiing, fishing, etc.) or as a drinking water source. Disinfection process alternatives consist of chlorination, UV light, and ozonation, with chlorination being by far the most common choice. Typically, chlorination is followed by sulfur dioxide dechlorination to remove any free and combined chlorine residuals prior to discharge.

***3.2.7 Sludge Management.*** Wastewater treatment results in the production of several sludge streams requiring further handling, treatment, and final disposal. These sludges are comprised of suspended matter removed during primary treatment and excess biomass generated during secondary treatment. Additionally, smaller waste sludge streams can be produced if tertiary treatment is practiced.

The primary and secondary sludge streams are often treated biologically (either aerobic or anaerobic digestion) to destroy a portion of the organic matter and excess biomass. The purpose of sludge digestion is to stabilize organic matter, thus rendering it less

susceptible to rapid decomposition upon final disposal. Uncontrolled rapid decomposition is accompanied by noxious odors and may serve as a vector attractant promoting the spread of disease. Aerobic and anaerobic processes used for sludge digestion are single-pass systems requiring very long contact times (SRTs ranging from 40 to 60 days for aerobic digestion and 10–28 days for anaerobic digestion) [10]. Consequently, concentration of the sludge stream prior to the digestion unit operation is highly desirable to minimize digester volume. Primary sludge is more concentrated than waste secondary sludge and, therefore, may not require preconcentration (thickening) prior to digestion as may be necessary for waste secondary sludge.

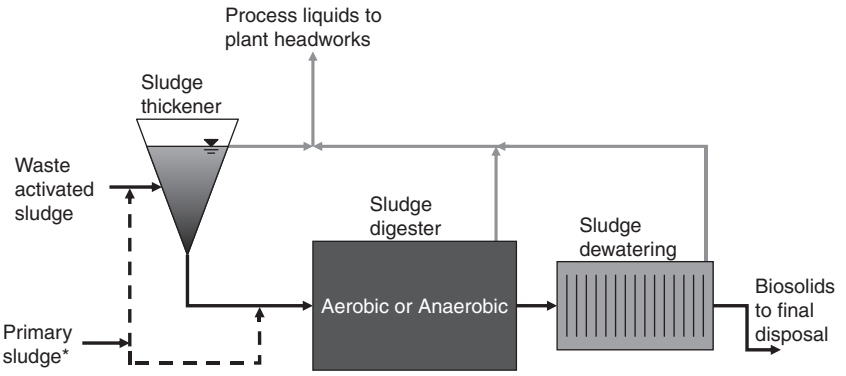
Sludge thickening is often accomplished using separate gravity settling tanks optimized to generate sludges with solid contents in the 3–5% range. The thickening process generates a very turbid supernatant that is recycled to the head of the plant for treatment. Alternately, waste secondary sludge can be recycled to the primary clarifier for cothickening with the primary sludge.

Aerobic sludge digestion is carried out in aeration basins under oxidative and ambient temperature conditions and yields destruction of organic suspended solids in the range of 38–50%. Conversely, anaerobic digestion occurs under reductive (fermentative) conditions and often requires heating to elevated temperatures to achieve mesophilic conditions (37–42°C) as well as destruction of organic suspended solids by approximately 50% [11]. Some WWTPs utilize even higher temperatures for anaerobic digestion (into the thermophilic range of 50–57°C) [10] to promote even greaterdestruction of solids and sludge stabilization. Aerobic digestion converts organic carbon into $CO_2$, whereas under anaerobic conditions, organic carbon is converted into methane and $CO_2$. The methane is often used to partially satisfy the energy needs of the WWTP.

Prior to final disposal and to reduce handling costs, digested sludge is typically subjected to dewatering that can yield sludge solid contents ranging from 12 to 40% depending on the selected dewatering device [8]. Processes utilized for sludge dewatering include centrifuges, vacuum filters, belt presses, filter presses, and sand drying beds.

Sludges that have been subjected to biological stabilization and dewatering are known as *biosolids*. Biosolids can be disposed in sanitary landfills or applied for soil conditioning to agricultural fields or for land reclamation (land application) [8]. Despite its inherent reuse of nutrients and other constituents in soil, biosolids land application is currently being subjected to increased public scrutiny due to potential nuisance and health concerns arising from aerosols drift, contact hazards, runoff to surface waters, and groundwater contamination. Incineration, while practiced historically, is less common today due to increasing costs, increasing community resistance, and perceived health issues with stack emissions. A schematic diagram of a typical sludge management system is illustrated in Figure 5a. Photographs of heated and unheated anaerobic digesters at the Fairfield Ohio WWTP are presented in Figure 5b and c, respectively. Photographs of two belt filter presses used for sludge dewatering are depicted in Figure 5d, whereaswhile a centrifuge and vacuum filter are shown in Figure 5e.

***3.2.8 Wastewater Reuse.*** Wastewater reuse can be divided into two categories, potable and nonpotable uses. Typical nonpotable reuse includes agricultural, irrigation and industrial applications. Agricultural and irrigation applications involve the reuse of wastewater that has received varying degrees of treatment prior to its application to crop, forage, and recreational areas [10]. Treated wastewater is generally used by industries for process and cooling water applications.



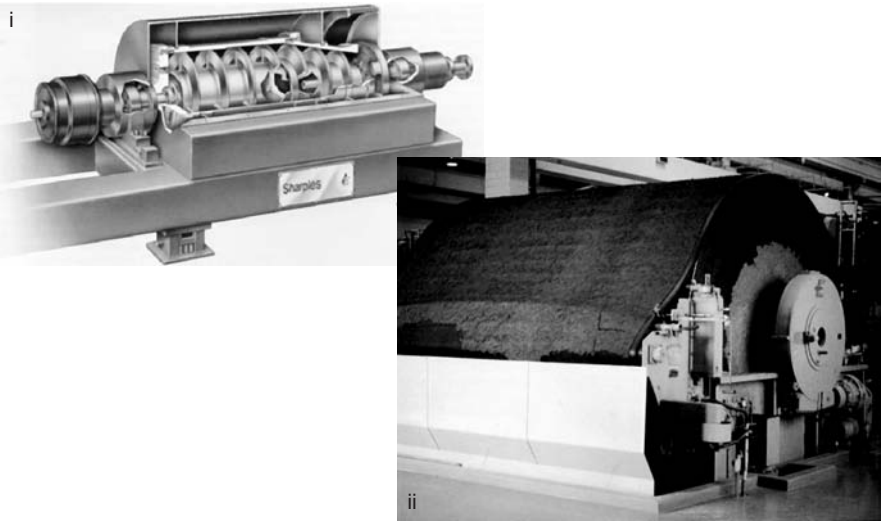

(a)

(b)

(c)

**FIGURE 5** (a) Schematic diagram of a typical sludge management system. *Primary sludge to sludge thickener or sludge digester. (b) Photograph of heated anaerobic digester at the Fairfield, Ohio WWTP. (c) Photograph of unheated anaerobic digester at the Fairfield, Ohio WWTP. (d) Photographs of belt filter presses used for sludge dewatering (adapted from www.adrcompany.net and www.argesmakina.com). (e) Photographs of centrifuge (i) and vacuum filter (adapted from www.student.nvcc.edu) (ii) used for sludge dewatering (adapted from www.fsid.cvut.cz).

(d)




(e)

**FIGURE 5** (*Continued*)

Direct potable water reuse involves treatment of WWTP effluents employing traditional or more advanced water treatment technologies to produce finished drinking water that meets all applicable quality standards. Indirect water reuse has been practiced historically, either inherently or by design. Water withdrawn from surface and groundwater sources for human consumption frequently contains a significant fraction of treated or untreated municipal wastewater or agricultural runoff. In the arid western and southwestern portions of the United States, population pressures are increasingly dictating the use

of effluent dominated flows as drinking water sources [11]. Such instances mandate the use of fail-safe, nontraditional technologies, such as membrane separation and advanced oxidation treatment. Membrane separation is often employed for the removal of dissolved inorganic species, while advanced oxidation targets dissolved refractory organic matter.

Direct potable water reuse is not normally allowed in the United States, but aquifer recharge combined with specific minimum aquifer retention times prior to use appears to be gaining in popularity as an indirect water reuse option. Extended residence of this recharged water in the aquifer can mitigate or dilute residual contaminants inherent to wastewater.

## 4 PUBLIC RISK AND WASTEWATER TREATMENT INFRASTRUCTURE

Public vulnerability to disruptions of wastewater collection and treatment systems is of a secondary nature and not as critical as disruptions to drinking water, power, communications, and public health systems. Nevertheless, there are severe implications associated with wastewater treatment disruption or reduced capacity. These impacts, which are proportional to wastewater flow, have both immediate human health and longer-term ecological and economic effects. For that reason, this chapter emphasizes treatment technologies more often associated with larger systems. If the disruption is of a physical nature, such as fire, explosion, or structural failure, disablement of collateral infrastructure, such as drinking water, communication, and power systems may also occur. Chemical disruption, whether intentional or inadvertent, would result in temporary loss of biological treatment capability with no resulting damage to the physical structure of the collection system or the plant.

The large number of manholes in conventional gravity sewer systems offers numerous access points where toxins can be introduced to sewers from where they can be spread to a larger segment of the population and/or upset WWTP processes, which will lead to contamination of receiving waters and downstream drinking water intakes. Pumping stations are less numerous than manholes, but they are vulnerable to explosives. Any destruction of such vital infrastructure can result in sewer backups and massive basement and surface contamination leading to high potential for disease, as witnessed by the after effects of Hurricane Katrina on the Gulf Coast.

Combined sewers are still found in many older US cities, although most are implementing sewer separation or overflow event minimization efforts. The vulnerabilities of these systems are somewhat different from those for sanitary sewers. Because these conveyance systems have so many more access points in the form of stormwater inlets, they are more easily contaminated by a large dose of toxins. However, during rainfall or snow melting events, they carry much more water and thus have a greater potential for dilution during wet weather periods.

All the sewers described above can also be vulnerable to deliberate contamination of groundwater when they are located in deep coarse-grained or karst subsoils that lie above unconfined aquifers. Under these conditions, exfiltration of sewer contents becomes a serious potential vulnerability when these aquifers supply drinking water for municipalities. Newer sewer designs that use pressure and vacuum as motive forces do not have manholes and greatly reduce exfiltration potential, and are thus less susceptible to the above man-made disruptions.

Cessation or reduction of effective treatment at a WWTP may render down-gradient water supplies unsuitable for processing with the existing water treatment facilities. This disruption could be short term or longer term in nature. Short-term disruption would have limited economic and health implications, while longer term disruption may render the receiving water unsuitable as a drinking water supply for the indefinite future. Disruption of or damage to the collection system, on the other hand, could have severe immediate health, economic, and esthetic ramifications to the community. The inability to convey wastewater away from the source can rapidly lead to flooding of homes and accumulation of wastewater on streets and low-lying areas, resulting in direct contact with water-borne pathogens and the spread of disease.

Since the primary removal mechanism for organic contaminants in wastewater is biological degradation, any materials added to the wastewater that can inactivate the biomass will lead to loss of effective treatment. If the introduced material is inhibitory but not toxic, the plant will recover after a relatively short disruption upon dilution and purging of the material. This plant disruption can be longer term if the introduced material is toxic to the biomass, resulting in plant washout and the need for microbial regrowth. This phenomenon can also occur in WWTPs that receive combined wastewater and stormwater and are not equipped to bypass or equalize excessive flow due to major storm events. In such instances, the increased stormwater flow can lead to failure of the final clarifiers and washout of biomass.

The proximity of the traditional collection system to the general population and its accessibility, especially in the case of combined sewer systems, makes it highly susceptible to intentional or accidental disruptions. These disruptions could include blockage with large objects with resultant sewer backup and flooding, structural failure, power failure at lift stations, and introduction of flammable or explosive materials. A fire or explosion could result in localized or widespread infrastructure damage of water supply, communication, power, and transportation systems. Whereas the collection system is dispersed throughout the community and not readily amenable to increased security, the WWTP itself can be more effectively protected from intentional disruption with increased security measures.

## REFERENCES

1. Babbitt, H. E. (1947). *Sewerage and Sewage Treatment*, 6th ed., John Wiley & Sons, New York.
2. Reible, D. D. (1998). *Fundamentals of Environmental Engineering*, Lewis Publishers, Florida.
3. Zimmerman, R. (2002). *Goodbye to Tea in Boston? Water Environment and Technology*, Water Environment Federation, Alexandria, VA, pp. 24–27.
4. U.S. EPA (2005). *EPA's National Section 303d List Fact Sheet*, http://www.epa.gov/waters/national_rept.control.
5. U.S. EPA (2002). *Onsite Wastewater Treatment Systems Manual*, EPA/625/R-00/008.
6. Davis, M. L., and Cornwell, D. A. (2008). *Introduction to Environmental Engineering*, 4th ed., McGraw-Hill, New York.
7. Vesilind, P. A., Peirce, J. J., and Weiner, R. F. (1994). *Environmental Engineering*, 3rd ed., Elsevier-Science, Massachusetts.

8. Hammer, M. J., and Hammer, M. J. Jr. (2004). *Water and Wastewater Technology*, 5th ed., Pearson Prentice Hall, New Jersey.
9. Weiner, R. F., and Matthews, R. (2003). *Environmental Engineering*, 4th ed., Elsevier-Science, Massachusetts.
10. Metcalf & Eddy (2003). In *Wastewater Engineering, Treatment and Reuse*, 4th ed., G. Tchobanoglous, F. L. Burton, and H. D. Stensel, Eds. McGraw-Hill, New York.
11. Viessman, W., and Hammer, M. J. (2005). *Water Supply and Pollution Control*, 7th ed., Pearson Prentice Hall, New Jersey.

# WATER SUPPLY AND WASTEWATER MANAGEMENT REGULATIONS, STANDARDS, AND GUIDANCE

VANESSA M. LEIBY
*The Cadmus Group, Inc., Damascus, Maryland*

## 1 INTRODUCTION

A number of governing authorities pertain to drinking water and wastewater utilities, collectively known as the *Water Sector*. Most provide broad environmental authority that may support security-related activities and initiatives; some specifically address homeland security. Existing authorities provide for public health and environmental protection measures; identify and regulate hazardous chemical, radiological, and biological substances; provide for worker safety; and ensure that the public receives information about water quality and chemical hazards. These laws also provide enforcement authorities for the US Environmental Protection Agency (EPA) and state primacy agencies and permitting authorities that implement many of EPA's environmental laws. New security-related directives and authorities address collection of asset-specific information, further promote information sharing and protection, require vulnerability assessments and development of emergency response plans (ERPs) for certain sizes of community water systems (CWSs), and encourage or require identification of protective strategies and implementation of protective programs. Unless otherwise noted, the authorities identified in this article apply to drinking water and wastewater utilities. Pertinent authorities will be described in several broad categories: (i) presidential directives; (ii) general homeland security laws; (iii) drinking water and wastewater environmental laws; (iv) other environmental laws that may impact the Water Sector, and (v) laws that apply to access to information.

## 2 PRESIDENTIAL DIRECTIVES

The President of the United States has issued a series of Presidential Directives relating to matters pertaining to homeland security. The first directive, Presidential Decision Directive 63, was issued in May, 1998, and set the administration's policy on critical infrastructure protection. Since that time, the President has issued 15 additional Homeland

Security Presidential Directives (HSPDs), a number of which relate to the Water Sector. The Directives most pertinent to the Water Sector are discussed in more detail below. More information on all the Directives can be found at http://www.dhs.gov/xabout/laws/editorial_0607.shtm [1].

### 2.1 Presidential Decision Directive 63

In May, 1998, Presidential Decision Directive 63 (PDD-63) was signed. This directive set the administration's policy on critical infrastructure protection (CIP), identified key sectors, and assigned lead agencies for sector liaison. EPA was designated the lead for the Water Sector, working in cooperation with other federal agencies and the public and private sectors. PDD-63 also authorized the development of Information Sharing and Analysis Centers (ISACs) for each sector to serve as a mechanism for gathering, analyzing, and disseminating appropriate security-related information among the public and private sector and the government. The complete text of PDD-63 can be found at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm [2].

### 2.2 Homeland Security Presidential Directive/HSPD-7 (Critical Infrastructure Identification, Prioritization, and Protection—December 17, 2003)

This directive establishes a national policy for federal departments and agencies to identify and prioritize U.S. critical infrastructure and key resources to protect them from terrorist attacks that could:

- cause catastrophic health effects of mass casualties comparable to weapons of mass destruction;
- impair the ability of federal departments and agencies to perform essential missions or ensure the protection of public health and safety;
- undermine state and local government capacities to maintain order and deliver minimum essential public services;
- damage the Water Sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
- have a negative impact on the economy through the cascading disruption of other critical infrastructure or key resources;
- undermine public morale and confidence in our national economic and political institutions.

The Secretary of Department of Homeland Security (DHS) is charged with integrating and coordinating implementation efforts among federal departments and agencies, state and local governments, and the Water Sector. The Secretary is to establish uniform policies, approaches, guidelines, and methodologies for integrating infrastructure protection and risk management activities within and across sectors and developing metrics as part of a national plan for critical infrastructure and key resources protection. The Secretary also maintains an organization to serve as a focal point for the security of cyber space, and prepares an annual federal research and development plan to support this directive. Federal agencies are required to work with state and local governments and the Water Sector to accomplish these objectives, and are instructed to appropriately

protect information associated with carrying out this directive. The directive focuses on critical infrastructure and key resources that, if exploited, could cause catastrophic health impacts or mass casualties. It identifies EPA as the Sector-Specific Agency (SSA) for the Water Sector (drinking water and wastewater systems) and calls on SSAs to:

- identify, prioritize, and coordinate infrastructure protection activities within their sectors;
- collaborate with relevant federal departments and agencies, state and local governments, and the Water Sector, and conduct or facilitate vulnerability assessments of the sector;
- encourage development of risk management strategies to protect against and mitigate the effects of an attack;
- promote the continued development of information sharing and analysis mechanisms, in collaboration with the Water Sector.

To implement this directive, EPA, in coordination with its Water Sector partners, created the Water Sector-Specific Plan (Water SSP), a broad-based critical infrastructure protection implementation strategy that depicts the mission, protective efforts, research priorities, indicators of progress, and necessary actions to improve the protection of the Nation's drinking water and wastewater utilities. A copy of the Plan can be found at http://www.epa.gov/safewater/watersecurity/pubs/plan_security_watersectorspecificplan.pdf [3]. More information on HSPD-7 can be found at http://www.dhs.gov/xabout/laws/gc-1214597989952.shtm [4].

### 2.3 Homeland Security Presidential Directive/HSPD-8 (National Preparedness—December 17, 2003)

This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies, through the development of a national domestic all-hazards preparedness goal. It provides for state grants to build—through planning, training, and exercises—the capacity of first responders to react to terrorist events. Funds can also be used to purchase equipment. States are required to develop state-specific plans. The directive also calls for the development of quantifiable performance measures. The text of this directive can be found at http://www.dhs.gov/xabout/laws/gc-121544427124.shtm [5].

### 2.4 Homeland Security Presidential Directive/HSPD-9 (Defense of United States Agriculture and Food—January 30, 2004)

This directive establishes a national policy to defend the agriculture, water, and food system against terrorist attacks, major disasters, and other emergencies. It calls on EPA and other federal agencies to:

- build upon and expand current monitoring and surveillance programs for public health and water quality, which provide early detection and awareness of disease, pest, or poisonous agents;

- develop nationwide laboratory networks for water quality, which integrate existing federal and state laboratory resources;
- develop and enhance intelligence capabilities to include collection and analysis of information concerning threats, delivery systems, and methods that could be directed against the Water Sector;
- accelerate and expand countermeasure research, and development of methods for detection, prevention technologies, agent characterization, and dose–response relationships for high-consequence agents.

To implement HSPD-9, EPA has created a Water Security Initiative to design, deploy, and evaluate a model contamination warning system for drinking water security; developed a Drinking Water Laboratory Response Preparedness Project to develop and implement regional laboratory response plans for each of EPA's 10 Regions; and created a Water Laboratory Alliance to provide drinking water utilities with an integrated nationwide network of laboratories with the analytical capabilities and capacity to support monitoring and surveillance, response, and remediation to intentional and unintentional drinking water contamination events involving chemical, biological, and radiological contaminants. More information on these initiatives can be found at http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm [6], http://www.epa.gov/safewater/watersecurity/pubs/fs_watersecurity_dwlabresponseproject.pdf [7], and http://www.epa.gov/safewater/watersecurity/pubs/fs_watersecurity_waterlaballiance.pdf [8], respectively. More information on HSPD-9 can be found at http://www.dhs.gov/xabout/laws/gc-1217449547663.shtm [9].

### 2.5 Homeland Security Presidential Directive/HSPD-10 (Biodefense for the 21st Century—April 24, 2004)

This directive provides a comprehensive framework for the nation's biodefense. It builds on past accomplishments, specifies roles and responsibilities, and integrates the programs and efforts of various communities—national security, medical, public health, intelligence, diplomatic, agricultural, and law enforcement—into a sustained and focused national effort against threats from biological weapons. The directive focuses on threat awareness, prevention and protection, surveillance and detection, and response and recovery. Specific direction to departments and agencies to carry out this biodefense program is contained in a classified document. More information on this Directive can be found at http://www.dhs.gov/xabout/laws/gc-1217605824325.shtm [10].

## 3 GENERAL HOMELAND SECURITY LAWS

In addition to specific Presidential Directives, there are a number of general homeland security laws that provide for the necessary structure to support and implement these initiatives. The principal laws are discussed below.

### 3.1 Homeland Security Act of 2002, P.L. 107–296

This act created the DHS by bringing together a number of independent agencies to analyze intelligence and coordinate security research across government, academia, and the private sector.

Provisions encourage partnerships between Government and the Water Sector to better protect civilian infrastructure, and to create volunteer teams to help local communities respond to attacks on information systems and communication networks. Section 505 requires the Secretary of Homeland Security to provide funds to EPA for homeland security planning, exercises and training, and equipment. More information about the Law can be found at http://www.dhs.gov/xlibrary/assets/hr-5005-enr.pdf [11].

### 3.2 Critical Infrastructure Information (CII) Act of 2002

The Critical Infrastructure Information (CII) Act of 2002, defines critical infrastructure information, and provides for the development of programs to protect such information, particularly information submitted voluntarily. The act also defines information sharing and analysis organizations.

Under this act, DHS has created the Protected Critical Infrastructure Information (PCII) Program that is designed to encourage public and private industry, and others with knowledge about critical infrastructure, to share sensitive and proprietary business information with the Government. The focus of this program is: (i) analyzing and securing critical infrastructure and protected systems; (ii) identifying vulnerabilities and developing risk assessments; and (iii) enhancing recovery-preparedness measures. Information submitted, if it satisfies the requirements of the Critical Infrastructure Information Act of 2002, is protected from public disclosure under (i) the Freedom of Information Act; (ii) state and local disclosure laws, and; (iii) use in civil litigation.

More information about PCII can be found at http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm [12].

## 4 DRINKING WATER AND WASTEWATER ENVIRONMENTAL LAWS

The following laws govern the regulation of drinking water and wastewater systems in the U.S. While the discussion relates primarily to EPA, it is important to note that state governments most often have direct jurisdiction over drinking water and wastewater systems, and that state governments are most involved in fostering security at the local level through primacy agencies and permitting authorities. In order to obtain primacy, states and tribes must adopt regulations for contaminants that are no less stringent than the regulations promulgated by EPA.

### 4.1 Safe Drinking Water Act, 42 U.S.C. §§300F-300J-26 (Drinking Water)

The general provisions of the SDWA provide a basis for drinking water security by protecting the quality and underground sources of drinking water. To protect the quality of public drinking water, EPA establishes regulations for national primary and secondary drinking water standards. States may receive primacy from EPA to administer the safe drinking water program if they adopt regulations no less stringent than the federal government's, and meet other conditions, as described below.

- Have regulations for contaminants that are no less stringent than the regulations promulgated by EPA.
- Adopt, and implement procedures for the enforcement of state regulations;

- Maintain an inventory of public water systems in the state.
- Have a program to conduct sanitary surveys of the systems in the state.
- Have a program to certify laboratories that will analyze water samples required by the regulations, and identify a laboratory that is certified by EPA that will serve as the state's principal lab.
- Have a program to ensure that new or modified systems will be capable of complying with state primary drinking water regulations.
- Have adequate enforcement authority to compel water systems to comply with national primary drinking water regulations, including:
  - the authority to sue in court;
  - the right to enter and inspect water system facilities;
  - the authority to require systems to keep records and release them to the state;
  - the authority to require systems to notify the public of any system violation of the state requirements;
  - the authority to assess civil or criminal penalties for violations of the state primary drinking water regulations and public notification requirements.
- Have adequate record keeping and reporting requirements.
- Have variance and exemption requirements as stringent as EPA's, if the state chooses to allow variances or exemptions.
- Have an adequate plan to provide for safe drinking water in emergencies such as natural disasters.
- Adopted authority to assess administrative penalties for violations of their approved primacy program.

The statute applies to public water systems (PWSs)—systems for the provision of water to the public for human consumption through pipes and other constructed conveyances including federal facilities, such as military bases and hospitals, and other sites with their own drinking water systems. Drinking water programs most applicable to water security are as follows.

- *State wellhead protection.* This program provides that states establish programs to protect wellhead areas (i.e. the surface and subsurface areas surrounding water wells or well fields supplying a PWS) from contamination.
- *Source water protection.* The EPA must develop guidance for states to carry out source water assessment programs. States must delineate the source water areas of all PWSs, and identify actual or potential sources of contamination. Program elements include risk reduction (delineation and source inventories), risk ranking and screening (susceptibility analyses), risk management measures (prevention programs), and preparation for unexpected drinking water supply emergencies (contingency planning).
- *Protection of underground sources of drinking water.* The EPA must promulgate regulations for state underground injection control (UIC) programs to prevent underground injection that endangers drinking water sources.
- *Sanitary surveys.* States conduct regular sanitary surveys of PWSs. A sanitary survey entails a review of the water system's assets, distribution system plans and

maps, routine operation and maintenance (O&M) records, monitoring and sampling plans, and operator certification status.

- *Emergency powers.* The EPA is authorized to take necessary precautions upon receiving information that contamination of a PWS or underground water source may present an imminent and substantial danger to human health, and that appropriate state and local authorities have not acted to protect human health.
- *Maintaining records and monitoring.* Suppliers of potable water, and others subject to the requirements of the act, may be required by the EPA administrator to maintain records and conduct monitoring.
- *Public water system supervision grant program.* Helps states to implement drinking water programs to protect public health. These grants are used by state drinking water program administrators to monitor drinking water quality, conduct sanitary surveys, enforce drinking water standards, and provide technical assistance to local communities. Separate security grants have been provided to states to help focus and direct state-level security initiatives.
- *National drinking water standards.* As noted above, EPA is authorized to establish regulations for national primary and secondary drinking water standards, in order to protect the quality of public drinking water. Use of treatment techniques and technologies may be a requirement under some drinking water regulations, as well as monitoring requirements (see "Maintaining records and monitoring," above). In addition, EPA may establish an interim drinking water standard for a contaminant to address an urgent threat to public health, and may publish health advisories (which are not regulations) or take other appropriate actions for contaminants not subject to any national primary drinking water regulation.
- *Public Health Security and Bioterrorism Preparedness and Response Act, P.L. 107–188.* Also referred to as the *Bioterrorism Act of 2002* —see text below.

The text of the SDWA can be found at http://epw.senate.gov/sdwa.pdf [13].

### 4.2 Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Public Law 107–188 (Drinking Water)

Among other provisions, this act amends the SDWA by inserting Title IV—*Drinking Water Security and Safety* into Title XIV of the Public Health Services Act as sections 1433, 1434, and 1435. It requires the following activities:

- The EPA must provide to community water systems (CWSs) baseline probable-threat information required to complete vulnerability assessments.
- Each CWS serving 3300 or more persons must conduct a vulnerability assessment, certify its completion, and submit a copy of the assessment to EPA, according to a specified schedule.
- Each CWS serving 3300 or more persons must prepare or revise an emergency response plan that incorporates the findings of the vulnerability assessments, and must certify to EPA that the system has completed such a plan within six months of completing a vulnerability assessment.
- The EPA must develop a protocol to protect this information.

- The EPA must develop vulnerability assessment guidance for systems serving fewer than 3300 persons.
- The EPA must conduct research studies in the following:
  - Prevention, detection, and response to the intentional introduction of contaminants into CWSs and their source water.
  - Methods and means by which terrorists could disrupt the supply of safe drinking water or act against drinking water infrastructure.
  - Methods and means by which alternative supplies of drinking water could be provided in the event of the destruction, impairment, or contamination of PWSs.

The EPA has supported the development of a suite of vulnerability (risk) assessment tools for drinking water and wastewater systems of all sizes that address unique and fundamental security concerns. All vulnerability assessments are currently conducted at the utility level. Identification of priority assets is dictated by local conditions, and the determination of threats is identified by the specific Water Sector utility conducting the assessment. As part of the vulnerability assessment, utilities develop an inventory of system assets, including, but not limited to, physical, cyber, information technology, and personnel components, and identify which assets are most critical to the system's mission. To further assist Water Sector utilities, EPA coordinates with DHS's National Cyber Security Division to assist with the development of DHS's national strategy to secure cyber space, and to engage the Water Sector in better protecting cyber-assets.

Important to note is that "vulnerability assessment" is the accepted terminology in the Water Sector due to the language of the Bioterrorism Act of 2002. The term is equivalent to the DHS's "risk assessment" since the methodologies developed for the Water Sector considers all the components of risk (consequence, threat, and vulnerability). More information on the Bioterrorism Act of 2002 can be found at http://www.epa.gov/safewater/watersecurity/pubs/security_act.pdf [14].

### 4.3 Federal Water Pollution Control Act (Clean Water Act), 33 U.S.C. §§1251–1387 (Wastewater)

The Clean Water Act (CWA) governs the quality of discharges to surface and ground water. It establishes national technology-based standards for municipal waste treatment, and numerous categories of industrial point-source discharges (discharges from fixed sources, such as pipes and ditches) requires states, and in some cases tribes, to enact and implement water quality standards to attain designated water-body uses; addresses toxic water pollutants; and regulates dredge-and-fill activities and wetlands. The act provides a number of enforcement authorities for EPA, and states that have accepted permitting authority. The statute also applies these requirements to federal facilities, such as military installations and Department of Energy sites. Programs most applicable to security include:

- *Prohibition of discharges into waters of the United States.* Except as permitted by the act, the discharge of any pollutant by any person is unlawful. These discharges include the discharge into navigable waters of any radiological, chemical, or biological warfare agent; high-level radioactive waste; and medical waste. This provision authorizes the National Pollutant Discharge and Elimination System (NPDES) program.

- *Toxic and pretreatment effluent standards.* The EPA must identify toxic pollutants for which the application of best available technology (BAT) is required. In addition, EPA must promulgate pretreatment standards for pollutants that are not susceptible to treatment by publicly owned treatment works (POTWs) but are introduced into POTWs, and for pollutants that would interfere with the operation of such treatment works. The national pretreatment program is authorized by this provision.
- *Oil and hazardous substance liability.* The EPA is required to develop a list of hazardous substances (other than oil) that present an imminent and substantial danger to the public health or welfare. Any person in charge of a vessel or facility must, as soon as that person has knowledge of any unlawful discharge of oil or hazardous substance, notify the Federal government.
- *Imminent and substantial endangerment.* When EPA receives notice that a pollution source presents imminent and substantial endangerment to human health or livelihood, it may sue for the immediate restraint of anyone causing or contributing to the pollution, or take any other action necessary.

Information on the CWA can be found at http://epw.senate.gov/water.pdf [15].

## 5 OTHER ENVIRONMENTAL LAWS THAT IMPACT THE WATER SECTOR

In addition to laws that regulate the Water Sector directly, other environmental laws give EPA authority to take various actions that impact water security. These laws are described below.

### 5.1 Toxic Substances Control Act (TSCA), 15 U.S.C. §§ 2601–2692

TSCA addresses risks to public health and the environment from existing and new chemical substances, any number of which could be used to contaminate a water supply. It establishes a framework for identifying potentially harmful chemical substances, and controlling their use through a variety of regulatory tools. These tools include, screening new chemical substances, testing existing substances, labeling and record keeping, and restricting activities involving substances that present unreasonable health or environmental risks. The act also gives EPA the authority to address imminent hazards.

### 5.2 Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA), 7 U.S.C. §§ 136 et seq.

The primary focus of Federal Insecticide, Fungicide, and Rodenticide Act (FIFRA) is to provide federal control of pesticide distribution, sale, and use. Under FIFRA, EPA studies the consequences of pesticide use, and requires users (farmers, utilities, and others) to register when purchasing pesticides. Users must also take exams for certification as applicators of pesticides. All pesticides used in the United States must be registered (licensed) by EPA. Registration ensures that pesticides will be properly labeled and will not cause unreasonable harm to the environment if used according to specifications. This law provides authority for EPA to regulate the use of pesticides, including those that could be used to contaminate water supplies.

### 5.3 Comprehensive Environmental Response Compensation, and Liability Act (CERCLA), as amended (Superfund), 42 U.S.C. §§9601–9675

Comprehensive Environmental Response Compensation, and Liability Act (CERCLA) provides for the cleanup of sites where hazardous substances have been released into the environment, or where there is a substantial threat that they will be released. The statute authorizes EPA to clean up and take action to prevent releases of hazardous substances, and to recover costs from parties who may be responsible for a release or threatened release. It gives the President authority to remove hazardous substances, provide for long-term remedial action, and take any other action necessary to protect the public health or welfare, or the environment. It also creates the national contingency plan that establishes the minimum requirements of the hazardous substance response plan including methods of determining priorities among releases based on relative risk or danger to public health or welfare, or the environment.

### 5.4 Resource Conservation and Recovery Act (RCRA), 42 U.S.C. §§6901–6992K, Hazardous Waste Management (Subtitle C)

Resource Conservation and Recovery Act (RCRA) regulates the management and disposal of hazardous and nonhazardous solid waste. Subtitle C of the statute establishes a comprehensive system designed to manage hazardous waste from its creation, through its transportation, to its ultimate disposal. RCRA requires EPA to ban the disposal of certain wastes by injecting them deep under ground, if it may be reasonably determined that such disposal may not protect human health and the environment for as long as the waste remains hazardous.

### 5.5 Occupational Safety and Health Administration (OSHA) Process Safety Management Rule (29 CFR Part 1910.119)

Some water utilities that store or use more than 1500 pounds of gaseous chlorine (or other listed toxic chemicals) are required to comply with this rule. It is designed to prevent or minimize the consequences of catastrophic releases of highly toxic chemicals by requiring facilities to design and operate safe processes, and to plan for emergencies.

### 5.6 Other OSHA Safety Regulations

Several other important Occupational Safety and Health Administration (OSHA) safety regulations apply to work sites containing toxic chemicals such as chlorine gas. These regulations include the OSHA Hazard Communication Standard (29 CFR 1910.1200), Standard for Control of Hazardous Energy (lockout/tag out) (29 CFR 1910.147), Respiratory Protection Standard (29 CFR 1910.134), Personal Protective Equipment Standard (29 CFR 1910.132), and Hazardous Waste Operations and Emergency Response (HAZWOPER) Standard (29 CFR 1910.120).

### 5.7 Clean Air Act (CAA), Section 112(r), 42 U.S.C. §§ 7401–7671q, EPA Risk Management Plan Regulation, 40 CFR Part 68.150

Utility processes containing more than 2500 pounds of chlorine gas are required to implement an accident prevention program, conduct a hazard assessment, prepare and

implement an emergency response plan, and submit to EPA a summary report known as a *risk management plan* (RMP). The RMP must include an executive summary that provides a brief description of the facility's accidental release prevention and emergency response policies, the regulated substances handled at the facility, the worst-case release scenario(s) and alternative release scenario(s), the 5-year accident history of the facility, the facility emergency response program, and planned changes to improve safety at the facility (see 40 CFR Part 68). The full RMP also includes an Off-site Consequences Analysis (OCA), which provides the real extent of a worst-case scenario. Other chemicals that may be present at Water Sector utilities, including ammonia, sulfur dioxide, and chlorine dioxide, also trigger RMP regulatory requirements if they exceed certain threshold quantities.

## 6 LAWS RELATED TO ACCESS TO INFORMATION

The following acts affect the public's ability to obtain information pertaining to the critical infrastructure of drinking water and wastewater systems.

### 6.1 Emergency Planning and Community Right-To-Know Act (EPCRA), 42 U.S.C. §§11001–11050

Emergency Planning and Community Right-To-Know Act (EPCRA) requires states to establish State Emergency Response Commissions (SERCs) that, in turn, are required to establish Local Emergency Planning Committees (LEPCs). The LEPCs are to develop local emergency response plans for releases of extremely hazardous chemicals. Each facility handling extremely hazardous chemicals in excess of threshold quantities must notify the LEPC, and must report any releases over a threshold quantity to the LEPC. If the facility is required under the Occupational Health and Safety Act of 1970 (29 U.S.C. 651 et seq.) to maintain Material Safety Data Sheets (MSDSs), the facility must submit an MSDS for each extremely hazardous chemical on site above the threshold quantity, or a list of such chemicals, grouped by hazard (flammable, toxic, etc.), to the LEPC, the SERC, and the local fire department. The facilities must also submit annual inventories of toxic chemicals managed at the facility over the threshold quantity during the previous year.

### 6.2 Freedom of Information Act (FOIA), 5 U.S.C. §§552–552A

Freedom of Information Act (FOIA) provides a mechanism for members of the public to obtain documents and other information from federal government agencies. The act exempts from disclosure matters relating to national defense or foreign policy, matters specifically exempted by statute, trade secrets and privileged or confidential commercial matters, inter and intraagency memoranda not available by law outside of litigation, certain records or documents compiled for law enforcement purposes, and other categories of sensitive information. Vulnerability assessments provided to EPA under section 1433 of the SDWA, and any information derived from them, are exempt from disclosure under FOIA.

### 6.3 Federal Advisory Committee Act (FACA) 5 U.S.C. §§5—Appendix 01/02/01

The purpose of FACA is to ensure that advice rendered to the executive branch by the various advisory committees, task forces, boards, and commissions formed by Congress and the President is objective and accessible to the public. Committee memberships must be fairly balanced in terms of the points of view represented and the functions to be performed. Committee meetings must be open to the public, and their records must be publicly available.

## REFERENCES


### Drinking Water and Wastewater Environmental Laws

1. Presidential Decision Directives. http://www.dhs.gov/xabout/laws/editorial_0607.shtm, 2008.
2. Presidential Decision Directive—63. http://www.fas.org/irp/offdocs/pdd/pdd-63.htm, 2008.
3. Water Sector-Specific Plan. http://www.epa.gov/safewater/watersecurity/pubs/plan_security_watersectorspecificplan.pdf, 2008.

### EPA Initiatives

4. Homeland Security Presidential Directive—7. http://www.dhs.gov/xabout/laws/gc-1214597989952.shtm, 2008.
5. Homeland Security Presidential Directive—8. http://www.dhs.gov/xabout/laws/gc-1215444247124.shtm, 2008.
6. Water Security Initiative. http://cfpub.epa.gov/safewater/watersecurity/initiative.cfm, 2008.
7. Drinking Water Laboratory Response Preparedness Project. http://www.epa.gov/safewater/watersecurity/pubs/fs_watersecurity_dwlabresponseproject.pdf, 2008.

### General Homeland Security Laws

8. Water Laboratory Alliance. (2008). http://www.epa.gov/safewater/watersecurity/pubs/fs_watersecurity_waterlaballiance.pdf.
9. Homeland Security Presidential Directive—9. http://www.dhs.gov/xabout/laws/gc-1217449547663.shtm, 2008.

### Presidential Directives

10. Homeland Security Presidential Directive—10. http://www.dhs.gov/xabout/laws/gc-1217605824325.shtm, 2008.
11. Homeland Security Act of 2002. http://www.dhs.gov/xbirary/assets/hr-5005-enr.pdf, 2008.
12. Protected Critical Infrastructure Information. (2008). Protection Program. http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm.
13. Safe Drinking Water Act. http://epw.senate.gov/sdwa.pdf, 2008.
14. Bioterrorism Act of 2002. http://www.epa.gov/safewater/watersecurity/pubs/security_act.pdf, 2008.
15. Clean Water Act. http://www.epw.senate.gov/water.pdf, 2008.


## FURTHER READING


Department of Homeland Security Web site. http://www.dhs.gov/index.shtm, 2008.

EPA's National Homeland Security Research Center. Web site http://www.epa.gov/ordnhsrc/, 2008.

EPA Security Web site. http://cfpub.epa.gov/safewater/watersecurity/index.cfm, 2008.

Water Information Sharing and Analysis Center. Web site http://www.waterisac.org/, 2008.

# ROLES OF FEDERAL, STATE, AND LOCAL AUTHORITIES IN WATER INFRASTRUCTURE SECURITY

J. A. ROBERSON
*American Water Works Association, Washington, D.C.*

## 1 INTRODUCTION

Response and recovery from any incident always starts at the local level, but in many cases, when local resources are inadequate, state and/or federal assistance is needed. The Department of Homeland Security (DHS) is now playing a more prominent role in national security and preparedness, and the Environmental Protection Agency (EPA) still plays a significant role as the Sector-Specific Agency (SSA) for the water sector. The federal role is still evolving based on 9/11, and Katrina and other natural disasters, and is not always clear. Much progress has been in clearly defining everyone's roles and responsibilities, but more work is needed to ensure appropriate preparedness, response, and recovery capabilities at all levels.

## 2 BACKGROUND

Similar to all other critical infrastructure (CI), security took on a whole new meaning for water and wastewater utilities after 9/11. These utilities now have to balance security along with all of their other competing priorities such as water quality, finances, efficiency, customer service, infrastructure investment, and others. Utilities have now taken a hard look at the vulnerabilities of the different facilities within their systems, and began to make the investments to lessen those vulnerabilities and to instill a culture of security in the daily operations of the utility. In many instances, utilities developed their vulnerability assessment (VA) with the assistance from consultants, with tools developed to guide them through critical questions. Small utilities often applied a simple checklist method depending on the complexity of their operations.

The approximately 8000 water utilities serving greater than 3300 people were required under the Public Health and Safety Act of 2002 (The Bioterrorism Act, PL 107–188) to conduct VAs, and then revise their emergency response plans (ERPs) based on what they learned in conducting their VAs. The VAs were required to be submitted to the EPA, which had significant constraints placed on it by the Bioterrorism Act on how these VAs could be reviewed and used. The utilities only had to submit a certification of a revised ERP to EPA. Many wastewater utilities also voluntarily conducted similar VAs and revised their ERPs.

In most cases, only a small portion of a typical utility VA might include working with the local fire and police departments to improve response time to the different facilities scattered throughout the local community. Response and recovery from any incident (natural or manmade) always starts at the local level. Utilities and/or local authorities initiate the response as soon as possible, but in many cases, soon find that their own resources are inadequate. State and federal resources will then be brought in to assist the local authorities when local resources cannot handle larger and more significant incidents.

A new paradigm has emerged in the past few years. In essence, utilities need to go beyond internal analysis and internal discussions. Utilities need to go beyond minimal contact with the local fire and police departments and engage with a broad range of outside organizations. Making the time commitment and investing the resources necessary to cultivate working relationships with a variety of other organizations at the local, state, and federal level to develop appropriate response and recovery plans and to improve preparedness capabilities are critical. A utility manager should neither be exchanging business cards on the hood of a pickup truck during an emergency nor should that utility manager be the only utility representative forging such relationships. These relationships need to be established and cultivated before disaster strikes, or before the emergency hits, as part of the utility's preparedness activities. The need for these relationships with different authorities will likely vary based on local, state, and institutional frameworks, but would typically include first responders such as

1. fire, police, and emergency management;
2. public health officials such as city and county health officials and staff at the local hospitals;
3. local and state elected officials, public information staff within these authorities;
4. local and state homeland security staff; and
5. federal agencies such as the Federal Bureau of Investigation (FBI), the Centers for Disease Control and Prevention (CDC), and the DHS.

## 3 THE FEDERAL ROLE

The federal role in water infrastructure has evolved significantly since the initial designation of the water sector as one of the CI sectors in Presidential Decision Directive 63 (PDD-63). This designation occurred during President Clinton's Administration, and some might argue that this action was instigated by the Oklahoma City bombing in April 1995. However, it was more likely a combination of several other issues such as ongoing instability in the Middle East. Homeland security became a significant national priority after 9/11, and more federal resources were directed to this issue. The federal government had to respond to new threats to homeland security, and needed to restructure its preparedness and response functions. The Homeland Security Act of 2002 assigned the responsibility of protecting critical infrastructure/key resources (CI/KR) to the newly created DHS, which was established by Congress in the Homeland Security Act of 2002 (PL 107–296).

The first attempt at a national strategy for homeland security that focused on CI came soon after 9/11 with the Executive Order on Critical Infrastructure Protection issued by President Bush on October 16, 2001. This was followed by *The National Strategy*

*for Homeland Security* that was developed by the Office of Homeland Security in the White House in July 2002. This broad strategy defined homeland security, established a framework for organization, and identified critical mission areas. *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* was more geared specifically toward infrastructure and was released in February 2003.

### 3.1 Homeland Security Presidential Directives

PDD-63 was replaced and supplanted by a series of Homeland Security Presidential Directives (HSPDs) during the Bush Administration. The federal role in infrastructure security is evolving due to these HSPDs, and this evolution clearly has impacts on the water sector. HSPDs typically require DHS and/or other federal agencies to develop some type of plan or take other specific actions. HSPDs do not have the force of law to require utilities (or other entities) to meet specific regulatory requirements—like the Bioterrorism Act. Although several HSPDs ultimately may impact the water sector, HSPD-5, HSPD-7, and HSPD-8 best define the federal role and the relationships between the federal, state, and local roles in water security and for all other CI/KR sectors.

### 3.2 HSPD-5 and the National Response Plan (NRP)

HSPD-5, released on February 28, 2003, addresses management of domestic incidents, such as the natural disasters such as hurricanes or floods, manmade accidents such as the derailment of chemical railcars, and acts of terrorism. In HSPD-5, DHS was directed to develop a new National Response Plan (NRP) to align federal capabilities and resources for an all-hazards approach for domestic incidents. An all-hazards approach refers to developing the capabilities to respond to natural disasters, manmade accidents, and acts of terrorism. For acts of terrorism, federal agencies will generally take the lead role from the homeland security perspective.

The first NRP [1] was released in December 2004. The NRP consists of several major elements, including a Base Plan that details the concept of operations, coordinating structures, and roles and several Emergency Support Function (ESF) Annexes. The ESF Annexes organize and merge capabilities and resources into functions, that is, transportation, and mass care, that are most likely needed during an incident. The water sector is listed under ESF-3, Public Works, and the United States Army Corps of Engineers (USACE) is the lead federal agency for ESF-3. There is an ongoing debate about whether a separate ESF is needed for the water sector because of its role in response and recovery and its potential economic effects within the community [2]. The USACE is typically more geared toward structural assessment and repair and debris removal. In some cases, the USACE has not completely understood that response for the water sector will need to go beyond delivery of bottled water to getting the water and wastewater system back to normal operations in order to restart the economic engine in a community.

Some issues with the initial NRP became apparent in the response to Hurricane Katrina, and some have severely criticized the federal response to that incident. The NRP is currently undergoing a significant revision to better spell out the federal, state, and local responsibilities and to incorporate lessons learned from Hurricane Katrina.

The NRP is a specific application of the National Incident Management System (NIMS). NIMS incorporates the use of the Incident Command System (ICS). ICS has traditionally been used by first responders such as fire and police, and to a degree, is a

new concept for the water sector. The use of an Incident Commander is one of the key ICS concepts. As an incident unfolds, the utility general manager or emergency manager will likely start off as the Incident Commander. But, this will likely change as the utility realizes that their resources are inadequate, and state and federal resources will be brought in to assist the local authorities. Utilities have to be prepared for transitioning the role of Incident Commander to the proper authorities, and that transition could vary from incident to incident. Understanding NIMS and ICS is critical now as any state or local entity receiving federal funding has to be NIMS-compliant.

### 3.3 HSPD-7 and the National Infrastructure Protection Plan (NIPP)

HSPD-7, released on December 17, 2003, addresses the identification, prioritization, and protection of CI for the purposes of preventing, deterring, and mitigating the effects of malevolent acts. Implementing this policy requires a substantial commitment to public–private partnership from both governmental agencies and the owner–operators of the actual infrastructure. Governmental agencies are not typically used to a partnership model, as agencies are typically regulators. Owner–operators are typically wary of the government due to its more traditional regulatory role.

In HSPD-7, the President directed the DHS Secretary to be the lead federal agency for the protection of 17 sectors of CI/KR through the development of a National Infrastructure Protection Plan (NIPP). Those 17 sectors are as follows:

1. Agriculture and Food;
2. Defense Industrial Base;
3. Energy;
4. Public Health and Healthcare;
5. National Monuments and Icons;
6. Banking and Finance;
7. Drinking Water and Water Treatment Systems;
8. Chemical;
9. Commercial Facilities;
10. Dams;
11. Emergency Services;
12. Nuclear;
13. Information Technology;
14. Telecommunications;
15. Postal and Shipping;
16. Transportation Systems; and
17. Government Facilities.

HSPD-7 assigned responsibility for each CI/KR sector to SSAs. DHS is the SSA for the 10 CI/KR sectors numbered 8–17 above. Other federal agencies have been designated as the SSA for sectors numbered 1–7 above on the basis of their expertise and experience with working that individual sector. EPA is the SSA for the water sector due to its expertise with water and wastewater systems and through its regulatory programs under the Safe Drinking Water Act (SDWA) and the Clean Water Act (CWA).

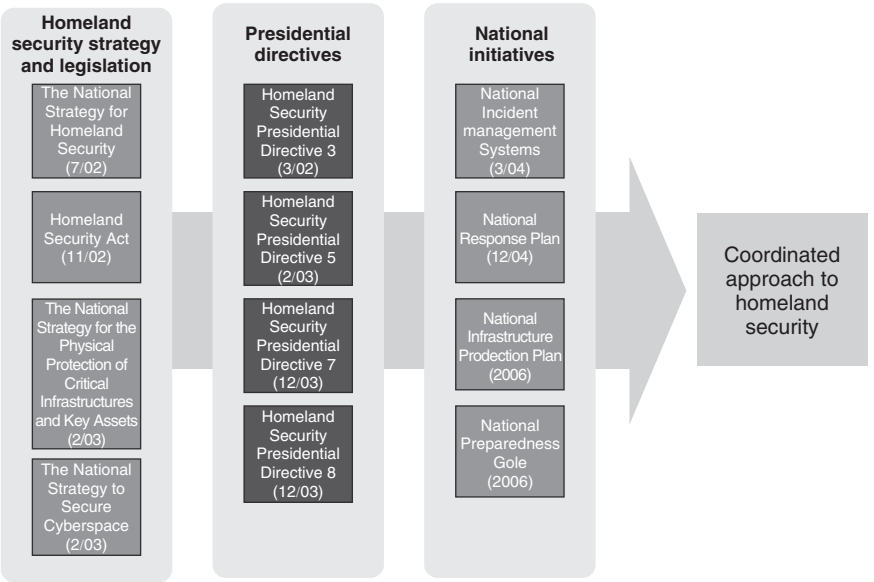



**FIGURE 1** Organization of Homeland Security: related authorities (from page 9, Water Sector-Specific Plan).

Figure 1 shows how the various bills, strategies, plans, and HSPDs fit together to achieve (or accomplish) a coordinated federal approach to homeland security. This is a high-level graphic of an extremely complex process, with multiple parts of multiple organizations moving concurrently toward the common goal of improving homeland security.

In June 2006, the NIPP [3] was completed by DHS. The NIPP is essentially the federal roadmap for the protection of all sectors of CI/KR. The NIPP provides the unifying structure for the integration of all efforts to "build a safer, more secure, and more resilient America". The cornerstone of the NIPP is its risk management framework that ultimately needs to be used by all CI/KR sectors. DHS wants to measure the effectiveness of CI/KR protection efforts to provide constant feedback, and development of those security metrics will be challenging for all of the 17 CI/KR sectors.

### 3.4 Sector Coordinating Councils and Sector-Specific Plans

As part of the implementation of HSPD-7 and as part of this new partnership model, DHS has encouraged each CI/KR sector to develop its own Sector Coordinating Council (SCC) to provide policy input to DHS and its SSA (if the SSA is not DHS). DHS wanted to hear a single voice from each CI/KR sector on the difficult security policy issues. Members of each SCC are selected by the owner–operators to represent the different subgroups of each sector, and each SCC develops its own governing documents. The Water SCC consists of two utility representatives from the following eight organizations:

- American Water Works Association (AWWA);
- American Water Works Research Foundation (AwwaRF);
- Association of Metropolitan Water Agencies (AWMA);

- National Association of Water Companies (NAWC);
- National Rural Water Association (NRWA);
- National Association of Clean Water Agencies (NACWA);
- Water Environment Federation (WEF); and
- Water Environment Research Foundation (WERF).

Staff from the each association serve as nonvoting representatives to the Water SCC and also provide logistical and technical support. These support functions include developing a vision and mission for each sectors and building a Sector-Specific Plan (SSP) and the associated metrics.

For the government side, that is, not the owner–operators, there is a corresponding Government Coordinating Council (GCC) for each CI/KR sector. Each SCC and GCC works with DHS and the appropriate SSA in a partnership, and sometimes that is easier said than done due to the number of parties involved.

After the release of the NIPP in June 2006, each of the 17 CI/KR sectors was required to develop its own SSP by the end of the 2006. All of the individual SSPs were reviewed by DHS and the White House in early 2007, and all of the SSPs were jointly released in May 2007.

The Water SSP has the following four goals:

1. sustain protection of public health and the environment;
2. recognize and reduce risk in the water sector;
3. maintain a resilient infrastructure; and
4. increase communication, outreach, and public confidence.

More detailed objectives have developed under each goal [4]. One of the challenges for the water sector today is the development of metrics that match up to the goals and objectives of the Water SSP. How do you really measure the effectiveness of specific water security and/or preparedness efforts? This question is being debated by all CI/KR sectors, as ultimately, DHS wants metrics from all sectors to be able to evaluate how well it is meeting its goal to "build a safer, more secure, and more resilient America". DHS would like all CI/KR sectors to develop these metrics and then voluntarily report data on meeting these metrics so it can evaluate not only how effective each sector is but also evaluate cross-sector, and then roll up all sectors into a national evaluation.

### 3.5 HSPD-8 and Water and Wastewater Agency Response Networks (WARNs)

HSPD-8, focusing on National preparedness, was also released on December 17, 2003. The purpose of HSPD-8 is to help entities at all levels of government develop and maintain the capabilities to prevent, respond to, and recover from major events or incidents of national significance. A key priority is the expansion of regional collaboration through mutual aid agreements and assistance compacts. A major initiative in the water sector is the expansion of the number of Water and Wastewater Agency Response Networks (WARNs), which is discussed in more detail later.

## 4 THE STATE ROLE

For most natural disasters, the State Emergency Management Agencies (EMAs) and Emergency Operations Centers (EOCs) will typically be the focal point for response and recovery efforts. As previously discussed, federal resources will be brought in to assist the state and local authorities when larger and more significant incidents require additional resources. Seats at the state EOCs are sometimes closely guarded, and utilities may or may not be able to get a seat. The EOC serves as a focal point for matching resources and requirements.

Since 9/11, most states have now established a Homeland Security Office that may or may not be separate from the State EMA, and this sometimes causes differences in priorities. However, these Security Offices are important as they serve as the conduit for federal funding.

The Emergency Management Assistance Compact (EMAC) provides a mechanism for crossing state lines for mutual aid and assistance. EMAC is a State-to-State Compact accessed through the State EMA. The request for equipment and/or personnel must be approved by both the requesting and assisting EMA before any assets can be deployed. EMAC addresses liability and other legal issues that may arise between states during the provision of assistance.

With recent hurricanes and other natural disasters proving that nature is the more likely threat than terrorists, utilities are debating how to balance physical security such as guns, guards, and gates with improved resiliency and response capabilities [5]. The AWWA has developed a white paper [6] to assist states in forming WARNs. This white paper details a 10-step program to form a WARN, and the water sector is holding workshops across the country to expand the number of state-level WARNs. The goal of these networks is "utilities helping utilities". In other words, what can utilities do to help each other in the first three days after an incident while the state and federal resources are being organized. Resources and requirements will be matched through these networks during an incident. The desire by water utilities to "do the right thing" is stimulating the growth in the number of WARNs. The next step in the evolution of WARNs is the formation of a national steering committee to address interstate issues.

## 5 THE LOCAL ROLE

As previously discussed, response and recovery from any incident (natural or manmade) always starts at the local level. Utilities started their effort with the VAs and ERPs required under the Bioterrorism Act. Many utilities are now evolving their ERPs into Business Continuity Plans (BCPs) to address new and emerging issues as potential reductions in workforce from pandemic influenza. In January 2007, DHS's NIMS Integration Center (NIC) recommended that state and local government adopt The National Fire Protection Association (NFPA) 1600: *Standard on Disaster/Emergency Management and Business Continuity Programs* (and other standards) as part of NIMS implementation [7].

Local and/or county EMAs and EOCs are typically the focal point for response and recovery efforts. If possible, utilities should have a seat at the local/county EOC. Utilities

should make the time commitment and invest the resources necessary to cultivate working relationships with the appropriate staff at the state and local EMAs.

## 6 SUMMARY AND CONCLUSIONS

Response and recovery from any incident (natural or manmade) always starts at the local level. Utilities and/or local authorities initiate the response as soon as possible, but in many cases, soon find that their resources are inadequate. State and federal resources will then be brought in to assist the local authorities when local resources cannot handle larger and more significant incidents.

The federal role is not always clear and that role is evolving as the various HSPDs are moving further in the implementation process. Much process has been made, but more work is needed to ensure appropriate preparedness, response, and recovery by the various local and state entities, and by the various federal agencies.

## REFERENCES

1. Department of Homeland Security (2004). *National Response Plan*, www.dhs.gov/nrp December 2004.
2. Roberson, J. A. (2007). Making the Business Case for Water Security and Preparedness. *J. AWWA* **99**(1), 34–36.
3. Department of Homeland Security (2006). *National Infrastructure Protection Plan*, www.dhs.gov/nipp June.
4. Morley, K. M. (2007). A Vision and Direction for Water Sector Security and Preparedness Initiative. *J. AWWA* **99**(2), 38–42.
5. Roberson, J. A., and Morley, K. M. (2006). Water Security: Shifting to an All-Hazards Resiliency Approach. *J. AWWA* **98**(5), 46–47.
6. Morley, K. M., and Riordan, R. (2006). *Utilities Helping Utilities: An Action Plan for Mutual Aid and Assistance Networks for Water and Wastewater Utilities*, AWWA, Denver, www.awwa.org/Advocacy/govtaff.
7. Federal Emergency Management Agency. *NIMS Recommended Standards*, www.fema.gov/emergency/nims/fact_sheet_standards.shtm.

## FURTHER READING

Department of Homeland Security (2004). *National Response Plan*, December Available at http://www.dhs.gov/xprepresp/committees/editorial_0566.shtm.

Department of Homeland Security (2006). *National Infrastructure Protection Plan*, June. Available at http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

Emergency Management Assistance Compact (EMAC). www.emacweb.org.

The White House (2003). *Homeland Security Presidential Directive/HSPD-5, Management of Domestic Incidents*, February 28. Available at http://www.whitehouse.gov/news/releases/2003/02/print/20030228-9.html.

The White House (2003). *Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection*, December 17. Available at http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html.

The White House (2003). *Homeland Security Presidential Directive/HSPD-8, National Preparedness*, December 17. Available at http://www.whitehouse.gov/news/releases/2003/12/20031217-6.html.

Water and Wastewater Agency Response Networks (WARNs). http://dev.awwa.org/Advocacy/Govtaff/Issues/Issue07_Water_Response_Networks.cfm.

Water Sector Coordinating Council (2006). *The First Eighteen Months*, March. http://www.awwa.org/Advocacy/Govtaff/Documents/WSCC_Annual_Report.pdf.

# POTENTIAL CONTAMINATION AGENTS OF INTEREST

ROBERT M. CLARK
*Cincinnati, Ohio*

## 1 INTRODUCTION

There are nearly 60,000 community water supplies in the United States serving over 226 million people. Over 63% of these systems supply water to less then 2.4% of the population and 5.4% supply water to 78.5% of the population. Most of these systems provide water to less then 500 people. In addition, there are 140,000 noncommunity systems that serve schools, recreational areas, trailer parks, etc. [1]. Some of the common elements associated with water supply systems in the United States are as follows:

- *Water source,* which may be a surface impoundment such as a lake, reservoir, river, or ground water from an aquifer;
- *Conventional treatment facilities,* including filtration, which removes particulates and potentially pathogenic organisms, followed by disinfection, primarily for surface supplies;
- *Transmissions systems,* which include tunnels, reservoirs, and/or pumping facilities, and storage facilities;
- *Distribution systems,* carrying finished water through a system of water mains and subsidiary pipes to consumers.

## 2 WATER SYSTEM VULNERABILITY

Water systems are spatially diverse and therefore, have an inherent potential to be vulnerable to a variety of physical, chemical and biological threats that might compromise a

systems' ability to reliably deliver safe water. Community water supplies are designed to deliver water under pressure and generally supply most of the water for firefighting purposes. Therefore a loss of water or a substantial loss of pressure could disable firefighting capability, interrupt service, and disrupt public confidence. This loss might result from sabotaging pumps that maintain flow and pressure, or disabling electric power sources that might lead to long term disruption. Many of the major pumps and power sources in water systems have custom-designed equipment and could take months or longer to repair and/or replace [2].

Major areas of vulnerability include the following:

- raw water source (surface or groundwater);
- raw water channels and pipelines;
- raw water reservoirs;
- treatment facilities;
- connections to the distribution systems;
- pump stations and valves;
- finished water tanks and reservoirs.

Each of these system elements present unique challenges to a water utility in safeguarding water supply [3].

## 2.1 Physical Disruption

The ability of a water supply to provide water to its customers can be compromised by destroying or disrupting key physical elements of the water system. These elements include raw water facilities (dams, reservoirs, pipes, and channels), treatment facilities, and distribution system elements (transmission lines and pump stations).

Physical disruption may result in significant economic cost, inconvenience, and loss of confidence by customers, but has a limited direct threat to human health. Exceptions to this generalization include (i) destruction of a dam that causes loss of life and property in the accompanying flood wave and (ii) an explosive release of chlorine gas at a treatment plant. Water utilities should examine their physical assets, determine areas of vulnerability, and increase security accordingly. An example of such an action might be to switch from chlorine gas to liquid hypochlorite, especially in less secure locations which decreases the risk of exposure to poisonous chlorine gas. Redundant system components would provide backup capability in case of accidental or purposeful damage to facilities.

## 2.2 Contamination

Contamination is generally viewed as the most serious potential terrorist threat to water systems. Chemical or biological agents could spread throughout a distribution system and result in sickness or death among the consumers, and for some agents the presence of the contaminant might not be known until emergency rooms report an increase in patients with a particular set of symptoms. Even without serious health impacts, just the knowledge that a group had breached a water system could seriously undermine consumer confidence in public water supplies [4].

Accidental contamination of water systems has resulted in many fatalities. Examples of such outbreaks include cholera contamination in Peru [5], *Cryptosporidium* contamination

in Milwaukee, Wisconsin (US) [6], and *Salmonella* contamination in Gideon Missouri (US). In Gideon the likely culprit was identified as pigeons infected with *Salmonella* that had entered a tank's corroded vents and hatches [7].

## 3 MICROBIAL THREATS

Waterborne pathogens have been recognized as a threat to human public health throughout history but the development of drinking water treatment techniques have controlled this threat since the beginning of the twentieth century. Although modern drinking water treatment has virtually eradicated waterborne disease from developed countries, drinking water treatment systems have been identified as a potential security vulnerability.

Water-related microbial pathogens can be categorized as water-based or waterborne pathogens. Water-based pathogens spend part of their life cycle in water to reach and infect a potential host. An excellent example of a water-based pathogen is malaria for which mosquitoes are a vector. Since water-based pathogens are not transmitted totally through water they are not potential agents of bioterrorism.

Waterborne pathogens, however, are those transmitted through ingestion of contaminated water primarily through the fecal-oral route. In this case water acts as a passive carrier of infectious agents. Some waterborne pathogens that can cause problems in drinking water include *Campylobacter jejuni*, pathogenic *Escherichia coli*, *Yersinia enterocolitica*, enteric viruses such as rotavirus, calicivirus, astrovirus, and parasites such as *Giardia lamblia*, *Cryptosporidium parvum* and *Microsporidia* sp. Table 1 provides useful summary information related to these organisms. Some species of environmental bacteria have demonstrated the ability to survive in drinking water biofilms and have been identified as opportunistic pathogens including *Legionella* spp., *Aeromonas* spp., *Mycobacterium* spp., and *Pseudomonas aeruginosa* [8–10].

Bacterial pathogens can cause gastroenteritis, including cramps, diarrhea, nausea, vomiting, chills, and mild fever. Bacterial pathogens are generally sensitive to disinfectants such as chlorine and include the following [2, 3, 8, 14]:

- *Salmonella;*
- *Shigella;*
- *Escherichia coli* O157:H7;
- *Yersinia;*
- *Vibrio;*
- *Campylobacter;*
- *Legionella*.

Viral pathogens can pose a 10- to 10,000-fold higher infection risk then bacteria. Important waterborne viral pathogens include the following:

- *Adenovirus;*
- *Astroviruses;*
- *Hepatitis A;*
- *Hepatitis E;*
- *Norovirus;*
- *Rotaviruses*.

**TABLE 1 Pathogens of Public Health Significance[a,b,c,d,e]**

| Pathogen | Disease | Incubation Period |
|---|---|---|
| *Salmonella bongori and Salmonella enterica* | Salmonellosis | 12–36 h |
| *Salmonella paratyphi A, B, and C* | Paratyphoid fever | 8–14 d |
| *Salmonella typhi* | Typhoid fever | 1–3 wk |
| *Shigella dysenteriae, S. flexneri, S. boydii, and S. sonnei* | Shigellosis (bacillary dysentery) | 1–7 d |
| *Vibrio cholerae* | Cholera | 2–3 d |
| *Vibrio parahaemolyticus* | Gastroenteritis | 8–48 h |
| *Yersinia enterocolitica* | Yersiniosis | 3–7 d |
| *Clostridium perfringens* | — | 10–12 h |
| *Bacillus cereus* | — | 6–24 h |
| *Escherichia coli enteropathogenic* | Endemic diarrhea | 9–12 h |
| Coxsackeivirus | Gastroenteritis | 3–5 d |
| Hepatitis A virus | Hepatitis | 28–30 d |
| Polio virus | Poliomyelitis | 7–14 d |
| *Cryptosporidium sp.* | Cryptosporidiosis | 7 d |
| *Entamoeba histolytica* | Amoebiasis | 2–4 wk |
| *Naegleria fowleri* | Naegleriasis and Acanthamebiasis | 3–7 d |

[a]Abbaszadegan and Alum [8].
[b]Burrows and Renner [11, 12].
[c]Clark and Deininger [2, 3].
[d]American Public Health Association [13].
[e]http://www.bt.cdc.gov/agent/agentlist.asp.

Parasitic pathogens are a significant threat to drinking water supplies. Nearly 20,000 protozoan parasites have been identified of which 20 genera are known to cause diseases in humans some of which include the following:

- *Acanthamoeba*,
- *Cryptosporidium parvum*,
- *Entamoeba histolytica*,
- *Microsporidia*, and
- *Naegleria*.

In general, the most effective mechanism for controlling these pathogens is disinfection, especially with chlorine. Table 2 summarizes the capacity of chlorine for inactivating water-related pathogens based on *CT* values. In calculating *CT*, *C* is the concentration of disinfectant (chlorine) in mg/l and *T* time in minutes. Column 4 contains the *CT* value and the target reduction for a given *CT* is given in Table 5 [8, 15, 16]. However other disinfectants may also be effective. Table 3 summarizes *CT* times for a representative set of microorganisms based on the use of chlorine, chloramines, ozone and chlorine dioxide

**TABLE 2 Inactivation of Microbes using Chlorine[a,b]**

| Bacteria | Temperature (°C) | pH | C × T (mg/l × min) | Percentage Reduction |
|---|---|---|---|---|
| *Campylobacter jejuni* | 25 | 8.0 | 0.5 | 99.99 |
| *E. coli* | 25 | 7.0 | 3.0 | 99.99 |
| *Legionella pneumophila* | 21 | 7.6–8.0 | 17.5 | 99 |
| *Mycobacterium chelonei* | 25 | 7.0 | 42 | 99.95 |
| *Mycobacterium fortuitum* | — | 7.0 | 30 | 99.4 |
| *Mycobacterium intracellulare* | — | 7.0 | 9 | 70 |
| *Salmonella typhi* | 20 | — | 3 | 99 |
| *Shigella dysentriae* | 20–29 | 7.0 | 0.5 | 99.6–100 |
| *Vibrio cholerae S. strain* | 20 | 7.0 | 1 | 100 |
| *Vibrio cholerae R. strain* | 20 | 7.0 | 60 | >5 logs |
| *Yersinia enterocolitica* | 20 | 7.0 | 30 | 92 |
| Adenovirus | 25 | 8.8–9.0 | 0.132 | 99.8 |
| Hepatitis A | 25 | 6 | 0.42 | 99.99 |
| Norovirus | 25 | 7.4 | 22.5 | Not completely inactivated |
| Rotavirus | 25 | 7.4 | 22.5 | 100 |
| *Crytposporidium parvum* | 25 | 7.0 | 7200 | 90 |
| *Entamoeba histolytica* | 22–25 | 7.0 | 50 | 100 |
| *Giardia lamblia* | 25 | 6.0–8.0 | 15 | 100 |
| *Naegleria fowleri* | 25 | 7.3–7.4 | 45 | 99.99 |

[a]Abbaszadegan and Alum [8].
[b]http://www.bt.cdc.gov/agent/agentlist.asp.

[17]. As can be seen, ozone is the most effective disinfectant but it does not maintain a residual, and is therefore of only limited use in protecting a distribution system.

### 3.1 Biological Agents

In addition to general pathogens of concern in water supplies some pathogens can be categorized as biological warfare agents. Table 4 contains a basic listing of potential warfare agents and Table 5 contains potential warfare biotoxins. The biological agents listed in Tables 4 and 5 are not only deadly in their own right but also have the potential to be weaponized. Table 5 provides a general overview of the organisms that might be used in biological warfare.

Some of the organisms that have potential use in bioterrorism are discussed below [2, 3, 11, 12].

*Anthrax.* Anthrax, a highly infectious disease of hooved animals, is easily transmitted to humans. The three recognized forms of disease in humans are cutaneous,

**TABLE 3 Summary of *CT* Value Ranges Inactivation of Various Microorganisms by Chlorine, Preformed Chloramines, Chlorine Dioxide and Ozone [17][a]**

| Microorganism | Free Chlorine pH 6 to 7 | Preformed Chloramine pH 8 to 9 | Chlorine Dioxide pH 6 to 7 | Ozone pH 6 to 7 |
|---|---|---|---|---|
| *E. coli* | 0.34–0.05 | 95–180 | 0.4–0.75 | 0.02 |
| Polio virus-1 | 1.1–2.5 | 768–3740 | 0.2–6.7 | 0.1–0.2 |
| Rotavirus | 0.01–0.05 | 3806–6476 | 0.2–2.1 | 0.006–0.06 |
| Phage $f_2$ | 0.8–0.18 | ND | ND | ND |
| *G. lamblia* | 47–150 | 2200[b] | 26[b] | 0.5–0.6 |
| *G. muris* | 30–630 | 1400 | 7.2–18.5 | 1.8–2.0 |
| *Cryptosporidium parvum* | 7200[c] | 7200[d] | 78[d] | 5–10[c] |

[a]Note: All *CT* values are for 99% inactivation at 5°C except for *Giardia lamblia* and *Cryptosporidium parvum*.
[b]Values for 99.9 % inactivation at pH 6–9.
[c]99 % inactivation at pH 7 and 25°C.
[d]99 % inactivation at pH 7 and 25°C.
ND–no data.

pulmonary, and gastrointestinal. It is caused by a spore-forming bacterium, *Bacillus anthraces*, which has been weaponized for aerosol application and was used by the Japanese Army during World War II to contaminate food and water supplies of Chinese cities [12]. Abdominal pain, fever, vomiting, bloody diarrhea and shock are the principal manifestations of this form of the disease, which has an incubation period of 2–7 days. Anthrax spores are easily removed by any water treatment filter system with pore size $<1$ μm.

*Brucellosis.* Brucellosis is caused by *Brucella melitensis* and *Brucella suis* and because it is contracted through consumption of contaminated milk, water is a potential route of infection.

*Cholera.* Cholera is an acute infectious disease caused by the ingestion of food or water contaminated by the bacterium *Vibrio cholerae*. It was used by the Japanese Army during World War II to contaminate food and water supplies of Chinese cities [11] and is therefore a potential threat for contaminating potable water [3].

*Clostridium perfringens. C. perfringens* is a common organism found in secondary sewage effluent. Since it is commonly a cause of food poisoning it has potential for drinking water contamination.

*Melioidosis.* Melioidosis is caused by the bacillus *Burkholderia* (formerly *Pseudomonas*) *pseudomallei*. Since human disease can be caused by ingestion or by contact with contaminated water, it is a threat via the water route.

*Plague.* Plague is a disease of rodents, both wild and domestic, caused by the bacillus *Yersinia pestis* and transmissible to humans. It is generally considered to be a threat in water as well. Cultures were used by the Japanese Army during World War II to contaminate food and water supplies of Chinese cities [12].

*Coxiella (Q Fever). C. burnetii*, a rickettsial or rickettsia-like organism common among domestic farm animals, causes Q fever in humans and it has been noted that it is possibly transmitted from cattle through raw milk.

**TABLE 4 Biological Warfare Agents[a,b,c]**

| Agent/ Disease | Weaponized | Water Threat | Type of Organism | Infective Dose | Stable in Water | Chlorine Tolerance |
|---|---|---|---|---|---|---|
| Anthrax | Yes | Yes | Bacteria | $6 \times 10^3$ | 2 years | Resistant |
| Brucellocis | Yes | Probable | Bacteria | $10^4$ | 20–72 days | Unknown |
| Cholera | Unknown | Yes | Bacteria | $10^3$ | Survives well | Sensitive |
| *Clostridium perfringens* | Probable | Probable | Bacteria | $10^8$ | Common in sewage | Resistant |
| Glanders | Probable | Unlikely | Bacteria | $3.2 \times 10^6$ | 30 days | Unknown |
| Melioidosis | Possible | Unlikely | Bacteria | Unknown | Unknown | Unknown |
| Plague | Probable | Yes | Bacteria | 500 | 16 days | Unknown |
| Salmonella | Unknown | Yes | Bacteria | $10^4$ | 8 days | Inactivated |
| Shigellosis | Unknown | Yes | Bacteria | $10^4$ | 2–3 days | Inactivated |
| Tularemia | Yes | Yes | Bacteria | $10^8$ | 90 days | Inactivated |
| Fever | Yes | Possible | Rickettsia | 25 | Unknown | Unknown |
| Typhus | Probable | Unlikely | Rickettsia | 10 | Unknown | Unknown |
| Psittacosis | Possible | Possible | Bacteria-like | Unknown | — | Unknown |
| Encephalomyelitis | Probable | Unlikely | Virus | 25 | Unknown | Unknown |
| Enteric viruses | Unknown | Yes | Virus | 6 | 8–32 days | Inactivated |
| Hemorrhagic fever | Probable | Unlikely | | $10^5$ | Unknown | Unknown |
| Smallpox | Possible | Possible | Virus | 10 | Unknown | Unknown |
| Cryptosporidiosis | Unknown | Yes | Protozoa | 132 | Stable | Resistant |

[a]Burrows and Renner, 1989; Burrows and Renner [11, 12].
[b]Clark and Deininger, [2, 3].
[c]http://www.bt.cdc.gov/agent/agentlist.asp.

**TABLE 5 Potential Warfare Biotoxins[a,b,c]**

| Biotoxin | Weaponized | Water Threat | NOAEL | Stable Water | Chlorine Tolerance |
|---|---|---|---|---|---|
| Aflatoxin | Yes | Yes | 75 μ | — | Probably tolerant |
| Anatoxin A | Unknown | Probable | Unknown | — | Probably tolerant |
| Botulinum toxins | Yes | Yes | 0.0004 μg/l | Stable | Inactivated 6 ppm at 20 min |
| Microcystins | Possible | Yes | 1.0 μ/l | Probably stable | Resistant at 100 ppm |
| Ricin | Yes | Yes | 15 μg/l | Stable | Resistant at 10 ppm |
| Saxitoxin | Possible | Yes | 0.4 μg/l | Stable | Resistant at 10 ppm |
| Staphlococcal endotoxins | Probable | Yes | 0.1 μg/l | Probably stable | Unknown |
| T–2 mycotoxin | Probable | Yes | 65 μg/l | Stable | Resistant |
| Tetrodotoxin | Possible | Yes | 1.0 μg/l | Probably stable | Inactivated 50 ppm |

*Note:* NOAEL—No Observed Adverse Effect Level.
[a]Burrows and Renner, 1989; Burrows and Renner [11, 12].
[b]Clark and Deininger [2, 3].
[c]http://www.bt.cdc.gov/agent/agentlist.asp.

*Salmonelloses.* The Salmonellae are pathogens belonging to the enteric bacilli. *Salmonella typhimurium* is often found in outbreaks of food poisoning. It was used by the Japanese Army during World War II to contaminate food and water supplies of Chinese cities [12], and there are reports suggesting that it has been used by terrorists to contaminate drinking water [3].

*Shigellosis.* Shigellosis is a bacillary dysentery caused by the ingestion of various *Shigella* species, in particular *S. dysenteriae*. *Shigella* spp. are most commonly disseminated under conditions of poor hygiene through "direct or indirect fecal-oral transmission." *Shigella* cultures were used by the Japanese Army during World War II to contaminate food and water supplies of Chinese cities [12]. *S. dysenteriae* has been implicated in intentional food contamination and should be considered a threat to potable water supplies.

*Tularemia.* Tularemia is an epizootic disease of animals (especially rabbits and rodents), transmissible to humans, and caused by the bacillus *Francisella tularensis* (formerly *Pasteurella tularensis*). *F. tularensis* has been weaponized in the aerosol form; contaminated water is also a potential source of disease.

*Enteric viruses.* The enteric viruses, commonly transmitted by the fecal-oral route in infants, should be considered potable water threats. Iraq has researched enterovirus 17 (Picornaviridae) and human rotavirus (Reoviridae), both of which cause gastrointestinal disorders, but have apparently not been weaponized.

*Cryptosporidiosis.* Cryptosporidiosis is a gastrointestinal infection resulting from ingestion of the oocysts of a protozoan, *Cryptosporidium parvum*. It is commonly contracted from drinking water contaminated with cattle wastes. Although *C. parvum* has not been weaponized it has been suggested as a potential agent for sabotaging potable water supplies by reason of its infectivity and ready availability [3, 6].

*Anatoxin A.* Anatoxin A, also known as the very fast death factor, is an alkaloid neurotoxin produced by the filamentous freshwater cyanobacteria *Anabaena flos-aquae*. Wild and domestic animals poisoned by anatoxin through ingestion have been observed in the field to be staggering, gasping, and suffering convulsions. Death by respiratory arrest occurs in minutes to hours.

*Botulinum toxins.* Botulinum toxins are derived from protein toxins produced by *Clostridium botulinum* and exist in seven neurotoxic forms. They have been weaponized by Iraq and other countries for aerosol application [3, 18]. To successfully contaminate a potable water supply, a biotoxin even as lethal as the botulinum toxins must be introduced downstream from treatment facilities and be able to survive contact with chlorine. The quantities involved make it impractical to poison large reservoirs.

*Microcystins.* The microcystins are hepatotoxic products of freshwater blooms of cyanobacteria of the *Microcystis* spp., *M. aeruginosa* in particular. Microcystin-LR, also known as the fast death factor, is the most common of the microcystins and presumably the toxin of choice to be weaponized. Although the aerosolized form of microcystin is the most likely threat, ingestion—even from natural sources—must be considered a significant hazard.

*Saxitoxin.* Saxitoxin, the cause of paralytic shellfish poisoning, is produced by the marine dinoflagellate *Gonyaulax*, among others. Saxitoxin is highly toxic by ingestion, more toxic still by injection, and perhaps most toxic by aerosol administration. It has been weaponized for covert purposes. Saxitoxin is water soluble, acid stable, alkaline labile, and stable at normal atmospheric conditions.

*Staphylococcal enterotoxins.* Staphylococcal enterotoxin B (SEB), which has been weaponized, is one of a number of protein toxins produced by bacteria such as *Staphylococcus aureus*. SEB can be either inhaled (aerosolization) or ingested from contaminated water or food, and could be used to sabotage food or low volume water supplies.

*Mycotoxins, T–2.* The T–2 toxin is one of several trichothecene mycotoxins isolated from cereal grains infected with *Fusarium* and some other genera of fungi. Russian experience with infected agricultural products indicates that ingested trichothecenes could impose a deadly threat [12]. Unconfirmed and controversial findings suggest the use of trichothecenes as biological warfare agents in Laos, Cambodia, and Afghanistan. Iraq has investigated the weaponization of trichothecenes. Other trichothecenes, viz., nivalenol, 4-deoxynivalenol, and diacetoxyscirpenol may be present in crude preparations; their toxicities are probably similar to but no greater than that of T–2.

*Tetrodotoxin.* Tetrodotoxin is a potent neurotoxin that has caused the deaths of many humans as a result of consumption of improperly prepared pufferfish. It was investigated as a potential biological warfare weapon and may be sufficiently soluble to present a threat to drinking water.

## 4 CHEMICAL AGENTS

All water supplies are vulnerable to chemical spills. For example, the FMC Corp located in South Charleston, West Virginia caused one of the largest industrial spills in recorded history. The spill consisted of carbon tetrachloride that has serious human health effects. Exposure to very low levels of carbon tetrachloride increases the risk of liver damage and the spill caused the intakes of several water treatment plants on the Ohio River to be closed for several days.

In January 1988, a 4-million gallon oil storage tank owned by the Ashland Oil Company, Inc., split apart and collapsed at an Ashland oil storage facility located in Floreffe, Pennsylvania, near the Monongahela River. The spill released diesel oil into an uncapped storm drain that emptied directly into the river. The oil was carried by the Monongahela River into the Ohio River, temporarily contaminating drinking water sources for an estimated one million people in Pennsylvania, West Virginia, and Ohio, contaminating river ecosystems; killing wildlife; damaging private property; and adversely affecting businesses in the area [19].

### 4.1 Chemical Categories

Hazardous chemicals are categorized by the type of chemical or by the effects a chemical would have on people exposed to it. The categories used by Centers for Disease Control (CDC) are as follows:

- biotoxins;
- blister agents/vesicants;
- blood agents;
- caustics (acids);
- choking/lung/pulmonary agents;
- incapacitating agents;
- long-acting anticoagulants;
- metals;
- nerve agents;
- organic solvents;
- riot control agents/tear gas;
- toxic alcohols;
- vomiting agents.

Biotoxins are discussed under the section on microbial agents and are summarized in Table 5.

*3.1.1 Chemical Non-Warfare Agent*. Several chemical non-warfare agents pose a significant threat to public health if released in drinking water supplies. Some of these compounds are listed in Table 6 and some of them such as sodium cyanide are highly toxic. Column 3 of Table 6 contains $LD_{50}$ values for some of the compounds, which represents a dose at which 50% of a test population experiences lethality. Column 5 contains NOAELs for some of these compounds.

*3.1.2 Chemical Warfare Agents*. There is a broad range of chemical agents that might be utilized in an attack against a drinking water distribution system. Several chemicals

**TABLE 6 Summary of Some Potential Chemical Contaminants[a,b]**

| Common Name | Chemical Name | $LD_{50}$ ($mg \times kg^{-1}$) | NOAEL ($mg \times kg^{-1 \times d-1}$) |
|---|---|---|---|
| Compound 1080 | Sodium fluroacetate | 2–5 | 0.005 |
| Sodium cyanide | NaCN | 2.2 | 20.4 |
| Potassium cyanide | KCN | — | 27 |
| Cyanogen bromide | Cyanogens bromide (CNBr) | 20 | 44 |
| Aldicarb | 2-methyl-2(methylthio) propionaldehyde o-(methylcarbamoyl)oxime | — | — |
| Strychnine | — | 2.35 | — |
| Sodium azide | Sodium azide ($NaN_3$) | — | 3.57 |
| Potassium silver cyanide | Potassium silver cyanide ($KAg(CN)_2$) | 21 | 82.7 |
| Paris green | Copper acetoarsenite | 22 | — |

[a]Field [14].
[b]http:www.bt.cdc.gov/agent/agentlistchem.asp.

agents originally developed for aerosol dispersal during warfare may also be effective through direct ingestion, dermal adsorption, and inhalation during showering. The categories of chemical warfare agents that have potential for contaminating water systems are as follows:

- Incapacitating agents: Incapacitating agents are drugs that make people unable to think clearly or that cause an altered state of consciousness (or unconsciousness).
- Nerve agents: Nerve agent or organophosphate toxicity might result from multiple routes of exposure. These agents cause excess respiratory and oral secretions, diarrhea and vomiting, diaphoresis, convulsions, altered mental status, miosis, bradycardia, and generalized weakness that can progress to paralysis and respiratory arrest.
- Vesicants: The most common clinical effects after exposure to blistering agents or vesicants include dermal, respiratory, ocular and gastrointestinal signs and symptoms. These symptoms are normally manifested within minutes.
- Lung irritants: Lung or pulmonary agents are chemicals that cause severe irritation or swelling of the lining of the nose, throat and lungs.
- Blood agents: Blood agents are poisons that affect the body by being absorbed into the blood.

Table 7 lists some of these agents by type, along with the chemical name, $LD_{50}$ values and NOAELs.

## 5 CHEMICAL OR BIOLOGICAL RELEASE EXAMPLES

Consider two possible toxic releases into a water supply. A pathogenic organism might be *Vibrio cholerae* while a potential deadly chemical that could be released might include sodium cyanide. Possible attack scenarios involving these two agents are discussed in the following sections.

**TABLE 7 Summary of Potential of Chemical Warfare Agents[a,b]**

| Common Name | Chemical Name | Type of Agent | $LD_{50}$ (mg $kg^{-1}$) | NOAEL (μg $kg^{-1}$ $d^{-1}$) |
|---|---|---|---|---|
| Agent BZ | 3-Quinuclidinyl benzilate | Incapacitant | 18–25 | 0.5 |
| Lysergide | 9,10-Didehydro-*N*,*N*-diethyl-6-methylergoline-8$\beta$-carboxamide | Incapacitant | 46 | 0.5–2.0 |
| LSD-based BZ | — | Incapacitant | — | — |
| Mescaline | 3,4,5-Trimethoxy-$\beta$-phenethylamine | Incapacitant | — | — |
| Benzilates | — | Incapacitant | — | — |
| Agent GA (tabun) | Ethyl *N*,*N*-dimethylphosphoramido-cyanidate | Nerve agent | 9.3 | — |
| Agent GB (sarin) | Isopropyl methylphosphonofluoridate | Nerve agent | 43–158 | — |
| Agent GD (soman) | Pinacolyl methyl phosphonofloridate | Nerve agent | 20–165 | — |
| Agent GF | — | Nerve agent | — | — |
| Agent VE | *o*-Ethyl-*s*-[2-(diethylamino)ethyl-] ethylphosphonothiolate | Nerve agent | — | — |
| Agent VG | *o*,*o*-Ethyl-*s*-[2-(diethylamino)ethyl-] phosphorothiolate | Nerve agent | — | — |
| Agent VK | — | Nerve agent | — | — |
| Agent VM | *o*-Ethyl-*s*-[2-(diethylamino)ethyl-] methylphosphonothiolate | Nerve agent | — | — |
| Agent VR-55 | *o*-Isobutyl-*s*-[2-(diethylamino)erthyl-] methylphosphonothiolate | Nerve agent | — | — |
| Agent VX | *o*-Ethyl-*s*-[2-(diisopropylamino)ethyl-] methylphosphonothiolate | Nerve agent | — | — |

| | | | | |
|---|---|---|---|---|
| Sulfur mustard (H or HD) | Bis(2-choloethyl)sulfide | Vesicants | — | — |
| Distilled mustard (DM) | — | Vesicants | — | — |
| Nitrogen mustard (NM) | — | Vesicants | — | — |
| Lewisite (L) | 2-Chlorovinyldichloroarsine | Vesicants | — | — |
| Phosgene oxime (CX) | Dichloroformoxime | Vesicants | — | — |
| Mustard lewisite | — | Vesicants | — | — |
| Phosgene (CG) | — | Lung irritants | — | — |
| Diphogene (DP) | Trichloromethylchloroformate | Lung irritants | — | — |
| PS chloropicrin | Trichloronitromethane nitrochloroform | Lung irritants | — | — |
| Chlorine gas | — | Lung irritants | — | — |
| Perfluoroisobutene | 1,1,1,3,3-Pentafluoro-2-(trifluoromethy)propene | Lung irritants | — | — |
| Hydrogen cyanide (AC) | Hydrocyanic acid (HCN) | Blood gases | — | — |
| Cyanogen chloride | CNCl | Blood gases | — | — |

[a]Field [14].
[b]http:www.bt.cdc.gov/agent/agentlistchem.asp.

*Vibrio cholerae*: Some systems are very vulnerable to microbiological contamination but chlorine residuals are assumed to be protective. There are, however, natural microorganisms that are highly resistant to chlorine as illustrated in Table 5. In March 1991, the US EPA was requested by the Peruvian Ministry of Health to send a team of water supply experts to Peru. The team provided technical support to the field epidemiology staff of the US CDC, which had been in Peru for some time studying a major cholera outbreak.

During the course of the investigation, the EPA team began a series of disinfection experiments on several cholera strains [20–22]. One strain was an isolate recovered from a patient during the Peruvian epidemic. This isolate exhibited both a "rugose" variant as well as a "smooth" type of culture. The smooth culture which is normally associated with cholera exhibits a round smooth colonial morphology. The rugose variant represents an extremely rough form of *V. cholerae* and receives its name from the corrugated appearance of colonies on nonselective agar media. The EPA investigators found that the rugose variant was more resistant to disinfection than the smooth culture.

Chlorine inactivation experiments were conducted in triplicate for each condition as previously described. Both the Gulf Coast and Peruvian smooth strains were readily inactivated by free chlorine. The smooth cultures exhibited classical first order inactivation. At 1 mg/l free chlorine, the smooth strains were inactivated by greater than 4 orders of magnitude in less then 20 s. Rates of inactivation did not differ significantly between the two strains.

Disinfection of the rugose culture displayed a deviation from first order kinetics. After 80 s of exposure to free chlorine in samples containing both smooth and rugose organisms, the smooth strain was inactivated by approximately 3 orders of magnitude. The rate of inactivation of the rugose variant portion of the sample was significantly lower then that of the smooth culture and showed only limited inactivation. These results suggest that there are naturally occurring pathogens that are resistant to chlorination. Such organisms can be cultured and grown in a laboratory with ease and the normal chlorination practices can thus be defeated.

*Cyanide*: On February 2, 2002, four Moroccans were arrested for plotting an attack against the US Embassy in Rome [23]. Their plan was to contaminate the embassy water supply using 10 pounds of powdered potassium ferricyanide. Cyanide is one of the most lethal and rapidly acting poisons known to man. Clinical symptoms can occur within minutes of exposure and exposure can be fatal.

Cyanic compounds can be found in simple or complex forms and simple cyanic forms are more toxic than those in complex forms. The two most notable simple cyanide species are hydrogen cyanide and hydrocyanic acid and cyanogen chloride. Cyanide affects the central nervous system, cardiovascular system, thyroid, and blood.

Drinking water exposure includes the potential for inhalation, dermal absorption and ingestion. Ingestion of drinking water is the most important exposure route. The USEPA's Maximum Contaminant Level (MCL) for cyanide in drinking water is 0.2 mg/l. There are several analytical techniques that detect cyanide in water.

Free chlorine can be used to destroy cyanide and the resulting byproducts are bicarbonate ions and nitrogen gas.

## 6 PUBLIC HEALTH IMPACTS

If a biological or chemical attack should occur in a drinking water distribution system and if no other information is available, it would most likely be identified through the public

health system. Illness would be reported by hospitals, clinics, individual physician's offices, and there might be reports from pharmacies of increased demand for antidiarrhea medications. In addition sudden increases in absentees in schools or a spike in illness in nursing homes might be reported. However, a major challenge would be to differentiate between background illness in the system and the increases associated with an attack. To illustrate this effect data is presented in Figure 1 from a *Salmonella* outbreak identified in Gideon in early December 1993, which affected around 486 of the 1104 residents. Investigators concluded that all the affected residents had consumed municipal water [24].

During November 1993, the residents of Gideon reported objectionable tastes and odors in the residential water supply. The utility superintendent initiated an aggressive and comprehensive flushing program beginning at 8 a.m. on Wednesday, November 10, 1993, flushing all 50 hydrants in the system for 15 minutes each. Unfortunately, the largest municipal tank had apparently been severely contaminated with *Salmonella serovar typhimurium (S. typhimurium)* and the flushing caused the contaminant from the elevated tank to be dispersed throughout the network. This action led to a major waterborne disease outbreak.

On November 12, two days after the flushing event, 44 students from the elementary and the high school combined, were taken ill in Gideon, which was the largest number ill during the outbreak. This sudden spike in illness two days after the flushing was a response to the contaminant outbreak. However, there are only two cases of reported illness from the general population as early as November 12 as can be seen from Figure 1a. The Gideon school also shows a high percent disease incidence value of 70.1%. These observations suggest that some sensitive subpopulations such as school children are more susceptible than adults to illness caused by waterborne contaminants.

Although the nursing home had a lower percent disease incidence of 41.2% as compared to the school, eventually seven nursing home residents died of Salmonellosis. This could be indicative of water usage patterns that are different or it may be that once the nursing home residents contract disease, they are more likely to die.

Nilsson et al. [25] simulated a deliberate biochemical assault of a soluble conservative contaminant to a single node on the main line of a well-calibrated municipal drinking water distribution system. Migration of the contaminant plume was tracked for 55 h throughout the pipe network, and the cumulative mass loading was computed at four target nodes strategically located on looping links and deadend branches. This exercise was repeated for 1000 independent trials to establish a baseline distribution of consumer dose exposures at the target nodes. A battery of simulation experiments was then performed to examine the sensitivity of the nodal load distributions to various system characteristics and water-use patterns. Results from the simulation experiment show that variability in the total mass load received at a node can be apportioned between the variability in the water-use volume and variability in the mean delivered concentration. Overall, however, the operation of the network storage tank had the greatest influence on the nodal mass loadings.

## 7 SUMMARY AND CONCLUSIONS

There are nearly 60,000 community water supplies in the United States including a larger number of noncommunity systems that serve recreational areas, schools and other facilities. All of these systems represent some level of vulnerability. Drinking water

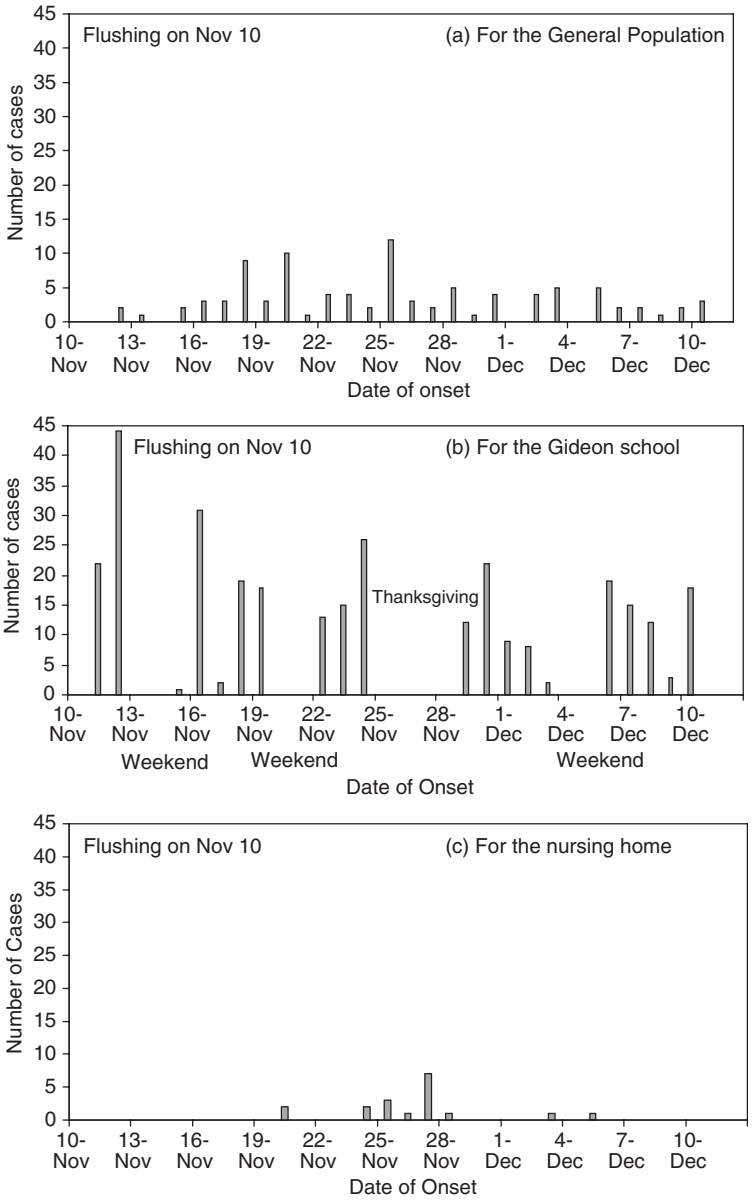



**FIGURE 1** (a)–(c) Disease onset in the Gideon network.

distribution systems are especially vulnerable to both microbial and chemical contamination and there are a number of organisms and chemicals (including biotoxins) that have this potential. In addition there are naturally or easily modified agents that could be a very serious problem should they enter a drinking water distribution system.

Identifying an attack once it has occurred may be difficult and it would most likely be identified through the public health system. Increases in illness especially among sensitive subpopulations might be the only manifestation of a waterborne attack.

It is clear that drinking water systems must be sensitive to the potential for deliberate attacks.

## REFERENCES


1. U.S. EPA. (1999). *25 years of the Safe Drinking Water Act: History and Trends*, EPA 816-R-99-007. Office of Water, December 3.
2. Clark, R. M., and Deininger, R. A. (2001). Minimizing the vulnerability of water supplies to natural and terrorist threats. *Proceedings of the American Water Works Association's IMTech Conference held in Atlanta, GA, April 8-11*, pp. 1–20.
3. Clark, R. M., and Deininger, R. A. (2000). Protecting the Nation's critical infrastructure: the vulnerability of U.S. water supply systems. *J. Contingencies Crisis Manage.* **8**(2), 73–80.
4. Clark, R. M. (2002). Assessing the etiology of a waterborne outbreak: public health emergency or covert attack. In *Proceedings of the First Water Security Summitt*, J. Hatchett, Ed. Haested, Heasted Methods, Waterbury, CT, pp. 170–179.
5. Clark, R. M., Rossman, L., and Wymer, L. (1995). Modeling distribution system water quality: regulatory implications. *J. Water Resour. Plann. Manage.-ASCE* **121**(6), 423–428.
6. Fox, K. R., and Lytle, D. A. (1996). Milwaukee's crypto outbreak investigations and recommendations. *J. Am. Water Works Assoc.* **88**(9), 87–94.
7. Clark, R. M., Geldreich, E. E., Fox, K. R., Rice, E. W., Johnson, C. H., Goodrich, J. A., Bsarnick, J. A., and Abdesaken, F. (1996). Tracking a *Salmonella serovar typhimurium* outbreak in Gideon, Missouri: role of contaminant propagation modeling. *J. Water Supply Res. Technol.-AQUA* **45**(4), 171–183.
8. Abbaszadegan, M., and Alum, A. (2004). Microbiological contaminants and threats of concern. In *Water Supply Systems Security*, L. W. Mays, Ed. McGraw-Hill, New York, pp. 2.1–2.12.
9. Rice, E. W., Clark, R. M., and Johnson, C. H. (1999). Chlorine inactivation of *Escherichia coli* 0157:H7. *Emerg. Infect. Dis.* **5**(3), 461–463.
10. Geldreich, E. E., Fox, K. R., Goodrich, J. A., Rice, E. W., Clark, R. M., and Swerdlow, D. L. (1992). Searching for a water supply connection in the Cabool, Missouri disease outbreak of *Escherichia coli* 0157:H7. *Water Res.* **26**(8), 1127–1137.
11. Burrows, W. D., and Renner, S. E. (1998). *Biological Warfare Agents as Potable Water Threats*. U.S. Army Combined Arms Support Command, Fort Lee , VA, p. 10.
12. Burrows, W. D., and Renner, S. E. (1999). Biological agents as threats to potable water. *Environ. Health Perspect.* **107**(12), 975–984.
13. American Public Health Association. (2000). In *Control of Communicable Disease Manual*, J. Chin, Ed. American Public Health Association, Washington, DC.
14. Field, M. S. (2004). Assessing the risks to drinking-water supplies from terrorists attacks. In *Water Supply Systems Security*, L. W. Mays, Ed. McGraw-Hill, New York, pp. 6.1–6.26.
15. Clark, R. M., Read, E. J., and Hoff, J. C. (1989). Analysis of inactivation of *Giardia lamblia* by chlorine: a mathematical and statistical analysis. *J. Environ. Eng.-ASCE* **115**(1), 80–90.
16. Clark, R. M. (1990). Modeling the inactivation of *Giardia lamblia*. *J. Environ. Eng.-ASCE* **116**(5), 837–853.
17. Adams, J. Q., and Clark, R. M. (2001). Control of microbial contaminants and disinfection by-products (DBPs): cost and performance. *Controlling Disinfection By-Products and Microbial Contaminants in Drinking Water*. U. S. Environmental Protection Agency, Office of Research and Development, Washington , DC 20460, EPA/600/R-01/110.
18. Deininger, R. A., and Meier, P. G. (2000). Sabotage of public water supply systems. In *Security of Public Water Supplies*, NATO Science Series, 2, Environment, Vol. 66, R. A. Deininger, P. Literathy, and J. Bartram, Eds. Kluwer Academic Publishers, Dordrecht, pp. 76–80.

19. Clark, R. M., Vicory, A., and Goodrich, J. A. (1990). The Great Ohio River Oil Spill of 1988: a case study. *J. Am. Water Works Assoc.* **82**(3), 39–44.
20. Rice, E. W., Johnson, C. J., Clark, R. M., Fox, K. R., Reasoner, D. J., Dunnigan, M. E., Panigrahi, P., Johnson, J. A., and Morris, J. G. Jr. (1992). Chlorine and survival of 'rugose' *Vibrio cholerae*. *Lancet* **340**, 740.
21. Rice, E. W., Johnson, C., Clark, R. M., Fox, K. R., Reasoner, D. J., Dunnigan, M. E., Panigrati, P., Johnson, J. A., and Morris, G. J. (1993). *Vibrio cholerae* 01 can assume a 'rugose' survival form that resists killing by chlorine, yet retains virulence. *Int. J. Environ. Health Res.* **3**, 89–98.
22. Clark, R. M., Rice, E. W., Pierce, B. K., Johnson, C. H., and Fox, K. R. (1994). The effects of aggregation on *Vibrio cholerae* inactivation. *J. Environ. Eng.* **120**(4), 875–887.
23. Whelton, A. J., Jensen, J. L., Richards, T. E., and Vladivia, R. M. (2003). The cyanic threat to potable water. *Proceedings of the AWWA Annual Conference and Exposition, June 15–19*.
24. Clark, R. M., Chandrasekaran, L., and Buchberger, S. (2006). Modeling the propagation of waterborne disease in water distribution systems: results from a case study. *Proceedings of the Environmental & Water Resources Institute (ASCE). Cincinnati, Ohio, August 2006*.
25. Nilsson, K. A., Buchberger, S. G., and Clark, R. M. (2005). Simulating exposures to deliberate intrusions into water distribution systems. *J. Water Resour. Plann. Manage.-ASCE* **131**(3), 228–236.

# UNDERSTANDING THE IMPLICATIONS OF CRITICAL INFRASTRUCTURE INTERDEPENDENCIES FOR WATER

RAE ZIMMERMAN

*Institute for Civil Infrastructure Systems (ICIS), New York University, Wagner Graduate School of Public Service, New York, New York*

## 1 INTRODUCTION

Water systems are dependent on and interdependent with many other infrastructures. This is an outcome of functional necessities, spatial proximity to other infrastructures, and economies of scale that have arisen over time. These relationships are growing with the size of the population, generally increased demand for water resources [1, p. 10] particularly for public supplies [2, p. 39], population distribution that has promoted the transmission of water over long distances, the geographic concentration of water-related infrastructure components, and changes in technology for water control and delivery

systems. This article begins by introducing the concept of dependence and interdependence, characteristics of water systems (covering water supply and wastewater treatment) essential to understanding the nature and impact of these relationships, and the relevance of this area of inquiry for security policy, including the allocation of resources for risk management and needs of emergency response. Finally, existing research organized by the major infrastructure sectors to which water is interrelated, how interdependencies can be measured, and recommendations for future research directions are discussed.

Dependence and interdependence as they pertain to infrastructure are usually considered distinct concepts. Rinaldi et al. [3, p. 14] define dependency as a relationship between two infrastructures in a single direction, that is, one infrastructure influences the state of another, whereas interdependency is bidirectional (and implicitly multidirectional) with two (and implicitly more) infrastructures influencing each other. Spatial and functional concentration is a key element associated with interdependence.

Although interdependencies are often beneficial, they may also be disadvantageous if they potentially increase the vulnerability of water systems and the systems that depend on water to threats posed by natural hazards and terrorism. Disruptions in systems upon which water is dependent, whether from natural hazards, terrorism, or accidents, necessarily magnify the effects on water systems. Security strategies now emphasize an all-hazards approach encompassing natural hazards, terrorism, and other intentional attacks given that outcomes or consequences of these different events are often similar. Natural hazards that often drive infrastructure disruptions have been increasing, with the annual rise in federally declared major US disasters estimated at 2.7% per year from 1953 to 2005 [4, p. 382]. Similarly, terrorist attacks disrupting the interdependent infrastructure can magnify the consequences. Although terrorist attacks directly on water infrastructure (as distinct from vandalism or acts of sabotage) are rare in the United States, the threat for water is real enough to prompt the US government to include it in the list of critical infrastructures slated for protection under federal homeland security programs. In the United States, water systems have been compromised in a manner analogous to a terrorist attack, and internationally, terrorist attacks on water have been quite prevalent [5, p. 528].

Interdependencies between the water sector and many other kinds of infrastructure and especially those that comprise emergency services have been identified as a critical element of federal security policy, including resource allocation for risk management. Interdependencies are a centerpiece of the National Infrastructure Protection Plan (NIPP), and are a component of assessing risk to the water sector. For energy and water interdependencies alone, the House and Senate Subcommittees on Energy and Water Development Appropriations requested "a report on energy and water interdependencies, focusing on threats to national energy production that might result from limited water supplies" [6, p. 9]. The US Department of Homeland Security (DHS) issued sector-specific plans (SSPs) to implement the NIPP with input from other agencies. The water sector is one of 17 critical infrastructure sectors to which the plan applies. The water SSP is the longest of the SSPs issued by the US DHS [7]. The water SSP defines dependency and interdependencies in the following way: "Reliance on another asset or sector for the functioning of certain assets is called a dependency; if two assets depend on one another, they are called interdependent" [7, p. 50]. Interdependencies between the communications sector and the water sector are included as an important element in the Communications SSP [8]. The water sector is mentioned in and regulated by over a dozen security and environmental laws combined and addressed in a half dozen federal directives and executive orders [7].

## 2 WATER SYSTEM COMPONENTS AND INTERDEPENDENCY

Water usage patterns provide a context for understanding water infrastructure and its relationship with other sectors. Figures 1 and 2 show the distribution of water use for total water and freshwater, respectively, in the United States (not including return flows, i.e. water consumption).

The type, extent, and impact of dependencies and interdependencies associated with water and other infrastructure vary depending on the water component and the type of technology used for each. Technologies for the provision of water and size of facilities are likely to dramatically alter the way in which other infrastructures are used to provide services for water infrastructure; for example, the Electric Power Research Institute (EPRI) [9, p. 3–5] estimates that unit electricity consumption for surface water treatment and wastewater treatment declines with the size of plant and for a given plant size, the variation in energy consumption for wastewater treatment can vary depending on the type of technology by one and a half to three times. The water-supply sector consists of a very complex system of interconnected resources, facilities, and services. Water sources exist both above and below ground. Large transmission systems, called *aqueducts*, primarily bring surface water supplies to the points of consumption connecting to the holding or storage reservoirs and extensive distribution lines. O'Rourke [10, p. 23] identifies water distribution lines as a type of "lifeline system" interdependent with other infrastructure lifelines noting that during the 2001 World Trade Center (WTC) catastrophe, water line breakages affected other infrastructure lifelines, flooding transit arteries and fiber-optic lines [10, p. 24; 11]. Underground water resources, accounting for about one-third of the

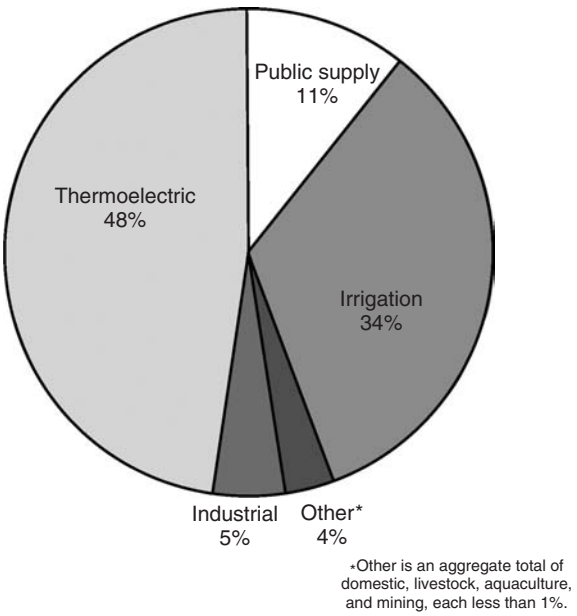



**FIGURE 1** Total water use by type of user, US, 2000. Note: This reflects total water use, and does not take into account return flow. (Source: diagrammed from US Geological Survey Estimated Use of Water in the United States in 2000, Figure 1, May 2004. http://pubs.usgs.gov/circ/2004/circ1268/htdocs/figure01.html.)

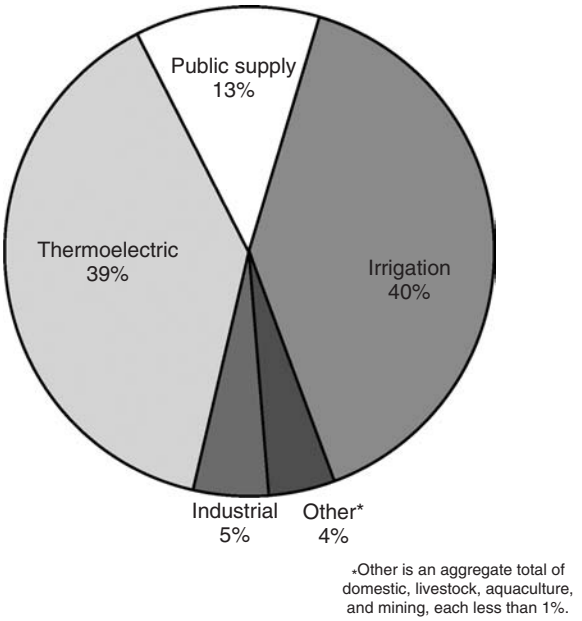



**FIGURE 2** Freshwater use by type of user, US, 2000. Note: This reflects total fresh water use, and does not take into account return flow. (Source: diagrammed from US Geological Survey, Estimated Use of Water in the United States in 2000, Table 2, May 2004. http://pubs.usgs.gov/circ/2004/circ1268/htdocs/table02.html.)

US public water supply [2], serve both large systems and individual users relying on wells usually associated with electricity-driven pumps for supply. Water storage represents another set of infrastructure facilities that interface with and are usually connected with the transmission and distribution systems.

Attributes of a couple of the key components—water and wastewater treatment plants and dams—are highlighted here because of their special significance for interdependencies and their consequences.

### 2.1 Water and Wastewater Treatment Plants

Water-supply plants are extensively distributed or localized throughout the US water supplies or community water supplies, defined under the Safe Drinking Water Act as serving 25 persons or more or having 15 service connections, as of 2004 numbered approximately 161,201 [7, p. 16] and serve 84% of the US population [7, p. 1]. In spite of the extensive geographic coverage of community water-supply facilities in the United States, they are concentrated, reflecting the fact that 45% of the US population is served by only 6.8% of the water-supply facilities [5, p. 531]. Wastewater utilities, regulated under the Clean Water Act, are far more concentrated than water systems, given their generally larger size and urban orientation, and the number of wastewater facilities is about one-tenth the number of water supplies. There are 16,255 regulated publicly owned treatment works [7, p. 19], serving 75% of the US population [7, p. 1]. The relatively greater degree of concentration of wastewater facilities is not accounted for by the lower percentage of people served, and has to do with economies of scale

in treatment technology. The degree of concentration is even greater in both the sectors when one considers that relatively few of these utilities serve the bulk of the population. These characteristics do not take into account private bottled water providers, organized and regulated differently, and is beyond the scope of this article.

## 2.2 Dams

Dams are another area where interdependencies can occur, since the provision of water (excluding individual water systems) usually begins with the use of dams, and the operation and control of dams depends on many other infrastructures. The National Inventory of Dams (NID) records close to 80,000 dams in the United States. The spatial distribution of dams is potentially significant for interdependencies and the vulnerabilities they may pose. At the state level, the number of dams and to a greater extent capacity (total maximum capacity) is highly concentrated: about half of all dams is located in only eight states, and about half of the total maximum dam capacity is located in only five states. The results of an initial analysis of the distribution of the number of dams and total maximum dam capacity as distributed by state in the United States are shown in Figures 3 and 4 [12]. People's dependency on storage of water by dams can in a gross way be portrayed in terms of where dams are located relative to population. The location of dams relative to population and population density is portrayed in Figure 5, indicating a modest relationship with a low, even though not significant, correlation. Numerous activities depend on the water supply that dams provide, reflecting the purpose that these dams serve (Fig. 6). Many dams serve multiple purposes. Analysis of data on the number of dams by primary purpose from the NID indicates that the following activities are dependent upon dams: recreation (33.4%), flood protection including storm water management (15.5%), and fire protection including stock and small pond farms (13.6%). In addition, 9.3% of the dams are used for water supply (as the primary purpose).

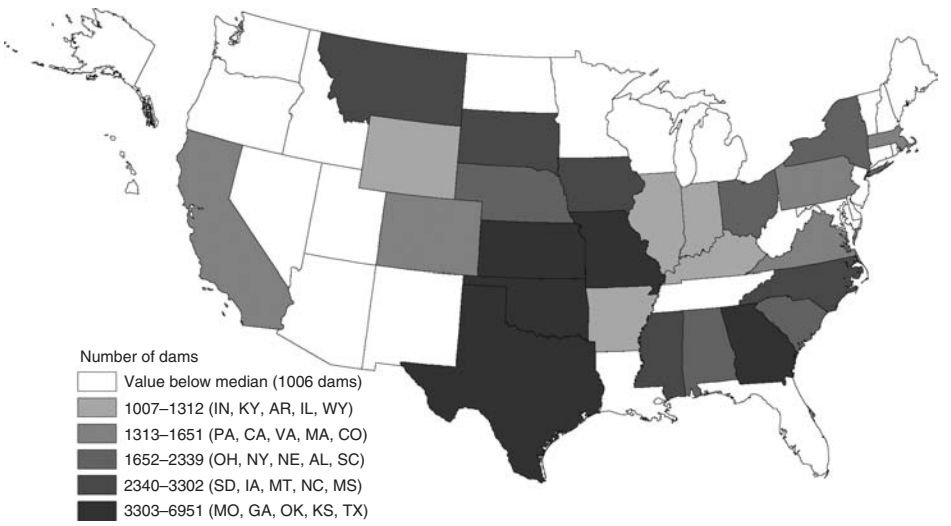



**FIGURE 3** Number of dams by state in the United States, 2006. (Source: mapped from The Stanford National Program on Dam Performance Database as of 2007 By Sara A. Clark, Graduate Research Assistant, NYU-Wagner, Institute for Civil Infrastructure Systems.)

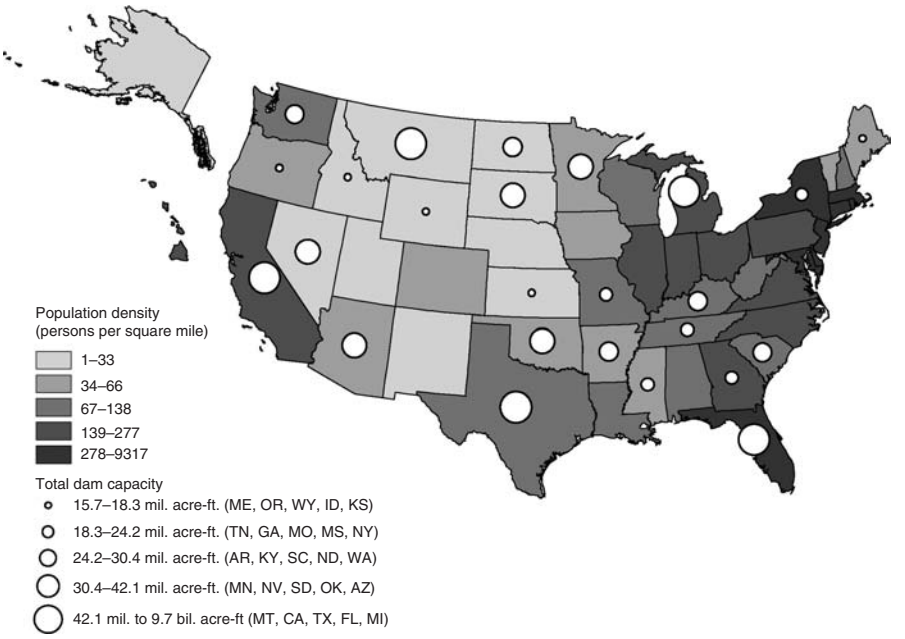



**FIGURE 4** Total dam capacity and state population density in the United States, 2006. (Source: mapped from The Stanford National Program on Dam Performance Database as of 2007; 2000 US Census; US UASI, DHS, 2006 By Sara A. Clark, Graduate Research Assistant, NYU-Wagner, Institute for Civil Infrastructure Systems.)

## 3 TYPES OF INTERDEPENDENCY

Conceptual literature in the infrastructure interdependency area emphasizes functional and geographic interdependencies as major types of interdependency, though other typologies have expanded or refined the number of categories [3, 13].

### 3.1 Geographic Interdependencies: Co-location

Physical interconnections often called *utility bundling* or *utilidors* [14] are enhanced in utility distribution systems by economies of co-location. Transportation is one infrastructure that has important physical linkages to water distribution systems. The water supply for the city of Paris, France, uses bridges to link water from the Left Bank to the Right Bank. A town in New Jersey shares wastewater treatment services with a town in Pennsylvania which involves transporting wastewater across a bridge. During a drought period, New York City constructed a temporary water-supply line, which traveled across the George Washington Bridge to supply water to New Jersey if required. Spatial linkages between water distribution systems and electric power and telecommunication lines are also common. Although these interdependencies provide many advantages and innovations, the proximity of water distribution lines to other infrastructures potentially magnifies vulnerabilities to disruption.

Large cities routinely experience water distribution disruptions, and causes vary. In New York City, environmental factors are a major factor contributing to the average

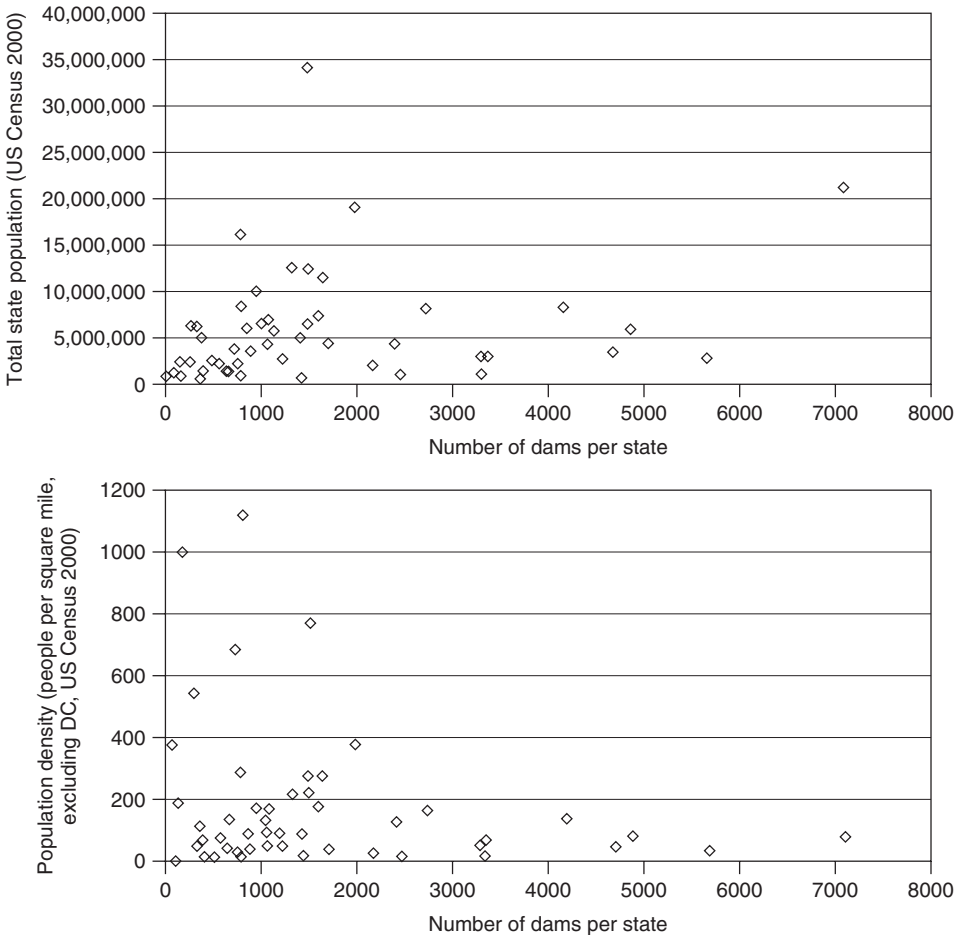



**FIGURE 5** Relationship of number of dams to state population and state population density in the United States, 2006. (Source: graphed from the national inventory of dams as of fall 2006 by Sara A. Clark, Graduate Research Assistant, NYU-Wagner, Institute for Civil Infrastructure Systems.)

of 500–600 water main breakages annually. Water main breakages can disrupt other infrastructure and vice versa. Ways that water disruptions affect other infrastructures include undermining or washing out of street surfaces by water releases, shorting out of electrical lines, and undermining support of gas lines. Ways that water disruptions are caused by other infrastructures include proximity to roads and transit systems [15], vibration, weakening of lines from the undermining of soil support due to construction, being hit by construction equipment, and electrical conductance created by proximity to electrical lines and voltages from trains. An analysis of about 100 cases of multiple infrastructure failures involving water main and other infrastructure breakages found that water main breakages are more commonly initiators of outages in other nearby infrastructures, such as gas main breaks and roadway washouts, than vice versa, but these findings are sensitive to the types of cases in the database [16].

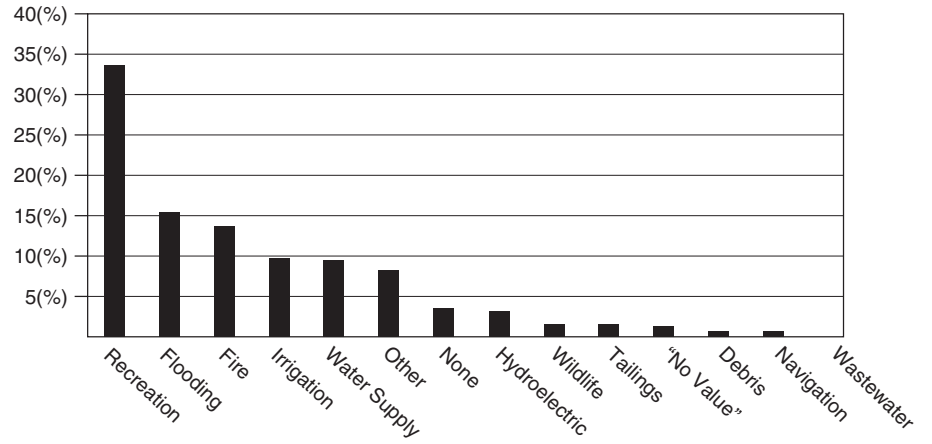



**FIGURE 6** Distribution of dams by purpose in the United States, 2006. (Source: graphed from The Stanford National Program on Dam Performance Database as of 2007.)

### 3.2 Functional Interdependencies by Infrastructure Sector

***3.2.1 The Energy Sector: Water and Energy Interdependencies.*** *Water for energy production*. As shown in Figures 1 and 2, 48% of total water usage and 39% of freshwater withdrawals in the United States in 2000 were accounted for by thermoelectric power [2, p. 35], though when consumption is considered, most of that water is returned and thermoelectric power production in 1995 accounted for 3.3% of consumption [6]. The U.S. Department of Energy (DOE) notes that "of the 132 billion gallons per day of freshwater withdrawn for thermoelectric power plants in 1995, all but about 3.3 billion gallons per day (3%) was returned to the source. While this water was returned at a higher temperature and with other changes in water quality, it was available for further use" [6, p. 17]. Thermoelectric generating plants using open-loop cooling in turn produce 31% of US energy generation [6, p. 18].

*Energy for water production and wastewater treatment*. The dependency of water on electric power has been underscored by a number of very large power outages that threatened water services or actually did bring water production and wastewater treatment to a halt. Electric power outages in California in 2001 nearly stopped major water pumps [3, p. 11; 17]. The August 2003 US and Canada electric power outage stopped wastewater pumps in New York City resulting in untreated water discharges to New York waterways. The same outage disrupted water-supply plants in major cities such as Cleveland and Detroit, and it took those two cities over two times as long to restore their water systems as relative to the amount of time it took to restore electricity (see Section 3). Electric power outages have been increasing at the rate of 7.2% in the United States between 1990 and 2004 [18]. Weather-related events have been dominating other conditions as causes of electric power outages, contributing to an increasing overall outage duration rate of 14% between 1990 and 2004 in the United States and higher rates since the late 1990s [19]. Both these trends are likely to affect water systems. Although water production and movement (for both treatment and supply) account for a small portion of energy produced in the United States, estimated at 4% across all functions [6, p. 25; 9, pp. 1–2], from the perspective of the individual water company, energy figures prominently in water

production, accounting for an estimated 80% of the costs for processing and distribution of municipal water supplies [9, pp. 1–2]. The estimated electricity consumption for fresh water supply in 2000 provided by public water-supply agencies was 30.6 billion kWh per year, and this was estimated to increase up to 45.7 billion kWh per year by 2050, an increase of about 50%, largely driven by population growth [9, p. A-3]. In the water production process, most of the energy is used for pumping and treatment. For example, the East Bay Municipal Utilities District, a water company that provides both water supply and wastewater treatment, uses half of its energy for pumping and treatment (Fig. 7). Its use of energy to acquire raw water is lowered by the fact that it obtains its water resources via gravity.

The transportation of water itself is dependent upon energy in most cases unless transport occurs via gravity. Although no comprehensive information exists on changes in the acquisition of water, it is often cited that water is being accessed from longer and longer distances to meet water needs, especially for urban areas, which will inevitably involve increases in the use of electricity.

***3.2.2 The Transportation Sector: Water, the Chemical Industry, and Transportation.*** The reliance of the water industry on transportation for the provision of chemicals to treat water is a potential vulnerability point, and has contributed to changes in the choice of chemicals. The viability of providing water services by centralized water utilities to dense urban areas is dependent on quality controls, which, in turn, is dependent on chemicals, in particular, chlorine gas for disinfection. Potential attacks on chlorine storage tanks and transport vehicles and accidents involving the transport of chlorine by truck or rail have underscored this as a distinct vulnerability. The water industry performs conversions from chlorine gas to the less vulnerable sodium hypochlorite and ultraviolet disinfection, and this conversion has been estimated to be $647,000 to $13.1 million per plant at about two dozen selected larger plants [20]. An analysis of the conversion cost data reveals a moderate but positive correlation between the cost of conversion and plant size as shown in Figure 8 [12].

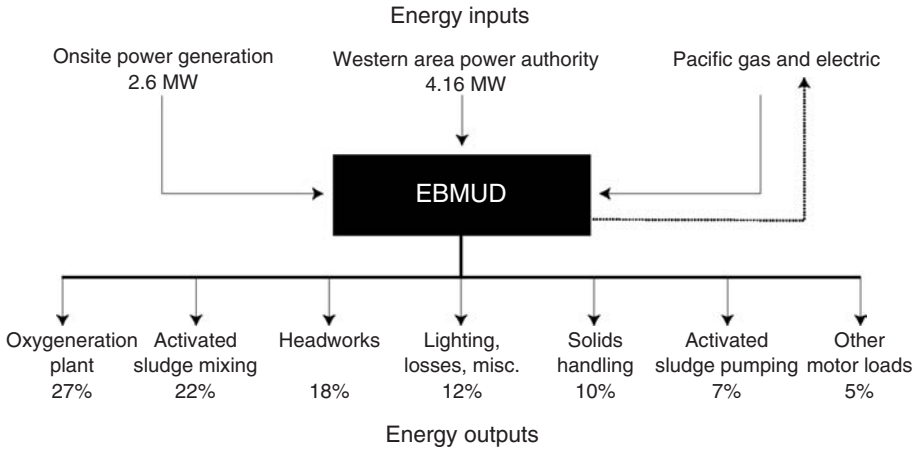



**FIGURE 7** Example of energy use in a water supply and wastewater treatment plant: East Bay Municipal Utility District, California, 2004. (Source: diagrammed from information in Hake, J. M., Gray, D. M. D., and Kallal, S. (2004). Power Diet. California's energy crisis prompts one treatment plant to reevaluate its power intake. *Water Environ. Technol*., May, 37–40.)

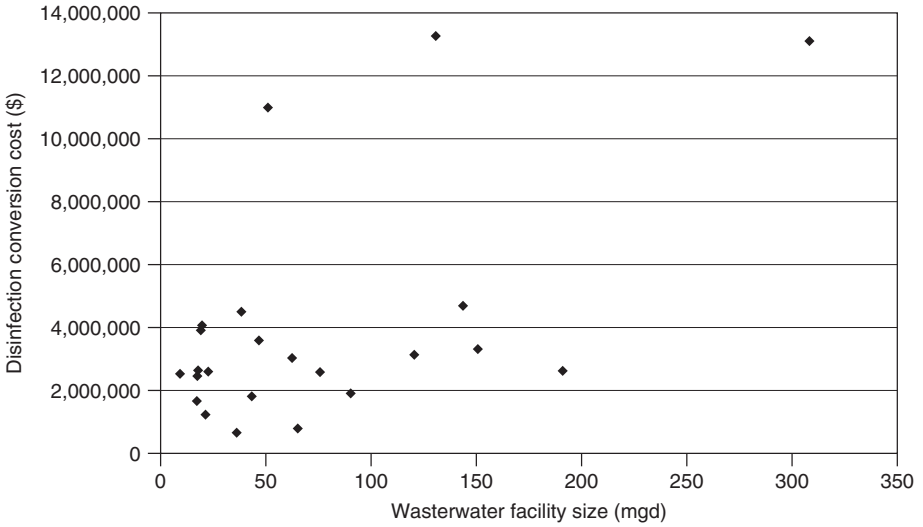



**FIGURE 8** Relationship between wastewater disinfection cost and wastewater facility size for sample facilities, 2007. (Source: analyzed from: US GAO (2007). *Securing Wastewater Facilities: Costs of Vulnerability Assessments, Risk Management Plans, and Alternative Disinfection Methods Vary Widely*. Report to the Chairman, Committee on Environment and Public Works, US Senate, GAO-07-480, March, Table 1, p. 14.)

***3.2.3 Water, Communications, and Information Technology.*** In the water sector, communication and information technologies increasingly control water quality, distribution, and customer interfaces. Information technologies are not only linked to water systems but also provide connections between water and other systems. The dependency of water on communications and information technology is identified in the Communications SSP [8, p. 41]. The effect of disruptions of computerized control systems, such as supervisory control and data acquisition (SCADA), on water systems is noteworthy. For example, in 2001, a hacker disabled the SCADA system operating the wastewater treatment system, Queensland, Australia, causing extensive discharge of sewage [21, p. 9].

Information technology, particularly as used in water applications, has been revolutionized by nanotechnology enabling detection of water chemicals to achieve extraordinary sensitivity. Wireless communication technologies further revolutionized water measurement. In the mid twentieth century, water-supply and wastewater quality standards were largely based on qualitative measures of chemical and biological material, for example, appearance, and by the late twentieth century quantitative standards gradually emerged, for example, expressed in parts per thousand and parts per million. In the twenty-first century those measures often went into the parts per trillion levels. These increasingly more stringent standards were made possible by newer detection technologies [22, p. 80]. As a result of the increase in the quantification of and limits of detection for water quality measures, the water industry has become more dependent on information technologies that are usually very specialized [22, 23]. In 2006, American Society of Civil Engineers (ASCE) and American Water Works Association (AWWA) draft guidelines for water utility security outlined an extensive set of criteria for sensor-based detection, which reflect the greater use of, and hence dependency upon information technologies for water infrastructure [24, Section 9].

## 4 MEASURING FUNCTIONAL INTERDEPENDENCY

When attention was first drawn to the importance and centrality of infrastructure interdependency, it was at a more conceptual and scenario-based level. Over the past decade or more, quantified measures of interdependence have emerged, potentially providing inputs for some of the modeling efforts underway in the area of infrastructure interdependencies. For example, Zimmerman and Restrepo [25, p. 223] applied the ratio of the amount of time it took for electric power to be restored and the time it took for water services to be restored after the August 2003 blackout, finding that the restoration time for the Cleveland water supply and Detroit system was at least two three times, respectively, as long as the time it took for electric power to be restored in those cities, assuming an average electricity outage of 24 h. Dependency on electricity-driven pumps (rather than reliance on gravity systems) accounted for most of the delay in these areas. In other cases, backup power enables water systems to be restored more quickly than relying on the restoration of the general electric power systems [25, p. 226].

## 5 GLOBAL CONSIDERATIONS

Considerable attention has been paid to the dependence of population growth and economic development on resource capacity, and water and the infrastructure that supports it is a key component of the resource base. A concept capturing the resource capacity and usage relationship is the "ecological footprint", defined as utilization of resources by a population or economy relative to the availability or production of that resource [26]. The footprint or imbalance cited by the World Wildlife Fund (WWF) is that the use of resources globally by 2006 has exceeded the ability to regenerate those resources by approximately 25% and the footprint has increased more than three times what it was in 1961 [26, p. 1]. Globally, water withdrawal per capita and the ratio of withdrawals to resources (water stress) vary dramatically from country to country. Globally, the correlation between water stress and the ecological footprint (defined at the country level) is positive at 0.4 and statistically significant; however, if the four countries (in the Middle East and Africa) with extreme values of water stress are eliminated, the correlation between these two factors approaches zero [12]. The ecological footprint appears unrelated to water consumption, however, it seems to be qualified by two factors that are likely to influence water consumption: a country's income and availability of water. With respect to income, the WWF [26, Table 2], for example, notes that high-income countries withdraw almost double the amount of water per capita (957,000 $m^3$ per year) than middle- or low-income communities do (552,000 and 550,000 $m^3$ per year, respectively). However, "water stress" is the same in high- and low-income countries (10% of total resources), whereas it is half of that (5% of total resources) in middle-income countries.

## 6 RESEARCH DIRECTIONS

Water systems depend upon other infrastructures, in particular, electric power, information technologies, and transportation, and indications are that this dependency is likely to increase with technological changes in water production and delivery. Other infrastructures in turn require water to function. These relationships imply that a disruption

in water systems or the infrastructures upon which water is interdependent creates a far more complex system of impacts than is typically portrayed by a direct or single disruption of one infrastructure, and in some cases can magnify the costs to human life, health, and welfare. Thus, a deeper understanding of the ramifications of these interdependencies and their consequences should disruptions occur is needed. A means to quantify these interdependencies and their consequences is a necessary prerequisite to comparing the nature and magnitude of consequences across different types of interdependencies.

Vulnerabilities from interdependencies exist on top of vulnerabilities posed by any condition or performance problems that water infrastructure may experience. Water and wastewater infrastructures nationwide were rated D–, the lowest grade given to any infrastructure area, by the ASCE in its 2005 infrastructure scorecard on the basis of condition alone from noncatastrophic sources [27]. Research is needed on how such ratings and other assessments can incorporate interdependencies and the natural hazard and terrorism context. This will ultimately affect the performance and viability of infrastructures dependent on water.

Global perspectives on water usage are important in addressing a new set of dimensions about dependency and interdependency that impact infrastructure and the people who depend on these systems. Water usage is a key component of the global resource base. An understanding of how patterns of water usage by different kinds of infrastructures influences resource capacity as measured by such concepts as the ecological footprint is critical to linking security with sustainability.

Interdependencies among infrastructures have a special significance in times of emergencies, since emergency response is heavily dependent upon infrastructure. In fact, it is likely that the impact of such interdependencies may become magnified given the compressed time frame necessary for emergency response.

Thus, the scope of the concept of infrastructure interdependencies is expanding and undergoing a transformation to adapt to the needs of security. The water sector represents a key part of that picture.

## ACKNOWLEDGMENTS

The author wishes to acknowledge the assistance of Dr Carlos E. Restrepo, Wendy E. Remington, and Sara A. Clark (for her graphing and mapping of data on dams) of the Institute for Civil Infrastructure Systems at New York University (NYU)'s Wagner School. This research was supported by the US DHS through the Center for Risk and Economic Analysis of Terrorism Events (CREATE), Grant number EMW-2004-GR-0112. This research was also supported in part by the US DHS through the Center for Catastrophe Preparedness and Response at NYU, Grant number 2004-GT-TX-0001 for the project titled *Public Infrastructure Support for Protective Emergency Services*. However, any opinions, findings, and conclusions or recommendations in this document are those of the author and do not necessarily reflect views of the US DHS.

## REFERENCES

1. Zimmerman, R., and Horan, T. (2004). What are digital infrastructures? In *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*, R. Zimmerman, and T. Horan, Eds. Routledge, London, pp. 3–18.

2. Hutson, S. S., Barber, N. L., Kenny, J. F., Linsey, K. S., Lumia, D. S., and Maupin, M. A. (2004). *Estimated Use of Water in the United States in 2000, Circular 1268*, U.S. Geological Survey, Reston, VA.
3. Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding and analyzing critical infrastructure interdependencies. *IEEE Control Syst. Mag.* **21**(6), 11–25.
4. Simonoff, J. S., Restrepo, C. E., Zimmerman, R., and Naphtali, Z. S. (2008). Analysis of electric power and oil and gas pipeline failures. In *Critical Infrastructure Protection*, E. D. Goetz, and S. Shenoi, Eds. Springer, New York, pp. 381–394.
5. Zimmerman, R. (2006). Critical infrastructure and interdependency. In D. G. Kamien, Ed. *The McGraw-Hill Homeland Security Handbook*, The McGraw-Hill Companies, Inc., New York, pp. 523–545.
6. U.S. Department of Energy (2006). *Energy Demands on Water Resources. Report to Congress on the Interdependency of Energy and Water*, December. Online. Available at http://www.sandia.gov/energy-water/docs/121-RptToCongress-EWwEIAcomments-FINAL.pdf. Accessed 6 July, 2007.
7. Water Sector Coordinating Council (WSSC), U.S. Department of Homeland Security and the U.S. Environmental Protection Agency (2007). *Water. Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, U.S. DHS, Washington, DC.
8. U.S. Department of Homeland Security (2007). *Communications Sector Specific Plan*, U.S. DHS, Washington, DC.
9. Electric Power Research Institute (2002). *Water & Sustainability (Volume 4): U.S. Electricity Consumption for Water Supply & Treatment—The Next Half Century*, EPRI. Online. Available at http://www.epriweb.com/public/000000000001006787.pdf. Accessed 5 July, 2007.
10. O'Rourke, T. D. (2007). Critical infrastructure, interdependencies, and resilience. *The Bridge* **37**(1), 22–29.
11. O'Rourke, T. D., Lembo, A. J., and Nozick, L. K. (2003). Lessons learned from the world trade center disaster about critical utility systems. In *Natural Hazards Research & Applications Information Center, Public Entity Risk Institute, and Institute for Civil Infrastructure Systems*, Beyond September 11th: An Account of Post-Disaster Research. University of Colorado, Boulder, CO, pp. 269–292.
12. New York University, Wagner Graduate School of Public Service (NYU-Wagner), Institute for Civil Infrastructure Systems (2006–2007). *Resource Allocation Based on Critical Infrastructure*, Research project for the Center for Risk and Economic Analysis of Terrorism Events (CREATE) at the University of Southern California, New York University, Wagner Graduate School of Public Service, New York, NY.
13. Zimmerman, R. (2005). Social implications of infrastructure network interactions. In O. Coutard, R. Hanley, R. Zimmerman, Eds. *Sustaining Urban Networks: The Social Diffusion of Large Technical Systems*, Routledge, London, UK, pp. 67–85.
14. U.S. Departments of the Army and the Air Force (1987). *Chapter 8: Utilidors in ARMY TM 5-852-5. AIR FORCE AFR 88-19*, **5**. Technical Manual.
15. Vanrenterghem-Raven, A. (2003). *Modeling of the Structural Degradation of an Urban Water Distribution System*, Polytechnic University of New York, Brooklyn, NY, p. 264.
16. Zimmerman, R. (2004). Decision-making and the vulnerability of critical infrastructure. In *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, W. Thissen, P. Wieringa, M. Pantic, M. Ludema, Eds. Delft University of Technology, The Hague.
17. Thompson, M. (2001). *Much of Northern California in the Dark: Water Pumps Stopped*, 17 Jan 2001. Online. Available at http://www.cnn.com/2001/US/01/17/power.woes.03/index.html.
18. Simonoff, J. S., Restrepo, C. E., and Zimmerman, R. (2007). Risk management and risk analysis-based decision tools for attacks on electric power. *Risk Anal*. **27**(3), 547–570.

19. Simonoff, J. S., Zimmerman, R., Restrepo, C. E., Dooskin, N. J., Hartwell, R. V., Miller, J. I., Remington, W., Lave, L. B., and Schuler, R. E. (2005). *Electricity Case: Statistical Analysis of Electric Power Outages*, CREATE Report No. 3, NYU-Wagner, New York.
20. U.S. General Accountability Office (2007). *Securing Wastewater Facilities. Costs of Vulnerability Assessments, Risk Management Plans, and Alternative Disinfection Methods Vary Widely*, GAO-07-480, USGAO, Washington, DC.
21. Energetics, Inc (2006). *Roadmap to Secure Control Systems in the Energy Sector*, sponsored by, U.S. DOE and U.S. DHS, Energetics, Inc, Columbia, MD.
22. Zimmerman, R. (2004). Water. In R. Zimmerman, and T. Horan, Eds. *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*, Routledge, London, pp. 75–95.
23. Synchrony (2001). *Trends in SCADA for Automated Water Systems*.
24. American Society of Civil Engineers (ASCE) and American Water Works Association (AWWA) (2006). *Guidelines for the Physical Security of Water Utilities*, ASCE, Reston, VA.
25. Zimmerman, R., and Restrepo, C. E. (2006). The next step: Quantifying infrastructure interdependencies to improve security. *Int. J. Crit. Infrastruct*. **2**(2/3), 215–230.
26. World Wildlife Fund (WWF) International, Zoological Society of London, and Global Footprint Network (2006). *Living Planet Report 2006*, WWF, Gland.
27. ASCE (2005). *Report Card for America's Infrastructure*, Online. Available at http://www.asce.org/reportcard/2005/index.cfm. Accessed 7 November, 2005.

## FURTHER READING

Apostolakis, G. E., and Lemon, D. M. (2005). A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. *Risk Anal*. **25**(2), 361–376.

Charles, J. (2007). *Neighborhood Report: New York Up High; Longtime Emblems of City Roofs, Still Going Strong*, NY Times. 3 June, 2007, p. 9.

East Bay Municipal Utilities District (2007). *EBMUD Mission Statement*, Online. Available at http://www.ebmud.com/about_ebmud/mission_statement/. Accessed 3 July, 2007.

Electric Power Research Institute (2002). *Water & Sustainability (Volume 3): U.S. Water Consumption for Power Production—The Next Half Century*, EPRI. Online. Available at http://www.epriweb.com/public/000000000001006786.pdf. Accessed 5 July, 2007.

Ezell, B., Farr, J. V., and Wiese, I. (2000). Infrastructure risk analysis model. *J. Infrastruct. Syst*. **6**(3), 114 –117.

Ezell, B., Farr, J. V., and Wiese, I. (2000). Infrastructure risk analysis of municipal water distribution systems. *J. Infrastruct. Syst*. **6**(3), 118 –122.

Hake, J. M., Gray, D. M. D., and Kallal, S. (2004). Power diet. California's energy crisis prompts one treatment plant to re-evaluate its power intake. *Water Environ. Technol*. **16**(5), 36–40.

National Research Council (2002). Making the Nation Safer, The National Academies Press, Washington, DC.

Vanrenterghem-Raven, A. (2007). Risk factors of structural degradation of an urban water distribution system. *J. Infrastruct. Syst. ASCE* **13**(1), 55–64.

Restrepo, C. E. (2004). Infrastructure and IT dimensions in the developing world. In *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*, R. Zimmerman, and Horan T., Eds. Routledge, London, pp. 179–202.

Restrepo, C. E., Simonoff, J. S., and Zimmerman, R. Analyzing vulnerabilities in the oil and gas sector from incident data. *Paper presented at the Los Alamos National Laboratories Risk*

*Symposium 2006—Risk Analysis for Homeland Security and Defense: Theory and Application*. Sante Fe, New Mexico.

Restrepo, C. E., Simonoff, J. S., and Zimmerman, R. (2006). Unraveling geographic interdependencies in electric power infrastructure. In *Proceedings of the Hawaii International Conference on System Sciences*, Wiley-IEEE Computer Society Press, 248a, Digital Object Identifier 10.1109/HICSS.2006518. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1579808.

U.S. Geological Survey (2004). *Estimated Use of Water in the United States in 2000*, Online. Available at http://water.usgs.gov/pubs/circ/2004/circ1268/htdocs/text-total.html. Accessed 6 July 6, 2007.

Wackernagle, M., and Rees, W. (1996). *Our Ecological Footprint*, New Society Publishers, Gabriola Island.

Zimmerman, R (2003) Public Infrastructure Service Flexibility for Response and Recovery in the September 11th, 2001 Attacks at the World Trade Center. In *Beyond September 11th: An Account of Post-Disaster Research*, Natural Hazards Research & Applications Information Center, Public Entity Risk Institute, and Institute for Civil Infrastructure Systems, University of Colorado, Boulder, CO, pp. 241–268.

Zimmerman, R., Restrepo, C. E., Simonoff, J. S., and Lave, L. B. (2007). Risk and economic cost of a terrorist attack on the electric system. In *The Economic Costs and Consequences of Terrorism*, H. W. Richardson, P. Gordon, and J. E. Moore II, Eds. Edward Elgar Publishers, Cheltenham, pp. 273–290.

# SURVEILLANCE METHODS AND TECHNOLOGIES FOR WATER AND WASTEWATER SYSTEMS

STANLEY STATES

*Pittsburgh Water and Sewer Authority, Pittsburgh, Pennsylvania*

## 1 INTRODUCTION

Drinking water utilities are potentially vulnerable to a variety of intentional malevolent acts. These include physical assaults with explosive or incendiary devices, intentional release of harmful treatment chemicals such as gaseous chlorine or ammonia, cyber attacks on utility SCADA (supervisory control and data acquisition) systems or information systems, and intentional contamination of the drinking water. Intentional

contamination is generally considered to be the scenario of greatest concern because this is the one that could potentially affect and could have significant effects on the greatest number of people. Furthermore, if a contamination attack is conducted clandestinely, officials may not become aware of the event until people become ill.

Wastewater utilities are also subject to physical and cyber attacks, as well as the intentional release of dangerous treatment chemicals to the environment. Although wastewater is not ingested, contamination of wastewater collection or treatment systems with flammable substances such as gasoline could result in serious explosions. The intentional addition of volatile toxic chemicals or pathogens could impact the health of wastewater workers and the public. Wastewater systems are also indirectly vulnerable to contamination events in that if the drinking water system becomes contaminated, it is likely that at least some of the contaminated water would end up in the sanitary collection system. Additionally, water used to decontaminate buildings and equipment that had been intentionally contaminated by chemical, biological, or radiological agents could also find its way into the municipal wastewater system. An example situation is the concern expressed over the disposal of contaminated water following the intentional contamination of post offices and government buildings during the mailborne anthrax attacks in 2001.

Contamination warning system (CWS) is an important tool for improving the security of drinking water or wastewater utilities, directly or indirectly, susceptible to intentional contamination events. A key component of CWS is the continuous, on-line network of monitoring equipment strategically located at various sites in the treatment plant and drinking water distribution or wastewater collection systems. The purpose of the monitors is to detect chemical, biological, or radiological contaminants that could pose a threat to the public or utility. The monitors might also be able to detect the carrier matrix within which a contaminant is injected, such as the growth medium supporting a bacterial culture. Ideally, the monitoring network would provide multiple benefits in that it might detect contaminants accidentally injected into a water or wastewater system as well as those injected intentionally. Monitoring devices such as chlorine analyzers may also be useful for utility process control or for ensuring regulatory compliance.

There are currently five approaches being taken for on-line, real-time monitoring for contaminants in drinking water:

- monitoring routine chemical parameters as surrogates or indicators for chemical, and perhaps even biological, contaminants (detecting a “chemical change of state”);
- real-time toxicity biomonitoring;
- monitoring for radiation to detect the presence of radionuclides;
- detecting, identifying, and quantifying specific chemical contaminants; and
- detecting, identifying, and quantifying specific pathogens.

Currently, there are few remote monitoring networks being installed in wastewater systems to detect intentional or accidental contamination events. However, wastewater monitoring networks follow the same five approaches.

The following is a description of some of the commercially available equipment, which is currently being used in CWS, and some of the emerging technologies that could be used in these five monitoring approaches.

## 2 MONITORING ROUTINE CHEMICAL INDICATORS OF CONTAMINATION

Currently, there are several practical obstacles for on-line detection of contamination in water systems. One of those is that a large number of chemical, biological, and radiological agents, accidentally or as a result of a malevolent act, contaminate drinking water or wastewater systems. It would be very difficult, and prohibitively expensive, to develop and deploy analytical devices that could qualitatively and quantitatively monitor, on a continuous on-line basis, for each of these specific agents. Currently, the technology for this type of specific monitoring exists at a fairly basic level. Furthermore, chemicals that have not previously been considered to be candidates for use as intentional contaminants could be used, or combinations of contaminants could be utilized, which would confuse analytical efforts to identify specific agents.

One of the approaches to deal with these obstacles is to utilize basic chemical parameters (such as pH, chlorine concentration, total organic carbon [TOC], and conductivity) as surrogates or indicators for many of the contaminants that could potentially appear in water. Changes in the values for these basic parameters could signal a significant chemical "change of state" in the water, thereby suggesting the presence of an unknown contaminant. This is similar to the use of coliform bacteria as indicators for the possible presence of waterborne pathogens; a practical approach that has been utilized for the past 100 years in the water industry. Monitoring for basic parameters is feasible because on-line monitoring equipment for these parameters has already been developed, and in some cases has been deployed in water systems for years. Additionally, the instrumentation is relatively inexpensive, especially when compared to the analytical instruments that would be needed to detect, identify, and quantify specific contaminants.

Several studies have been published supporting the feasibility of monitoring for contamination by measuring surrogate parameters. Byer and Carlson [1] conducted a series of both batch and pilot scale distribution system studies to test whether four credible contaminants for intentional contamination of drinking water could be detected using the routine parameters, such as chlorine concentration, pH, turbidity, conductivity, and TOC. The contaminants included pesticides, rodenticides, and industrial inorganic compounds. Their results showed that three of the four contaminants were detected below a concentration that would cause significant health effects, and the fourth was detected near the concentration for acute health effects. Hall et al. [2] utilizing both bench studies and recirculating plumbing loops with on-line sensors, investigated the extent to which changes in standard water quality parameters may indicate the presence of contaminants. The sensors were challenged with secondary effluent from a wastewater treatment plant, potassium ferricyanide, a malathion insecticide formulation, a glyphosate herbicide formulation, nicotine, arsenic trioxide, aldicarb, and *Escherichia coli* with growth media. The results of the study indicated that, while no single water quality parameter responded to all of the contaminants used, all of the contaminants caused at least one parameter to change significantly.

Some of the equipment currently being used for surrogate monitoring is described below.

### 2.1 On-line Chlorine Measurement

Residual chlorine is one of the most widely measured on-line chemical parameters in the water industry. Free and total chlorine concentrations can be measured on a continuous basis for regulatory compliance purposes to ensure adequate disinfection at the treatment plant and the maintenance of a protective residual in the drinking water distribution system. For process control purposes, chlorine can be measured on a continuous basis, and the results linked with an alarm system that notifies the operator of low chlorine concentrations and the need for increased dosage. Chlorine readings can also be tied into a feedback loop to automatically pace the dosage of chlorine applied at the treatment plant or at chlorine booster stations in the distribution system. Additionally, continuous measurement of chlorine concentration can be utilized to help ensure water system security. A significant decline in chlorine residual can signal an unexpected increase in disinfectant demand and suggest the presence of a contaminant in the water. The study published by Hall et al. [2], described above, indicated that a change in chlorine level is one of the most sensitive chemical indicators for a number of contaminants.

A variety of chlorine measurement devices are available from a number of manufacturers. These devices utilize amperometric, DPD, or polarographic membrane methods for free and total chlorine measurement.

### 2.2 General Organic Chemical Load

There are several analytical instruments that can be utilized to provide a gross measurement of the organic content of water. These include TOC analyzers and UV–visible spectrometers.

TOC analysis is a commonly used technique to measure the carbon content of dissolved and particulate organic matter present in water. Many drinking water utilities monitor TOC to evaluate raw water quality or to gauge the effectiveness of treatment processes designed to remove organic carbon. Some wastewater utilities also employ TOC analysis to monitor the efficiency of treatment processes. In addition to these applications, changes in TOC concentration can be used as a surrogate for contamination from organic compounds (e.g. petroleum products, industrial solvents, and pesticides). Although TOC analysis can not identify specific contaminants, gross deviations from normal TOC concentrations can be an indication of a chemical contamination in a system. On-line TOC analyzers could be placed at critical locations within a drinking water distribution system, either at the intake of a drinking water treatment plant or at a wastewater influent wet well to detect potential chemical threats. TOC analysis has been shown to be an especially sensitive method for detecting changes caused by a variety of contaminants that could potentially be introduced accidentally or intentionally into a public water supply [2]. The response time for TOC analyzers varies with manufacturers' specifications. However, 5–15 min is generally required to obtain stable readings. Detection limits vary from 0.2 to 1 mg/l carbon. A TOC monitor currently deployed within the Pittsburgh drinking water distribution system is the Sievers 900 On-Line TOC Analyzer[1] utilizing UV/persulfate oxidation and membrane conductometric detection.

Another surrogate parameter for general organic content of water is UV–visible absorbance. A UV–vis spectrometer will react with any organic contaminant that absorbs

[1] Ionics Instruments, Boulder, CO.

in the UV range. The alarm sensitivity for many organic contaminants is between 1 and 500 ppb. The types of organic compounds detected include phenol, toluene, xylene, many pesticides, some nerve gases, crude oils, and naphthalene, among others. The types of compounds not detected include short-chained aliphatics. Response time can be less than 1 min. Potential advantages of UV–vis spectrometry, compared with TOC measurement, are quicker response time, greater sensitivity, less maintenance, and lower initial cost. A commercially available product, which is deployed in the drinking water distribution system of Vienna, Austria, and some other European cities is the spectrolyser spectrometer with the ana::larm software package manufactured by scan Messtechnik.[2]

## 2.3 Oil and Petroleum Detection

Monitors are available for detecting the presence of oil and petroleum products in water. Light scattering devices are employed on commercial offshore oil rigs to detect surface sheens on the water. However, these are too insensitive for practical use in drinking water. On the other hand, fluorometry has been used for years to detect the presence of hydrocarbons in source waters at drinking water treatment plant intakes, and to help characterize the progress of petroleum product plumes in lakes and rivers following industrial spills. Commercially available fluorometers such as the Turner TD 4100[3] can detect dissolved gasoline, diesel, jet fuel, and oil components such as the BTEX compounds (benzene, toluene, ethylbenzene, and xylenes). These instruments continually measure the fluorescence of aromatic hydrocarbons in a flowing stream of water ranging from low parts per billion to high parts per million. Fluorescence occurs when a molecule absorbs light energy of a specific wavelength and emits light energy of a longer wavelength.

## 2.4 On-line Analytical Probes and Multiparameter Panels

On-line analytical probes are the most commonly used devices for early warning security systems. They are relatively inexpensive, simple to use, provide continuous monitoring with remote access to data, and are commercially available from a number of vendors. Many of these devices are already in place for process control both in treatment plants and in distribution systems. These include electrodes that measure a variety of chemical parameters (e.g. fluoride, dissolved oxygen, ammonia, nitrate), thermistors for temperature, potentiometric devices for oxidation–reduction potential, conductivity cells for specific conductance, and nephelometric units for turbidity.

Several manufacturers have combined a number of already available individual sensors into panels of sensors that track multiple water quality parameters. These multiparameter panels detect physical/chemical changes in one or more water quality parameters (change in chemical state), which suggest that a contaminant has been intentionally or accidentally added to the water. The idea is for the multiparameter monitor to provide an early warning for an unspecified contaminant. Some commercially available devices include the Clarion-Sentinal 500 Series,[4] the Rosemount Analytical WQS,[5] and the YSI 600 D.[6]

[2] s::can Messtechnik, Vienna, Austria.
[3] Turner Designs, Inc., Sunnyvale, CA.
[4] Clarion Sensing System, Inc., Indianapolis, IN.
[5] Rosemount Analytical, Irvine, CA.
[6] YSI Inc., Yellow Springs, OH.

A more advanced application of the multiparameter panels is the attempt to establish a characteristic pattern of changes in multiple parameters (a signature or fingerprint) that might be used to presumptively identify the contaminant. Several commercial entities and research groups are currently working to develop this approach. For example, the Hach Corporation[7] is marketing the GuardianBlue system. This unit consists of sensors, which the company has previously sold individually, that they have now combined into a preconfigured system, "water panel", for more comprehensive monitoring. The panel includes analyzers for TOC, chlorine, pH, turbidity, and conductivity. The system also includes an "event monitor" that facilitates real-time analysis of data from the monitoring panel. The event monitor integrates the readings for all the chemical parameters into a composite value or vector. If the composite value differs substantially from normal background level, and from routinely encountered deviations from the norm caused by utility operational changes such as turning on distribution system pumps, the event monitor triggers an alarm. Additionally, Hach has developed an agent library that contains a signature or fingerprint of the changes expected to occur in composite parameters when one of 80 different contaminants is introduced into the water. The 80 contaminants (which include arsenic, herbicides, ricin, and *VX*) are believed by the manufacturer to be potential candidates for used in an intentional contamination incident. The entire monitoring device can be set up remotely to communicate directly with a utility's SCADA system.

### 2.5 Multiarray Sensors

In addition to analytical probes, there are on-line sensors that measure a similar set of chemical parameters by utilizing electrochemical technology, rather than through the use of reagents. These sensors can be configured as a multiarray sensor to monitor for a number of chemical parameters. As with the on-line analytical probes, the multiarray sensors can be operated remotely with data reported to a SCADA system.

Censar Technologies Inc.[8] (formerly Dascore Six-Cense) manufactures a multiarray sensor called the *multiparameter water quality/security sensor*. This sensor, designed as a 1 in.$^2$ ceramic chip layered with gold, can be permanently inserted into a pressurized main stream or a side stream of water. It can monitor simultaneously for pH, dissolved oxygen, temperature, oxidation–reduction potential, conductivity, and either chlorine or monochloramine concentration. The sensor chip is field replaceable with a typical 6-month life according to the manufacturer.

## 3 REAL-TIME TOXICITY BIOMONITORING

Ultimately, the drinking water contaminants of most immediate significance are those that are acutely toxic to the people using the water. No analytical chemistry technique can directly measure toxicity. Specific analytes can be monitored for, but toxicity can only be inferred by comparing measured chemical concentrations with published toxicity values. However, it is possible to utilize living organisms, or biological systems, as biomonitors or sentinels to detect the presence of toxic substances. Some biomonitors measure changes

[7]Hach, Loveland, CO.
[8]Censar Technologies Inc., Wimborne Dorset, UK.

in the behavior or physiology of living organisms resulting from stresses induced by toxicity. Others detect toxic substances through cellular responses of prokaryotic cells (bacteria) or eukaryotic cells (from higher level organisms).

The use of biomonitors as toxicity screening devices is advantageous since the spectrum of contaminants potentially detected is much broader than that of analyte-specific determinations. The disadvantage of biomonitors is that they do not identify the specific chemicals causing a response. In this sense they are like biological smoke detectors. Additionally, biosensors can sometimes respond to water quality changes that are not harmful to people. These could include sudden shifts in temperature, pH, turbidity, and so on.

The classic example of a toxicity biomonitor is that of coal miners, years ago, bringing canaries into the mine with them to detect the presence of noxious gases such as methane. Although the concept seems simplistic for modern application, in reality there is no better broad spectrum indicator of potential toxicity for people than observing the toxic reactions among other organisms exposed to the environment in question.

A number of biosensors are commercially available for on-line monitoring of both source waters and finished drinking waters. These include organisms as diverse as bacteria, algae, mollusks, daphnia, and fish. Also available are biological sensors utilizing biological systems, such as enzyme systems, rather than whole living organisms.

The use of biomonitors in finished drinking water requires the removal of chlorine residuals since chlorine is toxic to most aquatic organisms. While this was a stumbling block several years ago, there are now commercially available dechlorinating units that continually remove chlorine through the addition of chemicals such as sodium thiosulfate. Reducing agents are typically not harmful to aquatic organisms at the concentrations needed to neutralize chlorine. However, there is always a concern that these chemicals could neutralize certain potential toxicants thus interfering with their detection. An example of a dechlorinating system currently on the market is the "portable dechlorinator" manufactured by Geo-Centers, Inc.[9]

The following is a description of some of the types of biomonitors that are currently available for use in source waters and finished waters.

### 3.1 Bacteria-Based Toxicity Sensors

Several bacteria-based sensors are being used by water utilities and response teams for rapid toxicity testing of grab samples of water collected during the investigation of contamination threats. These sensors are effective because the metabolism and/or cellular structure of bacteria can react rapidly to the presence of toxicants. Certain bacteria exhibit natural or genetically engineered bioluminescence that emits measurable light when the bacterial cells are healthy. Since the bioluminescence is closely tied to respiration, changes in the metabolism or cellular structure of the bacteria decreases bioluminescence. A reduction in bioluminescence, which can be measured with a photometer, suggests the presence of a toxic substance. Still other toxicity detectors monitor bacterial metabolism via changes in parameters such as bacterial oxygen demand.

A bacteria-based toxicity sensor that is commercially available for continuous on-line use in water is the TOXcontrol system manufactured by microLAN.[10] This automated

[9]Geo-Centers, Inc., Newton, MA.
[10]microLAN, Netherlands.

biomonitoring system utilizes freshly cultivated fluorescent bacteria, *Vibrio fischeri*, as the biological sensor. The natural luminescence of the bacteria is measured before and after exposure to 4.5 ml of the suspect water to estimate the amount of toxicity. This estimate is calculated using a computer software package that is part of the biomonitoring system. Toxicity standards are run at preset time intervals for system calibration. The bacteria are cultivated in a separate bioreactor for automatic and controlled cultivation. The manufacturer claims that only weekly maintenance of the system is required. A thiosulfate dechlorination system can be included with the system to permit operation within a chlorinated municipal water system.

### 3.2 Daphnia Toximeters

Daphnia (water fleas) are small free-swimming crustaceans that are visible to the naked eye and are very sensitive to toxicants. In fact, *Daphnia magna* has been utilized for over 100 years for toxicity testing of raw and treated waters, as well as industrial effluent. In on-line Daphnia toximeters, several daphnids are housed in a glass chamber through which the water being monitored continuously flows. The swimming behavior of the daphnids is monitored by closed circuit TV and the data are analyzed by computer. Changes in swimming behavior by several daphnids suggest the possible presence of a toxic substance in the water. This surveillance device has been used in Europe and was employed during the 2002 Winter Olympics in Salt Lake City, UT.

A Daphnia Toximeter manufactured by bbe moldanke[11] is deployed on-line with a measuring cycle of 30 min. Toxicity is monitored by observing swimming speed, swimming altitude, and turning and circling movements, as well as the number of live daphnia.

### 3.3 Mussel Monitors

Mussels are filter feeders that acquire their food by sifting through large volumes of water. If toxic substances appear in the water, mussels avoid exposure by closing their shells. The frequency of valve opening and closing can be monitored to indicate toxin avoidance behavior.

In commercially available mussel monitors, a number of mussels are glued to the top of a flow-through unit. Valve opening and closing is monitored by high-frequency induction sensors attached to the shells. A variety of mussels including clams, oysters, blue mussels, and even the nuisance organism, zebra mussels have been utilized for monitoring. Delta Consult[12] sells the MosselMonitor, which can be used to monitor chlorinated drinking waters since it utilizes a continuous thiosulfate pretreatment to remove chlorine. According to the manufacturer, the MosselMonitor can be operated on-line continuously for a 2–3-month period before replacement of mussels is required.

### 3.4 Algae Toximeters

In this toxicity monitoring device, chlorophyll fluorescence is utilized as the indicator of water quality. If water quality is good, algae photosynthesize and fluoresce. However, if substances are present in the water that negatively affect the algae, both photosynthesis and fluorescence are suppressed. A measured reduction in fluorescence indicates

[11] bbe moldanke, Kiel-Kronshagen, Germany.
[12] Delta Consult, Netherlands.

a decrease in the concentration of active chlorophyll and suggests the presence of a substance injurious to the algae. The commercially available systems utilize either algae already present in the water being tested or algae continually cultured in a fermenter and automatically injected in precisely defined amounts, into the measurement chamber. The algal fluorescence sensor is normally interfaced with a personal computer to facilitate interpretation of results.

A commercially available algae toximeter is manufactured by bbe moldanke, in which algae are continually cultured in a fermenter that regulates the concentration and activity of the algae. A raw water sample is automatically injected with a preset concentration of algae, at specified time intervals, and algal fluorescence is measured. Activity and fluorescence of the algae should be constant if no toxic substances are present.

### 3.5 Fish

Currently, several types of fish biosensors are in use. The simplest is the avoidance behavior sensor, which is based on the fact that fish tend to swim away from water containing poisonous or irritating substances. Such a system typically involves housing fish in a series of connected tanks through which the water being monitored continuously flows. The sentinel fish are fed in the first tank that initially receives the test water, and tend to spend most of their time there. However, if the quality of the incoming water deteriorates, the fish swim into the tanks located farther downstream and ultimately into an "escape tank" that is plumbed so that the water does not turn over as frequently as in the upstream tanks. This avoidance behavior suggests the possible presence of toxic substances in the water. Potentially, this type of system could be automated by using closed circuit TV or movement sensors in the pipes interconnecting the various tanks.

A more sophisticated approach to utilizing fish as biomonitors is employed by several commercial manufactures who sell systems that detect toxicants or degradation in water quality by observing changes in the ventilatory pattern or swimming behavior of fish. In these systems, a number of fish are held in individual chambers under continuous flow-through conditions. Electrical signals generated by muscle movements of individual fish are monitored, amplified, and sent to a personal computer for analysis. Ventilatory rate, ventilatory depth, gill purge (cough), and whole body movements are observed and measured. The stress caused by the sudden appearance of a toxic substance in the water will cause changes in ventilation and body movement and can trigger an alarm. Commercially available systems include the Bio-Sensor Fish Monitor,[13] Intelligent Aquatic Biomonitoring Systems IAC 1090,[14] and Medaka Sensor.[15]

Mikol et al. [3] described the New York City Department of Environmental Protection's experiences using ventilatory changes in fish, to protect the source waters for the New York City drinking water system. They found that the biomonitors could be operated for extended periods of time with minimal maintenance and downtime. They described several instances in which the biomonitors successfully detected the presence of accidentally discharged surface water contaminants in the source water. They also reported concentration ranges of some contaminants that elicited a response among bluegills in

[13]Bio-Sensors Inc., Blacksburg, VA.
[14]Intelligent Aquatic Biomonitoring System (iABS), Intelligent Automation Corp., Poway, CA.
[15]Seiko Corp., Japan.

laboratory studies that they and their associates had conducted previously. These included a positive response to cyanide at 0.01–0.10 mg/l, mercury and zinc at >0.1–1.0 mg/l, malathion at >1.0–10.0 mg/l, phenol at >10.0–100.0 mg/l, and acetone at >100 mg/l.

## 4 MONITORING FOR RADIATION TO DETECT RADIONUCLIDES

Radiation monitoring equipment is designed to measure either the total amount of radiation emitted from a source (gross radiation) or the specific types and energy levels of radiation emitted from a source. Responders trying to determine whether there is an elevated level of radiation in the water from accidental releases or intentional introductions do not necessarily require that the specific radionuclides causing the contamination be immediately identified. They would rather most likely be interested in utilizing some type of continuous, on-line screening equipment to measure gross radiation. The common types of gross radiation are $\alpha$, $\beta$, and $\gamma$.

On-line instruments for monitoring $\alpha$, $\beta$, and $\gamma$ radiation in water have been developed. However, there are a limited number of models available, and they can be expensive. Technical Associates[16] offers the SSS-33-5FT for approximately $58,000. This is a flow-through scintillation detection system for $\alpha$-, $\beta$-, and $\gamma$-radiation monitoring. The detector can be preset to measure one type of radiation, or all three combined, and can be equipped with a system that sends an alert if unusual counts are detected. Canberra[17] sells the OLM-100 on-line liquid monitoring system, which is attached to the exterior of a pipe and continuously measures the radiation in a liquid stream. The cost of this device is between $35,000 and $70,000 [4].

## 5 SCREENING FOR SPECIFIC CHEMICAL CONTAMINANTS

Unlike the general organic chemical load monitors (TOC and UV–vis spectrometry), gas chromatography (GC) and gas chromatography–mass spectrometry (GC–MS) can detect, identify, and measure the concentration of a wide variety of specific organic compounds. In fact, of all of the on-line physical/chemical monitors described above, GC and GC–MS are the only analytical techniques, currently being deployed in a continuous on-line mode, which can actually identify a specific chemical contaminant. Both these techniques can detect and identify a large number of volatile organic compounds in the low parts per billion (ppb) to parts per million (ppm) range, and can operate automatically and unattended. In the case of GC, the components of a complex mixture are separated, their retention times are compared to known standards, and then the concentrations are quantified. In GC–MS, the organic components are separated by GC, and a more definitive identification of contaminants is provided by mass spectrometry using mass to charge ratio of chemical compound fragments and comparing the mass spectrum with internal libraries that contain thousands of chemical fingerprints of known organic compounds.

Some of the on-line devices collect and concentrate volatile organic compounds (VOCs) from water using standard purge and trap technology. In the continuous on-line

[16]Technical Associates, Los Angeles, CA.
[17]Canberra, Meriden, CT.

mode, sample collection is automated and analysis occurs at regular programmable intervals throughout a 24-h period. INFICON[18] manufactures both GC and GC–MS instruments that utilize purge and trap, and can be operated as on-line monitors for either natural waters or finished drinking waters.

A highly specialized mass spectrometer is being utilized to screen water samples, in an on-line mode, at the Phoenix Arizona Water Services Department [5]. This photoionization and quadrupole ion trap, time-of-flight mass spectrometer provides high-speed screening and molecular identification for weaponized chemicals and other hazardous compounds. The commercially available mass spectrometer is used in an automated mode as an early warning system screening device. The advantage of this particular mass spectrometry approach is that it can be operated on-line and, unlike most mass spectrometers, can analyze mixtures of compounds without preliminary separation by GC. With its integrated autosampler, the instrument provides a high throughput monitor capable of analyzing samples every 45 s.

## 6 SCREENING FOR SPECIFIC PATHOGENS

While a number of devices are currently employed for real-time monitoring of the general chemical characteristics of water (e.g. chlorine concentration and TOC), and for screening for specific chemical contaminants (e.g. on-line GC–MS), the ability to continually screen drinking water for the presence of microorganisms is still quite limited.

A microbial sensor must include a recognition device (bioreceptor), which can react with a target microbe. One approach is to utilize immunoassay-based sensors that recognize specific proteins on the surface of a microbe. Another approach is to employ a bioreceptor that recognizes nucleic acid, either DNA (deoxyribonucleic acid) or RNA (ribonucleic acid), uniquely characteristic of a specific microorganism. When the target protein or nucleic acid is present in the sample, a biological reaction takes place between it and the bioreceptor, creating a physical or chemical change that is converted into an electrical signal proportional to the target microorganism's concentration in the solution. The signal is then amplified, processed, and displayed as a measurable piece of data [6].

In the case of immunoassay-based sensors, antibodies that have an affinity for specific antigens associated with a particular species are utilized. Antibody-based biosensors incorporate antibodies onto a sensor surface and utilize the hybridization between antigen and antibody as the recognition factor [7].

Nucleic acid-based bioreceptors contain on their surface an oligonucleotide that is complimentary to the nucleic acid sequence of the target organism. Recognition consists of hybridization between the bioreceptor's complimentary oligonucleotide and the target microbe's single stranded DNA or RNA. The hybridization reaction generates either an amperometric, optical, thermal, or mass differential signal that is amplified for quantification. The major technical problem associated with nucleic acid biosensing, unlike immunoassay biosensing, is that the DNA or RNA must first be extracted from the target cell. The extraction process requires reagents and incubation steps. Furthermore, following extraction, the double stranded DNA must be denatured into single stranded

[18]INFICON Corp., East Syracuse, NY.

DNA through a heating process. The challenge lies in fully automating the pretreatment extraction and denaturation steps.

An advantage of both immunoassay- and nucleic acid-based sensors is that they can be highly specific and, therefore, able to identify a specific target microbe with certainty. However, since there is such a variety of microbes that could accidentally or intentionally contaminate a water system, these approaches would require the deployment of a complicated array of bioreceptors to provide broad spectrum coverage. An additional disadvantage of both nucleic acid- and antibody-based biosensors is the lifespan and fragility of the recognition system. Nucleic acids and antibodies are biological macromolecules that can be damaged by conditions typical of water and wastewater systems.

Another biosensor approach for on-line biomonitoring of water systems utilizes amperometric detection of the $\beta$-galactosidase enzyme for detection of *E. coli* [8]. $\beta$-Galactosidase is an enzyme involved in lactose fermentation in *E. coli*. In this biosensor system, reagents are added to induce production of $\beta$-galactosidase in *E. coli* present in the sample, which, in turn, hydrolyzes the reagent phenyl $\beta$-D-galactopyranoside to produce phenol, which is detected by an amperometric sensor. Using this system, sensitivity of detection has been observed at a level of 10 CFU/ml of *E. coli* after a 5-h incubation period. Although the sensitivity of this system is generally greater than that of nucleic acid or immunoassay systems, the obvious disadvantages of its application as a real-time microbial sensor are the requirements for reagents, the 5-h incubation time, and the biosensors's specificity for a single bacterial species.

Still another biosensor approach for continuous monitoring is based on optical recognition of microbes [9]. Multiangle light scattering (MALS) is a reagent-less optical approach. MALS technology involves continual irradiation of a flowing column of water with a laser beam. Particles in the column of water scatter the laser beam producing a pattern that is detected by a number of detectors on the opposite side of the water column. Since a variety of angles are monitored simultaneously, a three-dimensional pattern is generated that represents the structure and size of the particle in the laser's path. The goal of MALS is to differentiate between waterborne microorganisms and inorganic particles based on the pattern of scattered light. An additional objective is to identify microbes by comparing the pattern of scattered light with a library of unique "bio-optical signatures" that have been developed by analyzing known microorganisms. The light pattern resembles a fingerprint since it is unique to the internal and surface features of the particles, including size, shape, morphology, and material composition. The current limitations of MALS for on-line monitoring include interferences from organic and inorganic particulate matter in the water sample stream, and difficulty achieving low detection limits. However, developmental efforts are being taken to address these issues.

## 7 PATHOGEN DETECTION SYSTEMS CURRENTLY UNDER DEVELOPMENT

Several continuous monitoring systems for pathogens have been designed, based on the biosensor approaches described above, and are deployed in several drinking water utilities in the United States. Two of these are described below.

JMAR Technologies[19] manufactures the Biosentry System which is a commercial application of the MALS technology optical approach [10]. This technique has been commercially applied in the beverage industry and is now being adapted for use in drinking water utilities [11]. Biosentry is a laser-based system that continuously monitors water for microbes of interest, including pathogens, and attempts to classify them. The system can be used simply as a monitoring device recording microbe counts against time. Alternatively, the system can provide a real-time warning when a predetermined threshold for a particular pathogenic microbe is reached. The device can operate remotely and transmit data into a SCADA network via an encrypted internet connection. The system can send an alert via a number of means, including e-mail and encrypted internet, or directly into a linked information system. Information is refreshed at 1-min intervals and microbial counts are displayed for the species being monitored as well as for unclassified microorganisms.

The system typically monitors a water stream of about 35 ml/min. Sensitivity, and the ability to discriminate between various particles and microbes, is optimal with water containing fewer background particles (i.e. $<1000$ particles/ml). Limits of detection, as reported by the manufacturer, are approximately 150 organisms per milliliter over a 5-min period of surveillance. The commercially available system is currently programmed to detect the protozoans, *Giardia* and *Cryptosporidium*, as well as rod-shaped bacteria. Future developments are aimed at reducing detection limits and identifying a variety of other microbes including the salmonellosis, shigellosis, and anthrax bacteria, as well as various algae and molds.

Another on-line pathogen monitoring device, whose prototype is currently being tested at a large California Bay Area water utility and at a municipal water station in Arizona, is the unattended water sensor (UWS) for water distribution systems [12]. Tenix and Sandia National Laboratories are refining an innovative technology for the near real-time detection of pathogens and biotoxins in drinking water and wastewater. This system is intended to provide rapid automated and unattended contaminant detection and identification at remote locations. The signal could then be sent to a SCADA system within minutes. This system identifies contaminants using a signature based on physical constants of proteins (such as molecular weight or charge to mass ratio).

The UWS is, based on the microChemLab technology, a handheld manually operated instrument originally developed by Sandia Labs. The sample enters the automated sampling device and a 100 nl sample of water is collected. This sample is pH buffered and reacted with a UV fluorogenic label. The sample then enters the detection system in which electrophoresis is used to separate components of the sample and a laser-induced fluorescent protein signature is recorded. The migration times are compared with a database of separations of threat agents and, if a specified matching threshold is reached, the system communicates the results.

The goal is to refine this system so that it can operate without operator intervention for up to 30 days. Ideally, a sample would be analyzed every 30 min. The system currently recognizes protein signatures for the biotoxins ricin and SEB. The next developmental targets include nitrifying bacteria, algal toxins, and *E. coli*. Ultimately, it is hoped that the system will be able to detect and identify a variety of bacteria, viruses, protozoans, and biotoxins.

[19]JMAR Technologies, San Diego, CA.

## 8 CONCLUSIONS

As indicated above, there are five basic approaches currently being utilized for on-line security monitoring of water. To date, most of the applications focus on drinking water. However, many of the same devices could probably be used effectively in wastewater collection and treatment systems.

Although a significant amount of research and development is being devoted to developing new equipment, current technical capabilities are still rather basic. Unfortunately, development of innovative continuous monitoring technology for drinking water and wastewater applications is probably limited due to the relatively small commercial market represented by the water industry. It is hoped that the current US government emphasis on establishment of CWSs for drinking water supplies, typified by the US Environmental Protection Agency's Security Initiative [13], will encourage additional technological advances.

## REFERENCES

1. Byer, D., and Carlson K. H. (2005). Real-time detection of intentional chemical contamination in the distribution system. *J. AWWA*. **97**(7), 130–133.
2. Hall, J., Zaffiro, A. D., Marx, R. B., Kefauver, P. C., Krishnan, E. R., Haught, R. C., and Herrmann, J. G. (2007). On-line water quality parameters as indicators of distribution system contamination. *J. AWWA*. **99**(1), 66–77.
3. Mikol, Y. B., Richardson, W. R., Van Der Schalie, W., Shedd T. R., and Widder, M. W. (2007). An online real-time biomonitor for contaminant surveillance in water supplies. *J. AWWA*. **99**(2), 107–115.
4. USEPA. *USEPA Water and Wastewater Product Security Guide*. www.epa.gov/safewater/security.
5. Calles, J., Gottlier, R., Evans, M., and Syage, J. (2005). Early warning surveillance of drinking water by photoionization/mass spectrometry. *J. AWWA*. **97**(1), 62–73.
6. Leonard, P., Hearty, S., Brennan, L., Dunne, L., Quinn, J., Chakraborty, T., and O'Kennedy R. (2002). Advances in biosensors for detection of pathogens in food and water. *Enzyme Microb. Technol*. **32**(1), 3–13.
7. Erickson B. (2001). Biosensors for detecting pathogens. *Environ. Sci. Technol*. **35**(9), 187–188.
8. Serra, B., Morales, M. D., Zhang, J. B., Reviejo, A. J., Hall, E. H., and Pingarron, J. M. (2005). In-a-day electrochemical detection of coliforms in drinking water using a tyrosinase composite biosensor. *Analyt. Chem*. **77**(24), 8115–8121.
9. Quist, G. M., DeLeon, R., and Felkner, I. C. (2004). *Evaluation of a Real-Time Online Monitoring Method for Cryptosporidium*, AWWA Research Foundation Project 91020F.
10. JMAR Technologies. (2006). Web Page. www.jmar.com.
11. Adams, J. A., McCarty, D., and Crousore, K. (2006). A real-time early warning system for pathogens in water. *Proceedings of the SPIE*, Vol. 6218. SPIE.
12. Sandia National Laboratory. (2007). *Sandia's Unattended Water Sensor Capable of 24/7 Detection of Toxins, Bacteria in Water Supplies*. www.sandia.gov/news/resources/releases/2007/watersensor.html.
13. USEPA. (2007). *U.S. EPA Water Security Initiative*. www.epa.gov/safewater/watersecurity/pubs/fs_watersecurity_security initiatives.pdf.

# DESIGNING AN OPTIMUM WATER MONITORING SYSTEM

WALTER M. GRAYMAN
*W.M. Grayman Consulting Engineer, Cincinnati, Ohio*

## 1 INTRODUCTION

Monitoring can serve as a window for observing the quality of water in a water-supply system at a location and at an instant in time. Water quality monitoring can serve several purposes including the following:

1. detect contaminants introduced intentionally or accidentally into the water supply;
2. assist in routine water quality operations of the water system;
3. fulfill regulatory requirements.

The monitoring system should be designed and operated to meet the specific designated objectives. Monitoring can be characterized by the frequency of sampling and the handling methods. With automated sampling/monitoring procedures, the water quality sample is collected and analyzed without human intervention. Continuous on-line monitors collect and analyze samples at a specified interval. Grab sampling involves the manual collection of a sample and analysis of the sample in the field or in the laboratory. Both automated and manual sampling procedures serve a role in most well-designed monitoring programs.

## 2 ROLE OF MONITORING IN WATER SECURITY

Within the context of water security, monitoring is typically performed in order to detect the presence of a contaminant within the water. When combined with a mechanism for communicating and using the information in a timely manner, the information can serve as an early warning that allows the water utility to modify operation or treatment, or to issue notifications to reduce the potential impacts of the contaminated water on customers. In the past, such early warning systems (EWSs) were used primarily to monitor the quality of surface water systems that served as sources for water supplies [1, 2]. The EWS for the Ohio River Basin implemented and managed by the Ohio River Valley Water Sanitation Commission (ORSANCO) over the past quarter of a century is the foremost example of this type of system in the United States [3]. This system is composed of 15 gas chromatographs (GC) located at key locations on the river that monitor for 22 volatile organic compounds and report and track the contaminants as they move downstream. In Europe, the Rhine River has the most comprehensive monitoring and EWS, which were constructed in response to a major chemical spill that occurred in 1987 [4].

In the twenty-first century, the emphasis within the water industry has evolved from source water monitoring to detect accidental contaminant spills to include monitoring in distribution systems to detect intentional contamination events. The focus on distribution systems as the most likely target can be attributed to the following factors: there is less dilution water than in surface water bodies; other than disinfectant residual, there is minimal treatment affecting a contaminant added within the distribution system, and the relatively short travel time from likely point of contamination to the customer. This has led to considerable research and development on the implementation of contamination (or early) warning systems within distribution systems.

## 3 CONTAMINATION WARNING SYSTEM

A contamination warning system (CWS) or EWS is a combination of monitors, institutional arrangements, analysis tools, emergency protocols, and response mechanisms designed to provide early warning of contaminants in order to minimize customer exposure. Formerly referred to as *early warning systems*, the term *contamination warning systems* is now used more frequently when referring to distribution systems because of the general acceptance that it is unlikely that a warning could be issued early enough that no customers would be impacted by the contamination.

The characteristics of the potential threat are an important issue in the design of a CWS. A threat is defined as the specific contamination (agent) that is introduced into the system, the quantity that is introduced and the location where it is introduced. The impacts of the contamination event will depend upon both the characteristics of the threat and the effectiveness of the CWS (and associated response process) in thwarting or mitigating the effects of the threat.

Monitoring and sampling are important elements in the CWS as a mechanism for detecting, characterizing, and confirming the threat. These three roles for monitoring/sampling within the context of an emergency response are shown in Figure 1. Initial detection generally requires the use of on-line monitors that continuously or frequently sample the water to determine the presence of an unusual constituent in the water. Manual rapid field assessment sampling is then used as a mechanism to confirm that there is a credible threat and potentially to characterize and identify the nature of the threat. Final confirmation and characterization of the actual constituent in the water generally requires the use of laboratory analytical analysis. In an actual system, final confirmation may not occur until after full-scale emergency response has been initiated. Additional information on this topic is presented in Environmental Protection Agency (EPA)'s Response Protocol Tool Box [5].

## 4 IDEAL CONTAMINATION WARNING TECHNOLOGY

It is useful to identify the characteristics of the ideal monitoring technology used in the detection phase of a CWS. These characteristics are enumerated below.

- fully automated (operates on-line and remotely);
- frequent sampling rate (continuous or frequent sampling);
- rapid response time;
- high sensitivity;

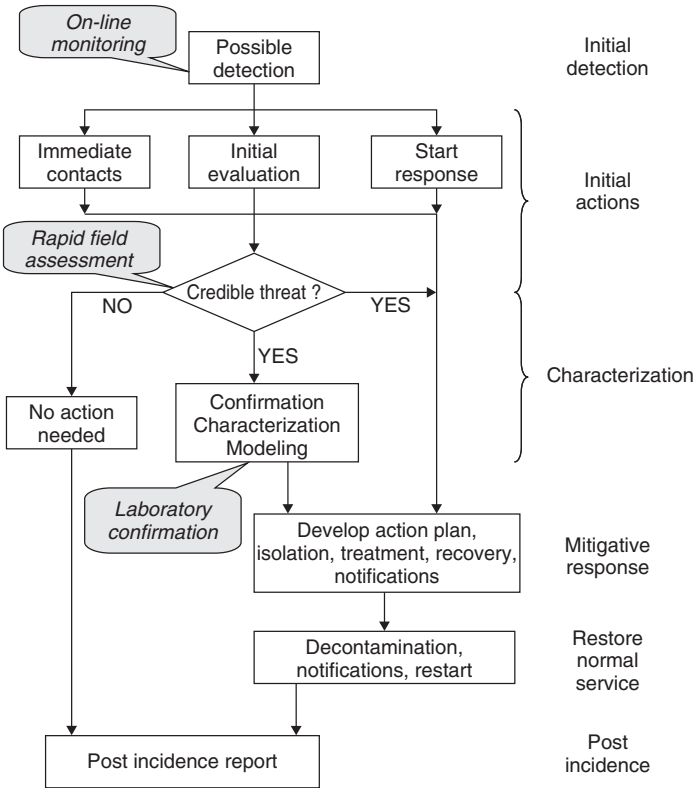



**FIGURE 1** Role of monitoring in an emergency contaminant response system.

- high specificity (low cross reactivity);
- high reproducibility;
- can detect many contaminants (broad spectrum);
- qualitative and quantitative;
- low rate of false positives/false negatives;
- rugged and minimal maintenance required;
- easy to use (little technical expertise required);
- inexpensive;
- communicates results to off-site responders.

Although many of the currently available on-line monitoring technologies that are being considered for use as part of CWSs display some of these characteristics, none of the available technologies currently meets all of the objectives stated above.

## 5 MULTIOBJECTIVE MONITORING PROGRAMS

As previously discussed, monitoring programs can serve many purposes in a water-supply system. Design of a single purpose monitoring system to address water security issues is

costly and frequently water utilities are unable or unwilling to make sufficient expenditures to develop a robust water security monitoring system. However, if the monitoring program can also serve additional purposes such as water quality characterization and process control, then the expenditures may be more easily justified. The primary issues in the design of a multiobjective monitoring program are the clear definition of the monitoring objectives and the design of a system that will adequately serve all desired objectives.

## 6 REVIEW OF MONITORING METHODS

Monitoring can be broadly characterized as (i) on-line continuous monitors and (ii) manual field level or laboratory analysis. As previously described, on-line monitors are typically used as a broad-scale method for detection of aberrations that may be contaminants in source or finished water while manual methods (either in the field or laboratory) serve as a means of confirming or characterizing the nature of the contamination.

On-line monitors may be further classified as physical/chemical sensors and biosensors. In most cases, on-line physical/chemical sensors measure changes in indicator parameters, such as chlorine, color, pH, conductivity, total organic carbon (TOC), and so on, individually or in a multiparameter analysis in order to detect a "change of state" of the water as a method of inferring the presence of a contaminant. In a few cases, on-line monitors may actually measure the concentration of one or more parameters. Table 1 summarizes the characteristics of on-line physical and chemical sensors.

On-line biosensors utilize biological species (e.g. fish, algae, mollusks, Daphnia, and bacteria) as sentinels for toxic contaminants. These are considered to be whole-organism sentinels that measure changes in physiology or behavior of living organisms resulting from stresses induced by toxins. This is similar to the "canary in the coal mine" that was used to determine the presence of carbon monoxide in the mine prior to entry by miners. Biosensors may suggest that there is something unusual in the water but do not identify the specific toxin. They monitor various characteristics of the biospecies to determine if they are stressed or responding to the potential presence of a contaminant. Biosensors indicate actual toxicity and can detect combined or synergistic effects of multiple toxins. Historically, biosensors have been used as part of source water EWSs for well over a quarter of a century. They are currently being applied in experimental cases to distribution systems. The primary needed change is that the water must be dechlorinated prior to use in the biosensor. Table 2 summarizes the characteristics of biosensors.

For both physical/chemical and biosensor approaches, prior to the actual use of the sensors as part of a CWS, a parameter baseline must be established. In this phase, the monitor is applied over a period (typically several months to a year) to establish the normal range and pattern of parameter values that would be expected. Additionally, the relationship between changes in parameters and the presence of specific contaminants must be understood. Computerized data systems may be used to analyze and report on significant changes in parameters indicating the potential presence of a contaminant [6, 7].

There is considerable recent and ongoing research in physical/chemical and biosensors in both the water industry and in other areas, such as the chemical, food processing, and medical industries. As a result, many technologies are emerging and being tested and can be expected to become commercial products within the 1–10 year horizon.

**TABLE 1 Summary of On-line Physical and Chemical Sensors**

| Category | Characteristics | Example Technologies |
|---|---|---|
| On-line analytical probes | Relatively inexpensive<br>Easy to use<br>Can provide continuous monitoring with remote access to data<br>Available from a variety of manufacturers | Ion-selective electrodes<br>pH<br>Elemental anions (e.g. Cl, Br)<br>Ammonium<br>Nitrate/Nitrite<br>Certain metals (e.g. Pb, Cn)<br>Surfactants<br>Hardness<br>dissolved oxygen (DO) probes<br>Multiple probe systems |
| Multiarray sensor | Replaceable ceramic chip<br>In-pipe or side stream | pH, $Cl_2$, DO, oxygen-reduction potential (ORP), temperature, conductivity |
| General organic chemical parameters | Provide gross measure of organic content<br>Analysis can be performed in batch mode or on-line<br>TOC or UV254 | TOC analyzers<br>Multi-wavelength spectrometer |
| Oil and petroleum | Light scattering detects floating oil<br>Fluorometry detects dissolved gasoline, diesel, jet fuel, BTEX, and so on | |
| Specific organic chemicals | GC detects volatile organic compounds (VOCs), fuel oil components<br>Mass spectrometry | Continuous on-line GC monitor for VOCs in water<br>On-line photo ionization (PI)/mass spectrometry–PI and quadrupole ion trap, time of flight mass spectrometry<br>GC/MS: in situ probe purge and trap GC/MS system |
| Radioactivity | Need to measure alpha, beta, and/or gamma radiation<br>Limited number of models currently available<br>Relatively expensive | |

Criteria for the selection of monitoring technology should reflect local objectives and include the following:

- cost (capital and operational);
- spectrum (broad spectrum or specific constituent);
- sensitivity;
- operational and maintenance requirements;
- environmental requirements (power, shelter);
- sampling frequency;
- communications requirements.

**TABLE 2 Summary of Biosensors**

| | |
|---|---|
| Daphnia toximeter | Several daphnids (water fleas) housed in a glass chamber through which sample water continuously flows |
| | Swimming behavior (speed, altitude, etc.) monitored by closed circuit TV and analyzed via integrated PC |
| | Extensively used in Europe and during Salt Lake City Olympics |
| Mussel monitors | Mussels avoid toxins in water by closing shells |
| | Mussel shells are glued to top of the flow-through unit. Valve opening and closing are monitored by high-frequency induction sensors attached to shells |
| | Mussels utilized include clams, oysters, blue mussels, and zebra mussels |
| Algae toximeter | Algae are cultured continually in a fermentor |
| | Test water flowing continually through the toximeter and algae is automatically injected into the measurement chamber |
| | Amount of living chlorophyll is measured by fluorescence technique |
| | Algae sensor is interfaced with a PC |
| Fish sentinel system | Utilize fish swimming in chambers |
| | Computer-linked (noncontact) electronic sensors monitor physiological responses (ventilatory frequency, ventilatory depth, etc.) and whole-body movement |
| | Changes in activity or physiological responses can signal toxic contamination |
| Bacterial monitoring system | Utilize either freeze-dried or customer-activated bioluminescent bacteria |
| | Reduction in luminescence suggests toxicity in water |

A detailed review of monitoring technology is available in *Technologies and Techniques for Early Warning Systems to Monitor and Evaluate Drinking Water Quality: A State-of-the-Art* [8] and *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System* [9]. Independent reviews of selected monitoring technologies have been conducted by EPA as part of their Environmental Technology Verification (ETV) program and Technology Testing and Evaluation Program (TTEP). Under the WaterSentinel (formerly called *WaterSentinel*) initiative, EPA is establishing a critical early warning detection capability in selected cities as a means of encouraging other cities to adopt monitoring and surveillance programs [10].

## 7 OPTIMAL MONITORING LOCATIONS

Roberson and Morley [11] state that "once a utility has determined the potential contaminants that need to be monitored and what monitoring technologies are appropriate, the utility must determine where to locate the sensors and how often to monitor. Monitoring could be conducted in the raw water sources, in the treatment plant, or in the distribution system. Many consider the distribution system to be the most vulnerable, so a significant portion of contamination monitoring research has focused on that portion of the water system."

Historically, monitoring sites have been selected primarily on the basis of informal selection criteria that reflect the representativeness and accessibility of the sites and

the specific purpose(s) of the monitoring system. However, with the increasing costs associated with more sophisticated monitors and the perceived need for greater coverage, attention has turned to more quantitative assessment tools. Optimization techniques that formally define specific objectives for the monitoring system and search for and evaluate alternative systems have been the subject of research and development.

In the pre-9/11 era, primary emphasis in the design of water quality monitoring systems was on systems that addressed regulatory requirements, process control, and identification of contamination associated with accidental spills. In water distribution networks, the initial use of models to select water quality sampling locations is attributed to Lee et al. [12] using the concept of coverage of a network by tracing flow pathways and evaluating the effectiveness of monitors to "cover" the network. Although other papers built upon the concept of coverage to select optimal monitor locations using alternative solution methods, such as mixed-integer programming and genetic algorithms, the primary emphasis was still upon identifying problems in the distribution system of water quality that gradually deteriorated [13–15]. Other applications addressed the case of rapid deterioration of water quality due to an external source of contamination of the distribution system. Kessler et al. [16] applied an "all-shortest-path" algorithm to determine the least time that it will take for the contaminant to travel from the pollution source to any other node and a minimum set covering algorithm (equivalent to a minimum cost) to select the optimal set of monitors. Grayman and Males [17] used Monte Carlo simulation to evaluate alternative water quality monitoring systems used as part of a source water EWS for detecting accidental spills in the Ohio River.

The context for selection of monitoring locations changed dramatically following the events of September 2001. Whereas previously, the objective of the monitoring stations was to identify rapid deterioration of water quality within a distribution system or due to accidental external contamination of the distribution system, after 2001, the emphasis changed to identification of intentional contamination of the distribution system. Within this context, monitors (sensors) were assumed to be part of an EWS.

Berry et al. [18] provide a succinct description of the sensor placement problem in the post-2001 era. "For EWS design, the goal of a sensor placement optimization formulation is simple: to place a limited number of sensors in a water distribution network such that the impact of an accidental or intentional injection of contaminant to public health is minimized. However, no specific, concrete formulation for sensor placement has emerged that is widely accepted by the water community. There are a wide range of alternative objectives that are also important when considering sensor placements, such as minimizing the cost of installing and maintaining the sensors, minimizing the response time to a contamination event, and minimizing the extent of contamination (which impacts the recovery costs). Additionally, it is difficult to quantify the health impact of a contamination event because human water usage is often poorly characterized, both in terms of water consumption patterns as well as how the water consumption impacts health effects. Consequently, surrogate measures like the total volume of water consumed at all sites have been used to model health impacts; this measure assumes that human water consumption is proportional to water consumption at all junctions within the network."

Since 2001, there has been extensive research in the development of algorithms for the optimal monitor location in order to detect an intentional contamination event. These

algorithms can be categorized as static models and dynamic models [18]. Static models simply consider whether an attack can reach a downstream population, whereas dynamic models use the temporal dynamics of contaminant flow to determine whether a downstream population is affected before the contaminant is detected. Since dynamic models represent the actual temporal variation in flow conditions in a distribution system, they are considered to be more realistic and are the subject of most ongoing research. The algorithms and solution methodologies have included various optimization techniques and heuristics to select monitor locations including mixed-integer programming [19], greedy heuristics [20], and genetic algorithms [21]. Other studies have considered the multiobjective analysis [22] and incorporated the effect of stochastic processes on selection of sensor locations [23].

Optimization and heuristic algorithms have been used to determine the best location of monitors in several real and hypothetical distribution systems. The largest application of such algorithms is EPA's Threat Ensemble Vulnerability Assessment (TEVA) program. Alternative sensor location algorithms have been used to identify the optimal sensor placement in large- and medium-sized water distribution systems [24]. The Monte Carlo simulation approach is used to evaluate alternative sensor locations, number of sensors, sensor characteristics, sampling frequency, response time, and the type and duration of the contamination events. The sensors are assumed to be part of a contaminant warning system and the performance assessed on the basis of minimizing the average number of persons who become ill from exposure to a contaminant. The average number of people who become ill is determined by examining nearly all possible contamination intrusion points. As part of the TEVA program, EPA and Sandia National Laboratories have developed the Sensor Placement Optimization Tool (SPOT) [25]. At this time, the availability and distribution of this tool has not been established by EPA.

Several methodologies for selecting sensor locations were tested as part of the Battle of the Water Sensor Networks with the results presented at the 2006 Water Distribution Systems Analysis Symposium [26]. This exercise objectively compared the performance of contributed sensor network designs, consisting of a set of sensor locations. Independent research teams and practicing engineers contributed their designs for two different water distribution networks (small 100-node system and large 12,000-node system). Each team was asked to develop designs according to a precise set of rules to facilitate design comparisons. These rules specify the design performance metrics, the characteristics of contamination events, and the detection technology used to raise an alarm. Contributed sensor network designs were evaluated using four quantitative design objectives: expected time of detection, expected population affected prior to detection, expected contaminated water demand prior to detection, and expected likelihood of detection. In another study, application of water distribution modeling in selecting sensor locations was demonstrated in a "red team–blue team" exercise designed for educational purposes [27].

An alternative ranking procedure for locating monitors in a distribution system was developed as part of the PipelineNet project developed by Science Applications International Corporation (SAIC) in conjunction with EPA, AwwaRF, Federal Emergency Management Agency (FEMA), and the interagency Technical Support Working Group [28]. In this approach, "initially, all the elements of the water distribution system are

available for monitoring. This universe is reduced to a smaller set based on priorities set by a water utility. These priorities may include physically accessible nodes, definition of priority areas based on flow, velocity, pressure and water quality, and proximity to critical facilities (i.e. schools and hospitals). Among the specific issues to be addressed are: (i) location of monitoring points in the distribution system, (ii) timing and frequency of monitoring, and (iii) monitoring techniques and water quality parameters." Though this methodology does not ensure an optimal solution, it can help a water utility to define the specific objectives of a monitoring plan and to design a monitoring system that is tailored to those objectives.

## 8 CASE STUDY

In order to demonstrate the design process for an on-line water quality monitoring program, a case study for Ann Arbor, Michigan is presented [29]. The Ann Arbor city's water system provides drinking water to about 130,000 customers and operates a distribution system that provides service to approximately 40 square miles of the city and surrounding customer communities. Increasing concerns about the water quality within this distribution system as well as concerns about potential contamination events within the distribution system led to the development of a comprehensive monitoring plan. To understand the issues and develop solutions, the city's water utility undertook an evaluation of how to select and locate water quality monitoring equipment most effectively to meet these multiple goals. The study was conducted as a joint effort between utility personnel and an interdisciplinary team assembled by the Camp Dresser Mckee (CDM) consulting engineering firm. The following activities were pursued as part of the Ann Arbor project:

1. *Define mission and objectives.* A representative group of utility managers and staff met in a facilitated setting to develop a mission statement for the project, establish a project schedule, and to define specific objectives to monitor design. The overall objective was defined as, "creating an optimized distribution system detection and monitoring network with respect to both contamination events and normal variation in system quality".
2. *Survey current industry practices in on-line monitoring.* A 1-day expert workshop on on-line monitoring was conducted for the utility. A questionnaire on current monitoring practices was developed and sent to key progressive water utilities based on the review of the literature and the workshop. Follow-up phone calls and site visits to selected utilities, research laboratories, and monitoring manufacturers provided information for the preparation of a project report on the state of the art of on-line monitoring.
3. *Identify and rank potential monitoring sites.* Utility personnel developed a list of 179 potential monitoring sites. This listing included current monitoring/sampling locations, utility facilities, public buildings including fire stations, and university and public school buildings in the city. The list of sites was subsequently reduced to 30 locations based primarily on accessibility. Each of these 30 field locations was visited, data were collected, and the sites were numerically ranked based on

the ownership of the site, availability of a connection to the distribution system, availability of power, communications, and existing heating, ventilating, and air conditioning (HVAC), and accessibility.

4. *Identify and test candidate monitors.* Based on the project objectives and the review of the state of the art of on-line monitoring, key parameters of interest were identified. Parameters were selected to serve either as water security indicators or water quality indicators or, as in the case of total chlorine, as indicators for both objectives. One or two candidate monitors were identified for each of these parameters and test instruments obtained from manufacturers. These instruments were each challenged with four different water sources (raw river water and groundwater, finished drinking water and one distribution system location). Pilot testing on each water type was performed for 1–3 weeks. Results were compared to the approved bench testing methods normally employed by the utility.
5. *Adapt and test water system hydraulic model.* A key element in the quantitative design of the optimum monitoring network was a hydraulic model of the Ann Arbor distribution system. An all pipes, extended period simulation model was available at the start of the project. Some adaptation was required in order to update the model to current conditions and to represent different seasonal/water usage periods. Further changes were made during a validation period that identified some inaccurate valve positions that resulted in improper prediction of the movement of water through the system.
6. *Apply modeling tools.* The monitoring design phase resulted in the development of a phased program for implementing different types of monitors at different locations within the distribution system. The primary tools that were used in this task were the TEVA and PipelineNet software products. The study team worked with EPA using the TEVA models and SAIC, developer of the PipelineNet model, in application of these tools. Both models require a significant policy-related input to guide their usage. The TEVA model was used to select the most effective locations for monitors that would be part of a CWS for intentional events. Input to this model included expected response times, critical seasonal cases, and the duration of contamination events, and was determined through facilitated sessions with utility staff. Figure 2 shows an example graphical output with the reduction in health effects plotted as a function of the number of monitors and the expected response time. As illustrated, the results are very sensitive to response time. The graphs also show that the benefits increase significantly for up to five monitors and then level off beyond that number. The models were applied for both the case where all locations in the distribution system were candidates for monitors and for the case where only the 30 top ranked sites were considered. A “regret analysis” showed that the loss in benefits associated with consideration of only these 30 sites, as compared to all locations, was relatively small indicating that the increased accessibility and lower costs associated with this subset of candidates was justified. PipelineNet was used to identify locations for monitors for real-time assessment of water quality. In a facilitated group meeting, Ann Arbor personnel identified surrogate parameters that would be indicative of potential water quality problems and provided weights for prioritizing these parameters. These included velocity, water age, and pipe roughness. PipelineNet was then used to rank water

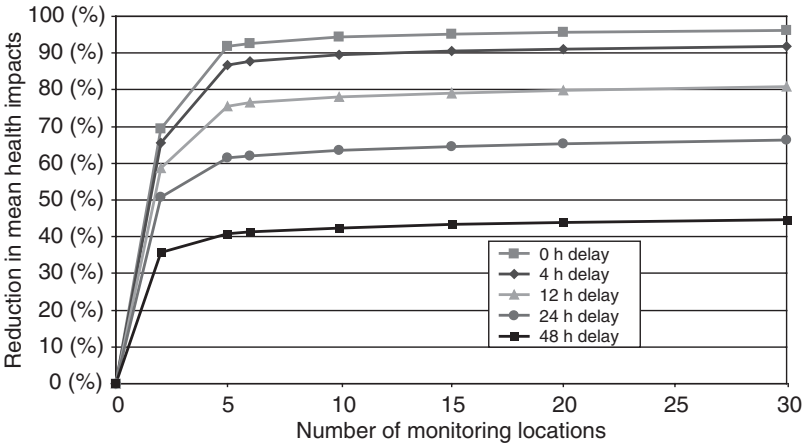



**FIGURE 2** Impact of response delay.

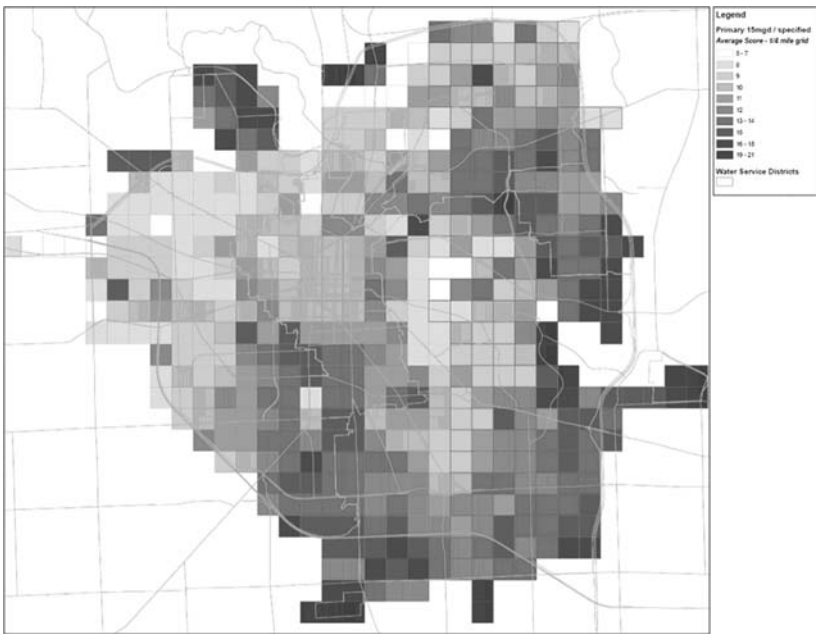



**FIGURE 3** Water quality ranking for alternative monitoring locations.

mains in the system based on these factors. This data was used to assess general water quality conditions in each one quarter square mile using a grid-based output shown in Figure 3.

7. *Select monitoring locations.* The results of the application of the TEVA and PipelineNet models were used to develop a prioritized list of monitoring locations. In general, there was no significant overlap in the location of monitors selected for water security as opposed to those selected for detection of water quality

problems. This lack of co-occurring sites was caused by the different drivers for security monitoring (protect as much population as possible) versus water quality monitoring (find the areas of deteriorating water quality, typically associated with high water age and, therefore, in more remote or isolated parts of the distribution system). Based on these results, several sites were selected for security monitoring and several locations were selected for water quality monitoring. One of the sites selected for security was the same as a site selected for water quality.

8. *Phased implementation plan.* A phased implementation plan has been developed for the monitoring program. In the first phase, two monitoring systems will be implemented at high-priority sites. During this phase, the CANARY event detection software developed by EPA/Sandia [30] will be tested. In a second phase, based on the results of the first phase, additional monitoring stations will be established at the remaining high-priority sites.

## 9 SUMMARY AND CONCLUSIONS

A contaminant warning system using on-line monitors for detection, linked with a coordinated emergency response plan, can serve as a mechanism for responding to intentional contamination events. With proper design, such systems can serve other purposes such as identification of more routine water quality problems. There has been a large surge in research in the area of design of optimum monitoring systems. However, significant research is still needed in the development of economical, robust on-line monitors and of software to evaluate rapidly the output from on-line monitors to identify the onset of contamination events.

## ACKNOWLEDGMENTS

The author would like to express his appreciation to the following individuals for their many helpful suggestions and contributions to the case study: Sumadh Bahl, Mark Ten-Broek, Janice Skadsen, Rob Janke, and William Samuels. He would also like to thank Stanley States and Alan Roberson for their insight and knowledge in the joint development of AWWA's contamination monitoring technologies workshop.

## REFERENCES

1. ILSI (1999). *Early Warning Monitoring to Detect Hazardous Events in Water Supplies*, T. M. Brosnan, Ed. International Life Sciences Institute, Washington DC.
2. Gullick, R. W., Grayman, W. M., Deininger, R. A., and Males, R. M. (2003). Design of early warning monitoring systems for source waters. *J. AWWA* **95**(11), 58–72.
3. Grayman, W. M., Vicory, A. H., and Males, R. M. (2000). Early warning system for chemical spills on the Ohio River. In *Security of Public Water Supplies*, R. A. Deininger, P. Literathy, and J. Bartram Eds. Kluwer Academic Publishers, Dordrecht, pp. 91–100.
4. Deininger, R. A. (1987). The survival of Father Rhine. *J. AWWA* **79**(7), 78–83.
5. USEPA (2003). *Response Protocol Toolbox: Planning for and Responding to Drinking Water Contamination Threats and Incidents*, USEPA Office of Water, Washington DC.

6. Cook, J. B., Byrne, J. F., Daamen, R. C., and Roehl, E. A. (2006). Distribution system monitoring research at Charleston Water System. In *Proceedings of the 8th Annual Water Distribution Systems Analysis Symposium*, University of Cincinnati, Cincinnati, OH.
7. McKenna, S. A., Klise, K. A., and Wilson, M. P. (2006). Testing water quality change detection algorithms. In *Proceedings of the 8th Annual Water Distribution Systems Analysis Symposium*, University of Cincinnati, Cincinnati, OH.
8. USEPA (2005). *Technologies and Techniques for Early Warning Systems to Monitor and Evaluate Drinking Water Quality: A State-of-the-art Review*, USEPA, Washington DC. Available at: http://www.epa.gov/nhsrc/pubs/reportEWS120105.pdf.
9. ASCE (2004). *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*, December 9, 2004, ASCE, WEF, AWWA, Reston, VA. Available at: http://www.asce.org/static/1/wise.cfm.
10. Janke, R., Murray, R., Uber, J., and Taxon, T. (2006). Comparison of physical sampling and real-time monitoring strategies for designing a contamination warning system in a drinking water distribution system. *J. Water Res. Plann. Manage*. **132**(4), 310–313.
11. Roberson, J. A., and Morley, K. M. (2005). *Contamination Warning Systems for Water: An Approach for Providing Actionable Information to Decision-makers*, AWWA, Denver, CO.
12. Lee, B., Deininger, R., and Clark, R. (1991). Locating monitoring stations in water distribution systems. *J. AWWA*. **83**(7), 60–66.
13. Kumar, A., Kansal, M. L., and Arora, G. (1997). Identification of monitoring stations in water distribution system. *J. Environ. Eng*. **123**(8), 746–752.
14. Tryby, M., and Uber, J. G. (2001). Representative water quality sampling in water distribution systems. In *Proceedings of the World Water & Environmental Resources Congress*, EWRI, ASCE, Orlando, FL.
15. Al-Zahrani, M. A., and Moied, K. (2001). Locating optimum water quality monitoring stations in water distribution system. In *Proceedings of the World Water & Environmental Resources Congress*, EWRI, ASCE, Reston, VA.
16. Kessler, A., Ostfeld, A., and Sinai, G. (1998). Detecting accidental contaminations in municipal water networks. *J. Water Res. Plann. Manage.* Reston, VA, ASCE, **124**(4), 192–198.
17. Grayman, W. M., and Males, R. M. (2002). Risk-based modeling of early warning systems for pollution accidents. *Water Sci. Technol.* London, UK **46**(3), 41–49.
18. Berry, J. W., Hart, W. E., Phillips, C. A., Uber, J. G., and Watson, J.-P. (2005). Validation and assessment of integer programming sensor placement models. In *Proceedings of the World Water & Environmental Resources Congress*, EWRI, ASCE, Reston, VA.
19. Berry, J. W., Fleischer, L., Hart, W. E., Phillips, C. A., and Watson, J.-P. (2005). Sensor placement in municipal water networks. *J. Water Res. Plann. Manage., ASCE* **131**(3), 237–243.
20. Uber, J., Janke, R., Murray, R., and Meyer, P. (2004). *Greedy Heuristic Methods for Locating Water Quality Sensors in Distribution Systems*, World Water & Environmental Resources Congress, EWRI, ASCE, Reston, VA.
21. Ostfeld, A., and Salomons, E. (2004). *A Stochastic Early Warning Detection System Model for Drinking Water Distribution Systems Security*, World Water & Environmental Resources Congress, EWRI, ASCE, Reston, VA.
22. Watson, J.-P., Greenberg, H. J., and Hart, W. E. (2004). *A Multiple-objective Analysis of Sensor Placement Optimization in Water Networks*, World Water & Environmental Resources Congress, EWRI, ASCE, Reston, VA.

23. McKenna, S. A., and Yarrington, L. (2005). *Impact of Sensor Performance on Protecting Water Distribution Systems from Contamination Events*, World Water & Environmental Resources Congress, EWRI, ASCE, Reston, VA.

24. Janke, R., Murray, R., Uber, J., and Allgeier, S. (2005). *An Evaluation of System Architectures for Contamination Warning Systems*, World Water & Environmental Resources Congress, EWRI, ASCE, Reston, VA.

25. Murray, R., Berry, J. W., and Hart, W. E. (2006). *Sensor Network Design for Contamination Warning Systems: Tools and Applications*, Water Security Congress, American Water Works Association, Denver, CO.

26. Ostfeld, A., Uber, J., and Salomons, E. (2006). Battle of the Water Sensor Networks (BWSN): a design challenge for engineers and algorithms. In *8th Annual Water Distribution Systems Analysis Symposium*, University of Cincinnati, Cincinnati, OH (available at: http://www.esnips.com/web/ostfeld).

27. Grayman, W. M., Ostfeld, A., and Salomons, E. (2006). Locating monitors in water distribution systems: a red team-blue team exercise. *J. Water Res. Plann. Manage., ASCE*, Reston, VA **132**(4), 300–304.

28. Bahadur, R., Samuels, W. B., and Pickus, J. (2003). *Case Study for a Distribution System Emergency Response Tool*, AwwaRF Project No. 2922, AwwaRF, Denver CO.

29. Bahl, S., Sanford, L., Steglitz, B., Perala, P., Grayman, W., Janke, R., Samuels, W., Skadsen, J., Cipparone, L., Rego, C., and TenBroek, M. (2006). City of Ann Arbor's multi-objective monitoring location strategy. In *Proceedings of the 8th Annual Water Distribution Systems Analysis Symposium*, University of Cincinnati, Cincinnati, OH.

30. Hart, D., McKenna, S. A., Klise, K., Cruz, V., and Wilson, M. (2007). *CANARY: A Water Quality Event Detection Algorithm Development Tool*, World Water & Environmental Resources Congress, EWRI, ASCE, Reston, VA.

## FURTHER READING

EPA (2005). *Technologies and Techniques for Early Warning Systems to Monitor and Evaluate Drinking Water Quality: A State-of-the-Art Review*. Available at: http://www.epa.gov/NHSRC/pubs/600r05156.pdf

ASCE (2004). *Interim Voluntary Guidelines for Designing an Online Contaminant Monitoring System*. Available at: http://www.asce.org/static/1/wise.cfm.

EPA (2007). *Interim Guidance on Planning for Contamination Warning System Development*. EPA 817-R-07-002. Available at: http://www.epa.gov/software/watersecurity/pubs/guide_watersecurity_securityinitiative_interimplanningpdf.pdf

EPA **ETV** (Environmental Technology Verification) and **TTEP** (Technology Testing and Evaluation) programs. *Tests Various Monitors*, For information see: http://www.epa.gov/etv/ and http://www.epa.gov/nhsrc/ttep.html, 2008.

EPA ***W**ater **C**ontaminant **I**nformation **T**ool (WCIT)*, For information see: http://www.epa.gov/wcit/, 2008.

EPA TEVA (Threat Ensemble Vulnerability Assessment) For information see: http://www.epa.gov/nhsrc/water/teva.html, 2008.

USEPA (2006). *Water Distribution System Analysis: Field Studies, Modeling and Management A Reference Guide for Utilities*, http://www.epa.gov/nrmrl/pubs/600r06028/600r06028.pdf.

# EMERGENCY RESPONSE PLANNING FOR DRINKING WATER SYSTEMS

LINDA WARREN
*Launch Consulting, Richland, Washington*
SANDRA DAVIS
*ECO Resource Group, Bainbridge Island, Washington*
CHRISTOPHER T. CYR
*Critigen, Portland, Oregon*

## 1 INTRODUCTION

Emergency response planning is designed to support operations during any type of emergency, and is built on the principles set forth in the National Incident Management System (NIMS) and the National Response Framework (NRF). Emergency Response Plans (ERPs), also known as *emergency operations plans*, serve as guidances for agencies and staff, should an incident occur. The ERP documents are required for water agencies by the Bioterrorism Act, and are suggested for any agency. A basic ERP should provide staff with procedures and contact information for use during potential emergency events for which the agency should prepare [particularly events identified as threats in the vulnerability assessment (VA)]. ERPs should be one part of an overall preparedness program that includes staff training, emergency exercises, business continuity planning, and yearly revisions. Such a program has the goal of utility resiliency. Any ERP should be consistent with other agency plans, as well as local ERPs, and should be developed in coordination with stakeholders.

### 1.1 Return on Investment for a Utility Preparedness Program

Preparedness planning and exercises can make even a major emergency more manageable and help speed recovery efforts. Utility emergency plans have been used to help save lives and property after a disaster. Emergency protective measures require capital; the return on investment of preparedness planning comes from the results of being prepared when a potentially costly or dangerous event occurs. This can be measured in lives saved, uninterrupted service/quickly restored service, and lower insurance rates on account of having an ERP.

The time and cost to develop a plan is well worth the reputation of dependability that is gained with customers by having an ERP. Although a utility's reputation with customers and local decision-makers is not an obvious operational issue, no utility can function properly without customer confidence and local support. A properly developed

and publicized ERP can go a long way toward consumer confidence, bringing consumer use and support to help secure funding for all utility programs.

## 2 LEGISLATION AND DIRECTIVES

There are several Homeland Security Presidential Directives (HSPDs) and federal laws that affect emergency planning for water and wastewater utilities. These are often evolving, and utilities can find the latest HSPD information at the Department of Homeland Security (DHS) web site: http://www.dhs.gov/xabout/laws/editorial_0607.shtm.

Emergency planning should address relevant and applicable water and wastewater utility emergency planning and response requirements, including, but not limited to, the following.

The *Public Health Security and Bioterrorism Preparedness and Response Act of 2002* (PL 107-188) requires community water systems to conduct VAs under the authority of the US Environmental Protection Agency (USEPA). The law requires water utilities that serve more than 10,000 customers to develop or revise an ERP.

***HSPDs*** establish nationwide policies and approaches for federal, state, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity, using a NIMS and Incident Command System (ICS). The National Integration Center (NIC) Incident Management Systems Division has been established as the lead federal entity to coordinate NIMS compliance. Specific HSPDs relevant to ERPs include, but are not limited to, the following (http://www.dhs.gov/xabout/laws/editorial_0607.shtm):

*HSPD 3—Homeland Security Advisory System.* HSPD 3 creates a Homeland Security Advisory System to inform all levels of government and local authority, as well as the public, about the current risk of terrorist acts. The system involves a five-level, color-coded Threat Condition indicator to correspond to the current situation. Agency-specific protective measures associated with each Threat Condition allow a flexible, graduated, and appropriate response to a change in the nation's level of risk [1].

*HSPD 5—Management of Domestic Incidents.* HSPD 5 serves to enhance the ability of the United States to manage domestic incidents by establishing a single, comprehensive NIMS. NIMS is designed to cover the prevention, preparation, response, and recovery from terrorist attacks, major disasters, and other emergencies. The implementation of such a system would allow all levels of government throughout the nation to work efficiently and effectively together. The directive gives further detail on which government officials oversee and have authority for various parts of the NIMS. HSPD 5 also establishes that utility staff are first responders and must be trained as such [2].

*HSPD 7—Critical Infrastructure Identification, Prioritization, and Protection.* HSPD 7 establishes a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from terrorist attacks. The directive defines relevant terms and delivers 31 policy statements. These policy statements define what the directive covers and the roles various federal, state, and local agencies will play in carrying it out [3].

*HSPD 8—National Preparedness and Annex 1, National Planning.* HSPD 8 establishes policies to strengthen the United States' preparedness in order to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies. The directive requires a national domestic all-hazards preparedness goal, with established mechanisms for improved delivery of federal preparedness assistance to state and local governments. It also outlines actions to strengthen preparedness capabilities of federal, state, and local entities. This is a companion directive to HSPD 5. Most utilities are one of the local entities that can receive federal assistance [4].

*HSPD 21—Public Health and Medical Preparedness.* It is the policy of the United States to plan and enable provision for the public health and medical needs of the American people in the case of a catastrophic health event through continual and timely flow of information during such an event, and rapid public health and medical response that marshals all available national capabilities and capacities in a rapid and coordinated manner. Utility staff, as first responders, are among those with priority for flu vaccines [5].

*Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended by Public Law 106-390, October 30, 2000* (the Stafford Act), authorizes the President to issue major disaster or emergency declarations in response to catastrophes that overwhelm state and local governments. Such declarations result in the distribution of a wide range of federal aid to individuals and families, certain nonprofit organizations, and public agencies. The forms of assistance authorized by the Stafford Act include temporary housing, grants for personal uninsured needs of families and individuals, repair of public infrastructure, emergency communications systems, and other forms of assistance. Congress appropriates money for activities authorized by the Stafford Act to the Disaster Relief Fund (DRF), which is administered by the Federal Emergency Management Agency (FEMA) within the DHS. Appropriations to the DRF remain available until expended. Utilities are able to apply for disaster mitigation funding [6].

## 3 EMERGENCY RESPONSE PLANNING WITHIN THE BUSINESS CONTINUITY PLANNING UMBRELLA

Unlike ERPs, which focus on disaster response activities, a business continuity plan (BCP) defines how a utility continues its everyday business functions in a not-so-everyday environment. This includes the financial effects of a crisis, as well as adapting policies to meet the changing needs of employees and the utility, resuming normal operations, keeping and paying employees, keeping and billing customers, and staying in business. A utility may choose to organize its resiliency program under the BCP umbrella, and include the ERP as one of the plans within that umbrella (Fig. 1).

An enterprise business continuity plan (EBCP) serves as an umbrella plan for emergency preparedness, response, and recovery. The resultant plan for a utility will facilitate federal and state compliance efforts by streamlining the organization of numerous disparate plans and documents, some that are required by law.

A utility must review its plans to determine which plans or parts of plans can be combined to help form the overall EBCP, and which plans should remain stand-alone documents. While doing this, the utility should also develop an outline for the EBCP, and basic principles to adhere to during its development.

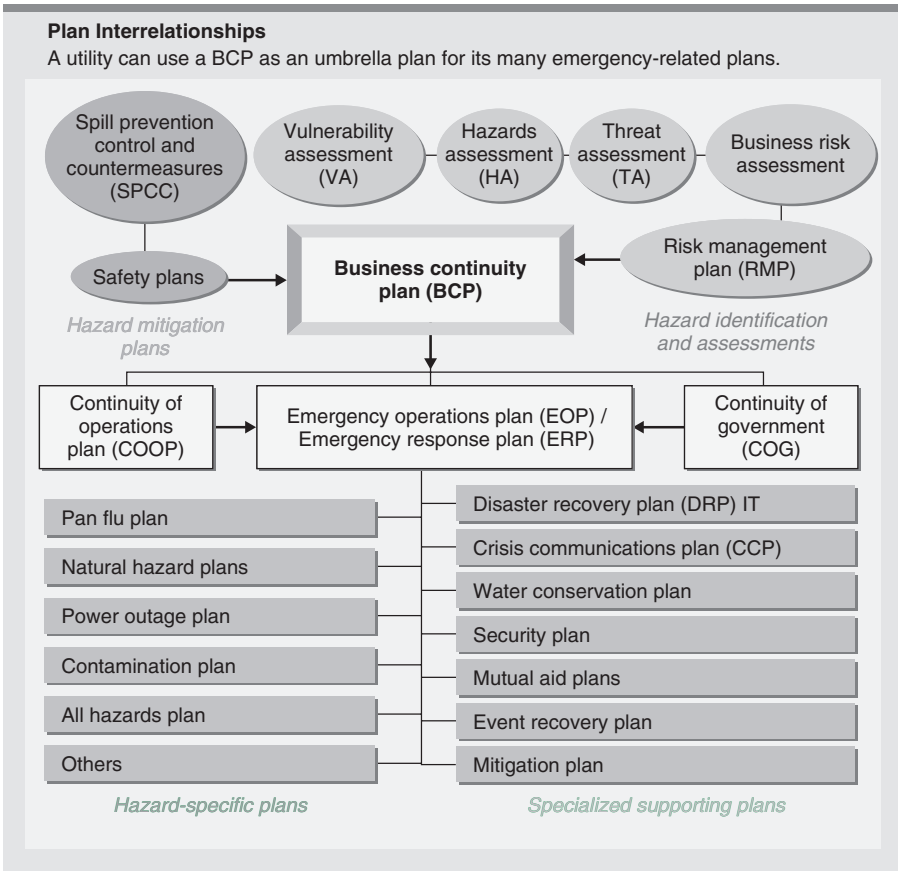



**FIGURE 1** Plan interrelationships (courtesy of AWWA [7]).

The utility may consider converting existing paper and electronic files into a common electronic format, like Microsoft Word, Excel, and Visio. This can be done using optical character recognition (OCR) software for any paper-only documents. Next, assemble the content of the electronic documents within a table of contents (TOC) according to the outline developed during the document review. Some content will be combined, revised, or discarded and the remaining content should undergo technical editing to catch any errors from the scanning and revising. Any plans that are required legally or contractually should be maintained in their full form within the EBCP or as an annex, but will still fall under the umbrella of the EBCP.

The restructured plan will designate how the content will be divided into discreet files and where cross-referencing the different plans (e.g. hyperlinks) can be used.

## 4 PHASES OF EMERGENCY MANAGEMENT

Emergency management involves five phases characterized in Figure 2: assessment, mitigation, preparation, response, and recovery. These phases occur based on an ongoing

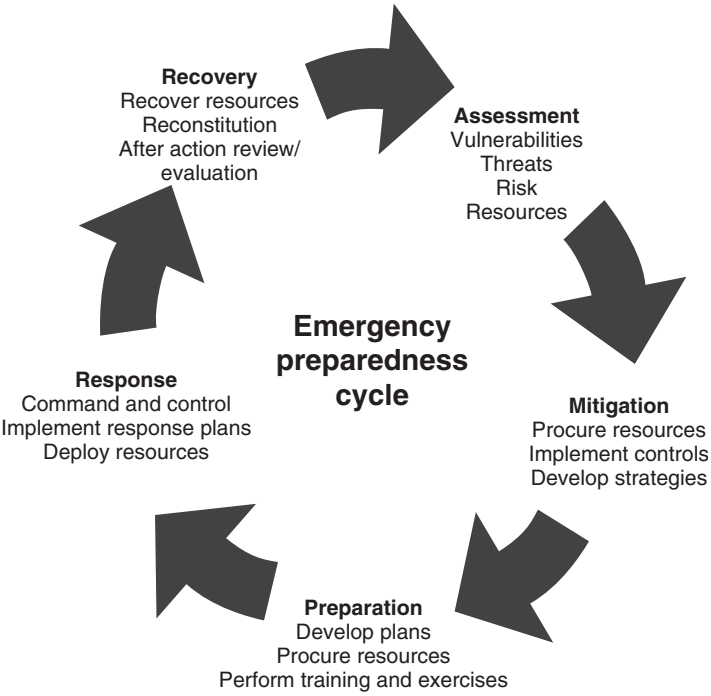



**FIGURE 2** Emergency preparedness cycle.

cycle that accounts for changes in operations, threats, vulnerabilities, and risks and builds upon lessons learned from exercises and actual incidents. This continuous cycle facilitates continuous improvement in emergency preparedness.

### 4.1 Assessment

The assessment phase comprises activities that increase the organization's understanding of the potential threats, vulnerabilities, and risks associated with facilities, operations, and personnel. The basic parameters of threat assessment include probability of occurrence and level of impact of a particular incident. Threats may include acts of terrorism, workplace violence, natural disasters, pathogenic outbreaks, chemical or radiological releases, explosions, and critical service interruptions. Applying potential threats to a specific facility allows assessment of vulnerability, which is the determination of specific factors that may increase or decrease the probability of occurrence. Information compiled via threat and VAs allows a general determination of risk for a particular facility or operation. Resource assessment identifies the pre- and postincident measures, equipment, personnel, and other resources in place to avert or minimize the impact of an incident.

### 4.2 Mitigation

Understanding threats, vulnerabilities, and risks, and the resources in place for incidents of concern allows mitigation planning. The mitigation phase comprises activities undertaken to lessen the occurrence of known and unknown hazards, and/or reduce the severity of

their potential impacts. During this phase, utility management will procure resources, implement controls, and develop strategies that serve to avert and/or minimize the impact of potential hazards in a prioritized manner based on the assessment phase. Examples of mitigation activities include relocating facilities and assets from flood-prone areas and enhancing physical and cyber-security measures against attack. Successful mitigation activities can greatly reduce the number of emergency event scenarios for which a utility would otherwise have to respond.

### 4.3 Preparation

The preparation phase involves developing overarching plans and hazard-specific plans, procuring preparedness resources, and training and exercising of response personnel. An ERP serves as the overarching response plan for all incidents occurring within a utility. Additional support annexes and procedures will augment an ERP for specific incidents, such as tornado response operations and chemical spills. Response planning also includes coordinating with response partners through joint training and exercises and mutual aid agreements; and procuring and prepositioning emergency resources and assets to where they will be most effective during a response.

### 4.4 Response

The response phase involves those actions taken to respond to and stabilize the impact of an emergency event. For events that are predictable to some extent, such as weather-related events, this can also include mobilization and preparatory actions taken immediately prior to the event (like positioning generators at pump stations). The primary objective of the response phase is to stabilize the situation and prevent loss of life and property and damage to the environment. The response phase will likely include the following tasks:

- activation of a utility's ICS and county, state, regional, and federal command and control systems;
- implementation of response, communications, operational, and other procedures contained in the ERP;
- deployment of resources and, as necessary, resource acquisition through the local Emergency Operations Center (EOC) that coordinates and accesses other local, state, and federal agencies.

The response phase can last from hours to days to weeks and may require 24/7 staff scheduling and emergency contractor support. The response phase will last until the Incident Commander determines that the event has terminated and demobilizes the Incident Command Team.

## 5 NATIONAL INCIDENT MANAGEMENT SYSTEM (NIMS) AND INCIDENT COMMAND SYSTEM (ICS)

Utility personnel, in addition to response partners, will implement the ICS when responding to an emergency event as set forth in the NIMS and the NRF. Emergency plans will go

into effect when an emergency event has occurred or a credible threat has been identified; employees may need to take on roles different from their everyday job during a disaster.

## 5.1 Incident Command System

ICS is a standardized on-scene emergency management system that provides for the adoption of an integrated organizational structure. ICS is the combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. It is used for all kinds of emergencies, and is applicable to small as well as large and complex incidents [8]. All utility staff must be trained in the basics of ICS to comply with federal laws; if a locality is not compliant then it may not receive federal funding/reimbursements from FEMA.

## 5.2 National Incident Management System

NIMS is a system mandated by HSPD-5 that provides a consistent nationwide approach for state, local, and tribal governments; the private sector; and nongovernmental organizations (NGOs) to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among state, local, and tribal capabilities, NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as ICS; multiagency coordination systems (MACSs); training; identification and management of resources (including systems for classifying types of resources); qualification and certification; and the collection, tracking, and reporting of incident information and incident resources.

## 5.3 NIMS Compliance

NIMS compliance is a requirement to receive federal emergency response and preparedness funding. All grant funding dealing with disaster mitigation, preparedness, and response requires compliance. The FEMA encourages utilities to take the following actions regarding NIMS compliance [9].

### *5.3.1 Adoption*

- Adopt NIMS for all departments/agencies; as well as promote and encourage NIMS adoption by associations, utilities, NGOs, and private sector emergency management and incident response organizations.
- Designate and maintain a single point of contact within government to serve as principal coordinator for NIMS implementation jurisdiction-wide (to include a principal coordinator for NIMS implementation within each department/agency).
- Ensure that Federal Preparedness Awards [to include, but not limited to DHS Homeland Security Grant Program and Urban Area Security Initiative (UASI) Funds] to state/territorial departments/agencies, as well as local governments, support all required NIMS compliance objectives.
- Audit agencies and review organizations should routinely include NIMS compliance requirements in all audits associated with Federal Preparedness Awards.

### *5.3.2 Planning*

- Revise and update emergency response/operations plans, standard operating procedures (SOPs), and standard operating guidelines (SOGs) to incorporate NIMS and NRF components, principles, and policies, to include planning, training, response, exercises, equipment, evaluation, and corrective actions.
- Promote and/or develop intrastate and interagency mutual aid agreements and assistance agreements (to include agreements with the private sector and NGOs).
- Include preparedness organizations and elected and appointed officials in the development of emergency response/operations plans.
- Plan for special needs populations in the development of ERPs (to include, but not limited to, individuals with limited English language proficiency, individuals with disabilities, children, the aged, etc.).
- Include preparedness organizations and elected and appointed officials in the development of ERPs.
- Plan for special needs populations in the development of ERPs (to include, but not limited to, individuals with limited English language proficiency, individuals with disabilities, children, the aged, etc.).

### *5.3.3 Training*

- Use existing resources such as programs, personnel, and training facilities to coordinate and deliver NIMS training requirements.
- Promote and encourage delivery of NIMS training (as identified in the Five-Year NIMS Training Plan Schedule, December 2007).
- Complete ICS-400 Advanced ICS training or equivalent by appropriate personnel (as identified in the Five-Year NIMS Training Plan, February 2008).
- Complete Emergency Management Framework Course—Awareness Training (as identified in the Five-Year NIMS Training Plan, February 2008)

### *5.3.4 Exercise*

- Incorporate NIMS concepts and principles into all appropriate state/territorial training and exercises.
- Plan for and/or participate in an all-hazards exercise program (e.g. Homeland Security Exercise and Evaluation Program) that involves emergency management/response personnel from multiple disciplines and/or multiple jurisdictions.
- Incorporate corrective actions into preparedness and response plans and procedures.
- Include NGOs and the private sector in an all-hazards exercise program, when appropriate.
- Promote the integration of ICS, MACS, and Public Information into appropriate exercises and evaluate against associated target capabilities [refer to Homeland Security Exercise Evaluation Program (HSEEP) Volume III and the Exercise Evaluation Guides].

### *5.3.5 Communications and Information Management*

- Apply common and consistent terminology as used in NIMS, including the establishment of plain language (clear text) communications standards.
- Utilize systems, tools, and processes to present consistent and accurate information (e.g. common operating picture) during an incident/planned event.
- Institute procedures and protocols for operational and information security during an incident/planned event.
- Institute multidisciplinary and/or multijurisdictional procedures and protocols for standardization of data collection and analysis to utilize or share information during an incident/planned event.
- Develop procedures and protocols for communications (to include voice, data, access to geospatial information, Internet/Web use, and data encryption), where applicable, to utilize or share information during an incident/planned event.

### *5.3.6 Resource Management*

- Inventory response assets to conform to NIMS National Resource Typing Definitions, as defined by FEMA Incident Management Systems Division.
- Ensure that equipment, communications, and data systems acquired through state/territorial and local acquisition programs are interoperable.
- Utilize response asset inventory for intrastate and interstate mutual aid requests [such as Emergency Management Assistance Compact (EMAC)], training, exercises, and incidents/planned events.
- Initiate state/territory-wide system to credential emergency management/response personnel to ensure proper authorization and access to an incident including those involving mutual aid agreements and/or assistance agreements.
- Inventory and type specific emergency management/response resources and assets to address unique needs beyond current "Tier One" NIMS National Resource Typing Definitions.
- Institute policies, plans, procedures, and protocols to prevent spontaneous deployment of resources/personnel and/or responding to a request that bypassed official resource coordination processes (i.e. resources requested through improper channels).
- Institute mechanisms to deploy, track, recover, demobilize, and to provide reimbursement for resources utilized during response and recovery.

### *5.3.7 Command Management*

- *ICS.* Manage all incidents/planned events in accordance with ICS organizational structures, doctrine, and procedures. ICS implementation must include the consistent application of Incident Action Planning (IAP), common communications plans, implementation of Area Command (AC) to oversee multiple incidents that are handled by separate ICS organizations or to oversee the management of a very large or evolving incident that has multiple incident management teams engaged, and implementation of unified command (UC) in multijurisdictional or multiagency incident management, as appropriate.

- *MACS.* Coordinate and support emergency management and incident response objectives through the development and use of integrated MACSs, that is, develop and maintain connectivity capability between local Incident Command Posts (ICPs), local 911 Centers, local EOCs, the state/territorial EOC and regional and/federal EOCs, and NRF organizational elements.
- *Public Information.* Institutionalize, within the framework of ICS, Public Information, [e.g. Joint Information System (JIS) and a Joint Information Center (JIC)] during an incident/planned event.
- Ensure that Public Information procedures and processes can gather, verify, coordinate, and disseminate information during an incident/planned event.
- Utilize access control measures during an incident, as appropriate.

### 5.4 NIMS Training

The FEMA has free on-line courses in emergency preparedness (www.fema.gov/prepared/train.shtm). The courses described in this section provide utilities with guidance as to how each Homeland Security Region collaboratively uses the NIMS and the ICS during emergency events.

*ICS 100: Introduction to Incident Command System.* ICS 100, introduces the ICS and provides the foundation for higher level ICS training. This course describes the history, features and principles, and organizational structure of the ICS. It also explains the relationship between ICS and the NIMS.

*ICS 200: ICS for Single Resources and Initial Action Incidents.* This course is designed to enable personnel to operate efficiently during an incident or event within the ICS. ICS-200 provides training on and resources for personnel who are likely to assume a supervisory position within the ICS.

*ICS 300: Intermediate ICS for Expanding Incidents.* This course provides training on and resources for personnel who require advanced application of the ICS. The target audience for this course is for individuals who may assume a supervisory role in expanding incidents or Type 3 incidents. These incidents may extend into multiple operational periods.

*ICS 400: Advanced ICS.* This course provides training on and resources for personnel who require advanced application of the ICS. The target audience for this course is senior personnel who are expected to perform in a management capacity in an AC or multiagency coordination entity.

*IS 700: National Incident Management System, An Introduction.* This course introduces and overviews the NIMS. NIMS provides a consistent nationwide template to enable all government, private sector, and NGOs to work together during domestic incidents.

*IS 800: National Response Framework, An Introduction.* The course introduces participants to the concepts and principles of the NRF [10].

### 5.5 NIMS/ICS Training for Utility Personnel

Utility upper management, middle managers, first-line supervisors, and certain entry level positions require appropriate NIMS compliance training. NIMS compliance for these units

will be based on FEMA recommendations for "predesignated first responders who are operationally driven during an emergency." This includes personnel who will be fulfilling responsibilities either in the Unified/ICP or in the field.

*Entry level.* FEMA IS-700: NIMS, An Introduction
ICS-100: Introduction to ICS
*First line, single resource, field supervisors.* IS-700, ICS-100 and ICS-200: Basic ICS or its equivalent
*Mid-level management: strike team leaders, division supervisors, EOC staff, and so on.* IS-700, IS-800.A NRP, ICS-100, ICS-200 and ICS-300*
*Command and general staff; area, emergency and EOC managers.* IS-700, IS-800.A, ICS-100, ICS-200, ICS-300* and ICS-400*

The courses above (with the exception of ICS-300 and ICS-400) are available for on-line training at http://training.fema.gov/IS/crslist.asp.

## 6 PROMOTING RESOURCE AND INFORMATION EXCHANGE AMONG STAKEHOLDERS

### 6.1 WARN

The Water and Wastewater Alert Response Network (WARN) is a voluntary agreement for utility mutual aid assistance in the event of an emergency within a network. All states have established a network or steering committee for a network to provide and receive emergency aid and assistance. The assistance may arrive in the form of personnel, equipment, materials, and other associated services as necessary from other water/wastewater utilities. Participation in a network is voluntary; there is no obligation to respond, and there is no direct cost to become a member of the network. For more about the WARN networks, see http://www.awwa.org/government/content.cfm?ItemNumber=30229.

### 6.2 Emergency Exercises

Emergency exercise programs include regular training of personnel; testing of systems and equipment to be used during implementation of the plan; and exercises to assess, validate, and identify problems with the plan, procedures, systems, and facilities. Consistent with the HSEEP guidance (https://hseep.dhs.gov/support/HSEEP_101.pdf), the objectives of an exercise program are as follows:

- assess and validate plans, policies, and procedures
- ensure personnel are familiar with emergency procedures
- ensure that personnel are sufficiently trained to carry out essential functions in an emergency situation
- test and validate equipment to ensure both internal and external interoperability
- discover planning weaknesses

- reveal resource gaps
- improve coordination
- practice using the communication network
- clarify roles and responsibilities
- improve individual performance
- improve readiness for an actual emergency.

## 7 HOW TO DEVELOP AN EMERGENCY PLAN

### 7.1 Types of Threats

The emergencies that may affect utility operations or services include natural, technological, and human-caused disasters. Natural disasters include severe thunderstorms, lightning, flooding, tornadoes, and earthquakes. Technological disasters result from accidents or other unintentional acts, and may include fire, power failure, and chemical release. Human-caused disasters are the result of an intentional malevolent act; examples of human-caused disasters are bomb threats, unauthorized entry, and terrorist attacks.

The hazards and emergency events that may be typically applicable to utility facilities and/or services are listed below:

- power failure
- severe weather
- earthquake
- medical emergency
- fire/explosion
- chemical release
- destruction/failure of any part of the water system
- bomb threat/suspected explosive device
- unauthorized entry
- workplace violence
- civil disorder/terrorism
- contamination threat to the water system
- identified contamination in water system
- SCADA (Supervisory Control and Data Acquisition system) attack/electronic
- SCADA attack/physical
- volcanic eruption (ash fall).

### 7.2 Plan Approval

Representatives of the water/wastewater system who are ultimately responsible, such as the system manager, owner, board members, commissioners, and council members,

should review, approve, and sign the ERP. This demonstrates support for the plan, acknowledges the effort put into its preparation, and puts it officially into effect.

Be sure to secure and protect the ERP as it may contain sensitive information about facilities and response activities that you may not want others to know in order to safeguard the water/wastewater system.

## 8 CONTENTS OF AN EMERGENCY PLAN

The purpose of an ERP is to provide written procedures for response actions associated with potential water and/or wastewater utility emergencies, including human-caused/intentionally-caused (e.g. terrorist event), natural (e.g. hurricane, tornado), and/or technological (e.g. process safety failure) emergencies and disasters.

The primary objective of an ERP is to provide clear and concise information to utility management to facilitate response actions and mitigate adverse impacts, in the event of emergency incidents involving water and/or wastewater utility personnel, assets, and/or services to the community.

There are many ERP examples for utilities. The following is a sample outline of an ERP that is specific for the planning needs of a water and wastewater utility. Each utility has unique needs and may require a simpler or more expansive ERP than suggested by this article. Any utility ERP should be NIMS compliant.

**Executive Summary**
**Introduction to the ERP**
- **Purpose of the Plan**
- **Goals**
- **Plan Organization**
- **Situation, Limitations and Planning Assumptions**
- **Plan Ownership and Requirements**
- **Authorities and References**
- Definition of Type of Emergency by Level
- **Overview of Facilities**
- Water Facilities
- Wastewater Facilities
- Solid Waste Facilities
- Natural Gas Facilities
- **Event Specific Response**
- Utility Critical Assets
- **Emergency Systems and Equipment**
- Backup Power
- Emergency Equipment Inventory

**Concept of Operations**
- **Phases of Emergency Management**

- Assessment
- Mitigation
- Preparation
- Response
  - Initial Response Operations
  - Sustained Response Operations
  - Recovery
- **Emergency Response Team and Emergency Operations**
- **Emergency Direction and Control**
- Incident Command
- Unified Command
- Initial Operations
- Sustained Operations
- **Incident Command and the Incident Management Team**
- Utility Incident Command Organization
- Incident Management Team
- **Technical Command Center Operations–General**
- **Mutual Aid Agreements**
- **Employee Care and Support**
- **Balancing Crime Scene Investigation and Emergency Response**

**Tactical Communication/Public Information Policy and Procedures**

- **Tactical Communications**
- Communication Resources
- Backup Telephone Service
- Mobile Radios for Incident Management Team
- Emergency Alert System
- **Responsibility and Authority for Communications**
- Chain of Command
- Contact Lists
- Communications with Elected Officials
- **External Communications (Public and Media)**
- Public Information
  - Hotline for External Communications to Public and Employees
  - Call Center for Two-way Communication with the Public and Employees
- Media Relations
  - Public Information Officer (PIO)
  - Spokesperson
  - Media Access Privileges
  - Information to be Reported and Released to the Media/Stakeholders
  - Initial Media Release
  - Follow-up Media Release
  - Tools/Technology Used to Contact Media

Media Contacts
**Items for Media and Public Information Distribution**

**Emergency Facilities and Equipment**
**Purpose**
**Emergency Operations Center Locations**
Location Maps
Suggested Supplies to be Stored at the EOC
**Transportation Resources**
**Procurement of Equipment and Supplies**

**Plan Activation**
**Triggers**
**Emergency Action Levels**
Internal Notification
External Notification

**Termination, Recovery, and Follow-Up**
**Recovery Organization**
**Recovery Operations**
**FEMA Documentation**
**Utility Operations Centers**
Financial
Electronic Records
Communications, Control and Coordination
**Resumption of Normal Operations**
**Evaluation of Response Effectiveness**
Document Lessons Learned
**Restock and Replenish Equipment and Supplies**

**Training, Exercises, and Documentation**
**Overview and Requirements**
**Training Requirements Matrix**
**Employee Awareness and Proficiency Training**
**Training**
**Emergency Exercises**
Discussion-Based Exercises
Operations-Based Exercises
**Documentation**
Formal Training
Exercise Participation

Exercise Control and Evaluation
After-Action Reports and Improvement Planning

**Administration and Logistics**
**Medical Needs of Responders/Support of Response Personnel**
**Site Security**
**Records Preservation and Document Control**
**Emergency Planning Activities**

**Emergency Response Plan Maintenance**
**Program Maintenance Team**
**Plan Review Responsibility**
Responsibility for Changes
**Plan Distribution**

## 9 CONSIDERATIONS FOR EMERGENCY RESPONSE PLAN CONTENT

Tips to consider when developing common sections of an ERP are discussed below.

### 9.1 Mutual Aid Agreements

Mutual aid and assistance agreements establish a Mutual Aid Assistance Program among its signatories and contain procedures and standards for a water and wastewater utility Mutual Aid and Assistance Program.

Before an emergency occurs, mutual aid agreements should be established with nearby water providers, emergency suppliers, and other agencies that can assist during an emergency.

The utility should coordinate with the fire department and Hazardous Materials (HAZMAT) teams to be certain that these groups have the utility dispatch contact information and will call the dispatch if a chemical spill occurs near a raw water source.

### 9.2 Intertie Connections and Agreements with Other Systems

An intertie to the other local water utilities serves to establish a link to most water systems in the state and allows the utility much greater flexibility in purchasing water from other water agencies or exchanging supplies following a disaster.

### 9.3 System Information

Basic information should be gathered on the locations of system components such as the well fields, distribution system, collection system, and so on. It must be ensured that system information is not available to unauthorized persons. This basic information must be kept easily accessible to authorized staff for emergency responders, repair people, and the news media. System information should include names, locations, and population served.

## 9.4 Response Actions for Specific Events

***9.4.1 Job Action Sheets.*** A Job Action Sheet (JAS) is a tool for defining and performing a specific emergency response functional role. The tasks on the JAS can be amended to fit the situation by adding or deleting tasks. The unit leader, branch director, or section chief issuing the JAS should review it for applicability and add in writing any incident-specific instructions or changes.

Developing good JASs, appropriate for specific personnel and emergency response roles, allows planners and responders to understand responsibilities and to identify gaps or duplicity. They also serve as guides for the development of training curricula. While regular planning, training, exercises, and evaluation are necessary to ensure that personnel are competent to perform assigned emergency response roles, JASs ensure that each responder understands and performs assigned duties according to plan. Each person assigned to serve in a response role serves a critical function and must become familiar with their JAS. JASs provide instructional information and serve as a good illustration of the division of labor that occurs in the other sections. While a single person might be competent to carry out all of the associated tasks, in a large emergency no one person can carry out all these tasks simultaneously.

***9.4.2 Situation Checklists.*** Utilities should establish an emergency response checklist to immediately guide employees through the essential actions they must undertake to ensure the protection of the organization's assets and human resources in the event of an emergency.

Utilities should research which emergencies could affect operations or their ability to provide services. Most of these specific hazards can be found in the utility's VA or Hazard Mitigation Plan. Checklists of procedure should be developed for each emergency event and added as an appendix to the ERP. The appendix can also contain checklists for general emergency response actions, such as evacuation and sheltering-in-place, which may be required during multiple types of emergencies. The checklists serve as a guideline only; as not every step on this list is appropriate for every organization or emergency.

## 9.5 Roles and Responsibilities

For disaster response to be successful, it is critical for the utility to have good, communicative relationships within each of their departments and with other city and county agencies. An ERP will support the utility's ability to respond to an emergency rapidly and to better integrate with other involved agencies. Rapid and efficient response to emergencies should minimize the impacts of the event, including reducing the impact to customers, and limiting the cost of recovery for the utility.

An important part of any emergency response is the familiarity of the responders with the ICS and the role of the Incident Commander at the site of the emergency situation. The Incident Commander is responsible for coordinating activities and calling in support from the utility and other agencies in order to properly respond to the situation at hand.

Many types of incidents will be handled by utility personnel. However, for those emergencies that require response by a fire department or police personnel, the Fire Chief or senior police officer on-scene may act in the role of the Incident Commander, as appropriate. This role may change from one person to another if the situation changes or requires the presence of outside agencies. The utility must recognize that its role may change as an emergency situation changes.

### 9.6 Succession Planning

Succession planning provides for an orderly and predefined assumption of senior official's duties in the event that an official is unavailable to execute their legal obligations. Orders of succession should include the conditions under which succession will occur, methods of notification, and any limitations of authority for the successors.

## 10 COMMUNICATIONS

### 10.1 Emergency Notification of Personnel

Upon notification of an incident, the incident is logged internally and information is communicated to the director of security and emergency management, public/media relations, and the emergency operation/control center (when applicable). As appropriate, notification would also be provided to commissioners, the mayor or county administrator, directors, managers, supervisors, and the mayor's office of communications.

### 10.2 Internal Communication

During an emergency managed primarily by the utility, the public information officer (PIO) can be responsible for providing information to on-site staff. Many utilities set up employee hotlines, which can be updated with current information and instructions. In the event of injuries or casualties, an employee's supervisor and human resources department will share responsibility for any notifications that may be required.

During an emergency managed by others, the local emergency response agency generally takes the lead in disseminating information to on-site staff and their emergency contacts. Assistance will be provided by the PIO, supervisors, and other utility staff as needed.

### 10.3 External Communication

Public information is critical as a means to support emergency response operations and to facilitate public safety during a major incident. Effective risk communication programs are particularly important in the initial phase of a crisis to ensure that the general public understands the risk, proper procedures, help center locations, and other crucial information. Communication strategies must focus on both pre- and postincident communications. Preincident communications provide the public with general information regarding evacuation and other preplanned strategies. Postincident communications provide information to facilitate safety among stakeholders and the general public following an incident. A structure to facilitate both pre- and postincident communications is described below in Figure 3.

### 10.4 Communication with the Public

Because public information is critical to incident management, it is imperative to establish Public Information Systems and protocols for communicating timely and accurate information to the public during emergency situations. Effective risk communication programs are particularly important in the initial phase of an incident to ensure that the

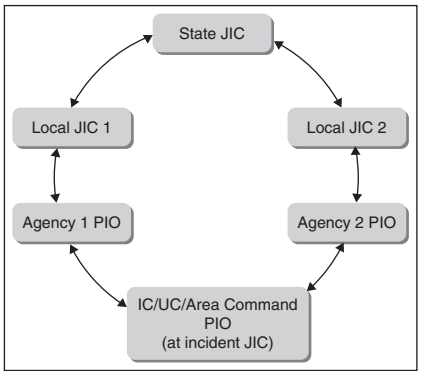



**FIGURE 3** Structure for Communications.

general public understands the risk, proper procedures, where to report for assistance, and other crucial information. Principles to support effective emergency Public Information Systems required by NIMS are addressed below.

***10.4.1 Public Information during Incidents.*** Under ICS, the PIO is a key member of the command staff. The PIO advises Incident Command on all public information matters related to management of the incident, media and public inquiries, emergency public information and warnings, rumor monitoring and control, media monitoring, and other functions required to coordinate and disseminate accurate and timely information related to the incident.

The PIO establishes and operates within the parameters established for the JIS. The JIS provides an organized, integrated, and coordinated mechanism for providing information to the public during an emergency and includes plans, protocols, and structures used to provide information to the public. It encompasses all public information related to the incident. Key elements of a JIS include interagency coordination and integration, developing and delivering coordinated messages, and support for decision-makers. The PIO, using the JIS, ensures that decision-makers and the public are fully informed throughout an incident response.

***10.4.2 Coordination of Public Information.*** During emergencies, the public may receive information from a variety of sources. Part of the PIO's job is to ensure that information received by the public is accurate, coordinated, timely, and easy to understand. One way to ensure coordination of public information is by establishing a JIC. Using the JIC as a central location, information can be coordinated and integrated across jurisdictions and agencies and among all government partners, the private sector, and nongovernmental agencies. The JIC is the physical location where public information staff involved in incident management activities can colocate to perform critical emergency information, crisis communications, and public affairs functions. JICs provide the organizational structure for coordinating and disseminating official information.

## 10.5 Communication with Critical Customers

Critical customers are the at-risk members of the community that resides within a utility's service area. Examples of critical customers include:

- hospitals
- schools
- elderly housing.

The utility's PIO is responsible for notifying priority water customers of changes in water quantity and/or quality that may seriously affect their operations. The resources available to make multiple notifications may be limited during an emergency. Therefore, the 911 Call Center, special call center or other city departments may provide assistance as needed.

## 11 PERSONNEL SAFETY

During any incident, particularly one requiring a lengthy response, it is important to provide for the health, security, and comfort of employees. The following list presents important elements to consider when supporting emergency response personnel.

- replacement clothing, additional protective clothing, replacement footwear and gloves, and other personal protective equipment (PPE);
- shift schedules and rest periods designed to avoid exhaustion;
- meals and safe support areas for removal of personnel from a site; and
- means for personnel to ensure the safety of their families.

Medical surveillance of emergency responders is required for those personnel who may come in contact with hazardous materials. According to 29 CFR 1910.120 (http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=standards&p_id=9765), hazardous material workers and technicians must undergo periodic medical exams. Medical certification for hazardous material work is maintained in personnel records maintained by organizational human resource offices. Additionally, appropriate Health Information Privacy Protection Act (HIPPA) requirements must be followed in collecting, storing, and using this data.

The Safety Officer is responsible for monitoring and assessing hazardous and unsafe situations and developing measures for assuring personal safety. Depending upon the nature and extent of the emergency, the Safety Officer may activate Assistant Safety Officers, additional staff from other disciplines, and/or specialized technical support.

Responsibilities associated with this position may include, but are not limited to:

- obtaining a briefing from the Incident Commander;
- identifying hazardous situations associated with the incident, and ensuring that adequate levels of protective equipment are available and are being properly used;
- identifying potentially unsafe acts, and ensuring implementation of corrective actions. Ensuring safety of on-scene operations, and immediately correcting any unsafe practices;
- reviewing proposed emergency response actions for safety. If an action is or may be unsafe, assist in identifying protective measures or alternative options;
- establishing and maintaining the proper level of security at the EOC and incident scene;

- if applicable, ensuring adequate sanitation and safety in food and beverage preparation;
- tracking accidents and/or injuries to response personnel. Developing and implementing recommendations for preventative and corrective actions;
- investigating any accidents that occur within the incident area. Ensuring that the scene is preserved for investigation and that the incident is properly documented; and
- documenting all significant actions and information in the event log.

### 11.1 Emergency Equipment

***11.1.1 Personnel Protective Equipment.*** *Personal protective equipment* (PPE) refers to protective clothing, hard hats, goggles, or other garments designed to protect utility personnel from job-related occupational safety and health hazards.

***11.1.2 Emergency Communications Equipment.*** Two-way radios, land-line telephones, and cellular telephones are examples of equipment that are most often used to maintain communication among the EOC, field personnel, and external agencies.

Radios should be distributed to management personnel such as the: Utility Director, Incident Commander, Chief Plant Operator, Engineering Manager, or designees for these positions.

## 12 ERP ACTIVATION

A utility must determine when to activate their ERP. Threat warnings and other triggers may be used as notifications for staff to begin their emergency actions.

### 12.1 Threat Warning System

A threat warning is defined as an unusual event, observation, or discovery that indicates the potential for contamination and initiates actions to address the concern. Threat warnings may come from multiple sources, including:

- security breach, which is an unauthorized intrusion into a secured facility that may be discovered through direct observation, an alarm trigger, or signs of intrusion;
- witness account of suspicious activity, such as trespassing, breaking and entering, or other forms of tampering;
- direct notification by perpetrator, either verbally or in writing;
- notification by law enforcement, including local, county, state, or federal agencies;
- notification by news media;
- unusual water quality parameters, when evaluated in the context of the established baseline and the performance characteristics of monitoring and detection equipment;

- unexplained or unusually high incidence of consumer complaints about the aesthetic qualities of drinking water, or minor health problems resulting from exposure to water; and
- notification by public health agencies regarding an increase in the incident of disease or death in a given population.

ERPs should be activated in the event of incidents that pose an unreasonable risk to human health, safety, and/or the environment and/or has the potential for catastrophic impact on utility operations (e.g. terrorist attack, fire and/or explosion, hazardous material spill or release, natural disasters). As such, an ERP provides a standard, yet flexible, framework for incident mitigation, preparedness, response, and recovery. Implementation of ERP procedures must be flexible to accommodate differing circumstances of critical events and changing conditions.

Incidental events (e.g. spills) that can be controlled without threat to human health or the environment by using appropriate engineering controls, work practices, PPE and/or can be contained within the immediate area of the event with NO potential to extend beyond the immediate area, do not require implementation of an ERP.

## 12.2 Triggers

Triggers are events that require activation of an ERP. When activated, utilities switch from normal operations to a operations designed to support activation, response, and recovery relative to a particular hazard or event. The specialized concept of operations supports resource acquisition and deployment to support mitigation and recovery efforts in a safe and effective manner. In addition to national or regional disaster declaration, triggers may include the following:

- notification from the health department that there may be a water quality problem
- medical illnesses or injuries preventing staff from working
- natural disasters (e.g. flooding)
- radiation release
- terrorist or criminal activity.

These ERP triggers require tiered levels of response. A small event may require only a small activation, while a larger incident may require full activation and outside support. Events which trigger activation of the ERP will dictate both the scope of the logistical response and the breadth of affected personnel and facilities. Foreseeable natural disasters such as tornadoes may require complete evacuation of certain facilities, while other events may only impact noninhabited structures.

In addition to utility-specific emergency action levels for response during an emergency event, the Office of Homeland Security has developed the Homeland Security Advisory System for the general public [11].

If the DHS threat level changes, the American Water Works Association (AWWA) will alert water systems via e-mail about the change and recommended emergency

preparations. AWWA's system is known as the *Water Information Sharing and Analysis Center* (WaterISAC) [12].

## 13 PLAN MAINTENANCE

An ERP is a valuable tool to prevent and minimize the impact of emergency incidents. It is critical that an ERP be maintained to reflect current conditions and that agency personnel are well trained and able to respond as planned. The contact list in an ERP should be checked and updated regularly (at least twice a year, and more frequently for some utilities). Updates to the entire plan should be made at least once a year, and should be timed to include lessons learned from emergency exercises.

## REFERENCES

1. Department of Homeland Security (2002). *Homeland Security Presidential Directive 3: Homeland Security Advisory System*, March 11, 2002. Available at http://www.dhs.gov/xabout/laws/gc_1214508631313.shtm.
2. Department of Homeland Security (2003). *Homeland Security Presidential Directive 5: Management of Domestic Incidents*, February 28, 2003. Available at http://www.dhs.gov/xabout/laws/gc_1214592333605.shtm.
3. Department of Homeland Security (2003). *Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection*. December17, 2003. Available at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm.
4. Department of Homeland Security (2003). *Homeland Security Presidential Directive 8*, December 17, 2003. http://www.dhs.gov/xabout/laws/gc_1199894121015.shtm.
5. Department of Homeland Security (2007). *Homeland Security Presidential Directive 21: Public Health and Medical Preparedness*. October 18, 2007. Available at http://www.dhs.gov/xabout/laws/gc_1219263961449.shtm.
6. Bazan, E. B., and Robert T. (2005). *Stafford Disaster Relief and Emergency Assistance Act: Legal Requirements for Federal and State Roles in Declarations of an Emergency or a Major Disaster*, September 16, 2005. Available at http://fpc.state.gov/documents/organization/53688.pdf.
7. Warren, L., Moyer, J., and Cyr, C. (2008). Sidestep Disaster with a Business Continuity Plan, Opflow, 34(7), 16.
8. NIMS Resource Center. Available at http://www.fema.gov/emergency/nims/IncidentCommandSystem.shtm, 2009.
9. *NIMS On-line*. Available at http://www.nimsonline.com/, 2009.
10. *All Course Descriptions are Provided by FEMA*. Available at http://training.fema.gov/IS/crslist.asp, 2009.
11. Homeland Security Advisory System. Available at www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm, 2009.
12. WaterISAC Home Page. Available at http://www.waterisac.org, 2009.

# TREATABILITY OF CONTAMINANTS IN CONVENTIONAL SYSTEMS

KIM R. FOX

*National Homeland Security Research Center, U.S. Environmental Protection Agency, Cincinnati, Ohio*

## 1 INTRODUCTION

Earlier articles in this book have pointed out the need for information on how to protect, detect, and respond to a terrorist attack on a water system. Those attacks may happen in many ways and this article focuses on the response to a contamination attack. The information presented here is to be used to help plan for and to respond to contamination of a water system. Other articles focus on the decontamination of the hard surfaces whereas this article focuses on the treatment of the contaminated water.

The treatment of the contaminated water depends on many factors and these factors include class of contaminant, water quality parameters, volume of water to be treated, location of the water to be treated, and more. Many of the factors above are site specific, and so are not addressed in this article. This article presents general treatment techniques that could be used based on various classes of contaminants. These treatment techniques are not solely for treatment of intentionally contaminated water, but are the same ones that would be used to remove contaminants from any water that contain these contaminants.

The US Environmental Protection Agency (EPA) has proposed a system to help communities detect an intentional contamination of distribution system as early as possible. That system is called the *water security initiative*. The architecture of this system describes the classes of contaminants that the EPA is concerned about [1]. The list of contaminant classes is shown in Table 1.

## 2 WATER TREATMENT

The various types of water treatment technologies available (or applicable) depend on the type of contaminant and the extent of the contamination. For example, if a storage tank was contaminated with a microbial contaminant that could be inactivated by disinfectant, then proper levels of the disinfectant could be added to the storage tank for the proper length of time and no additional treatment would be necessary. In the case where an inorganic chemical contaminant was introduced into an aquifer, a granular activated carbon (GAC) water treatment plant might need to be constructed in order to treat the water for very long periods of time. The various typical water treatment

**TABLE 1 Classes of Contaminants**

| Contaminant Class | Description |
|---|---|
| 1 | Petroleum products |
| 2 | Pesticides (chlorine reactive) |
| 3 | Inorganic compounds |
| 4 | Metals |
| 5 | Pesticides (chlorine resistant) |
| 6 | Chemical warfare agents |
| 7 | Radionuclides |
| 8 | Bacterial toxins |
| 9 | Plant toxins |
| 10 | Pathogens causing disease with unique symptoms |
| 11 | Pathogens causing diseases with common symptoms |
| 12 | Persistent chlorinated organic compounds |

practices are described below along with a summary of their capabilities and where they could be used. A full description of the following techniques can be found in the literature [2].

Conventional coagulation/settling/filtration water treatment uses chemical pretreatment to cause particulate material in a water system to form floc that would then be settled out in a sedimentation basin and/or be removed by filters. The typical pretreatment chemicals include aluminum or iron coagulants and lime or polymers, and the type and amount of chemical depends on the quality of water. This type of treatment is very good at removing particulate matter (including microorganisms), small amounts of various chemical contaminants, and to some extent various radionuclide contaminants. Although this process is very good at removing many contaminants, the process would be difficult to install during an emergency situation. There are some mobile water treatment units that utilize this technology, but these mobile units could not treat large quantities of water. This technology would be (and is) very useful in treating the drinking water for communities that use surface waters as their source water. As an added advantage, this process provides a measure of protection in case their source water becomes contaminated.

One modification to the conventional process is known as *direct filtration*. In direct filtration, the sedimentation step is eliminated. Source waters that contain low levels of particulate material may be suitable for direct filtration. The types of contaminants removed by direct filtration and the limitations of direct filtration are similar to conventional treatment.

GAC is an adsorption and absorption media that can be used to remove many organic contaminants from water. GAC is also effective in removal of low amounts of inorganic contaminants and radionuclides. The GAC is typically placed into a contactor and the water passes over and through the carbon. The contaminants attach themselves to the carbon and are removed from the carbon during reactivation or remain on the carbon for disposal (depending on the contaminant). GAC contactors can be installed

quickly, and the carbon can be replaced when the carbon is spent rather than trying to reactivate the carbon. GAC systems are also readily available for smaller applications, such as apartment buildings, homes, or even small enough for single faucets. Thus, during an emergency situation, GAC units could be utilized to treat only the water that was to be used for consumption or to treat all of the water that was being distributed.

One modification to GAC is known as *powdered activated carbon (PAC)*, where instead of the water flowing through a carbon contactor, the PAC is added to the water and then removed by other processes. The types of contaminants removed by PAC are similar to those listed under GAC. PAC is typically used in situations where seasonal (or occasional) contamination occurs and the activated carbon is only needed for relatively short times.

Aeration is a process where high volumes of air are passed through the water in an effort to transfer the contaminant from the water to the air and thus remove the contaminant from the water. There are several types of aeration systems utilized in drinking water treatment and they range from pipes that bubble air into a pool of water, to pressurized, diffused bubble systems, to tower aeration processes. In all cases, the treatment process is to pass air through the water to strip out the contaminant. Aeration techniques are typically used to remove volatile organic contaminants, but there are a few radionuclides that can be stripped from water by this process. Aeration systems can be installed in relatively short periods of time and they are adaptable to various sizes of systems. For example, aeration systems have been placed into open-air reservoirs, down the single wells or to centrally treat water in a community. One drawback to aeration systems is that the water will have to be repumped after aeration to pressurize the system.

Several treatment technologies, described under the category of membrane treatment, include reverse osmosis, nanofiltration, and microfiltration. In all three cases, the idea is to pass water through a membrane by applying pressure while leaving the contaminants on the other side of the membrane and removing from the system in a concentrated waste stream. In drinking water treatment, these three technologies are differentiated by the size of the contaminant that will go through the membrane. Reverse osmosis system is capable of removing chemicals (inorganic or organic), microorganisms, and radionuclides. Nanofiltration would typically be capable of removing inorganic chemicals, some large organic compounds, and microorganisms. Microfiltration is used only to remove the microorganisms.

All of the membrane technologies are such that they can be installed easily and range in size from single faucet application (home reverse osmosis units) to large-scale applications for treating water for large communities. There are mobile water treatment systems utilized by the military and some of these use membrane technologies to remove as many contaminants as possible.

Ion exchange technology is one where water passes over a bed of ion exchange media (typically resin beads). The resin beads have sacrificial chemical groups attached to them, such as sulfate, sodium, potassium, hydrogen, and others. The chemicals in the water exchange themselves for the chemical group on the resin. Currently, ion exchange systems are utilized for inorganic chemical, radionuclides, and some organic chemicals. Ion exchange system can be installed easily and readily available in cartridge systems

for small applications, whole house systems (home water softener), commercial size for industrial uses, and full-scale water treatment systems.

Activated alumina treatment is not a common practice in drinking water treatment, but is being used to remove specific inorganic chemicals from some water supplies. The removal process is by both adsorption and ion exchange within the activated alumina. Activated alumina has not been used to remove organics or microorganisms from drinking water.

One of the most common forms of water treatment that would be used during and intentional attack of a water system is the use of a disinfectant. Currently, the most common drinking water disinfectants used are chlorine, chloramines, and ozone. Ultraviolet light is also used to disinfect drinking water. Typically, the drinking water disinfection processes are utilized to inactivate microorganisms, oxidize inorganic chemicals, or destroy some organic compounds. The amount and type of disinfectant required depends on the water quality, type and number of organisms, and chemical to be oxidized. Disinfectant technologies are probably the easiest technology to implement in an emergency situation. Quantities of disinfectant could be added manually to a storage tank if necessary, the water utility could increase the disinfectant addition at the treatment plant, or disinfection equipment could be added in desired locations.

Heat inactivation is the final process to be discussed. During drinking water emergencies, boil water orders are often implemented. Notices are given for individuals to

**TABLE 2 Treatment Techniques for Individual Contaminant Class**

| Contaminant Class | Treatment Techniques |
|---|---|
| 1 | Aeration, membrane, carbon [3] |
| 2 | Granular activated carbon, powdered activated carbon, reverse osmosis, aeration, and disinfection [4] |
| 3 | Ion exchange, membrane, granular activated carbon, disinfection, and coagulation/filtration [2] |
| 4 | Ion exchange, lime softening, coagulation/filtration, reverse osmosis, activated alumina, and granular activated carbon [4] |
| 5 | Granular activated carbon, powdered activated carbon, reverse osmosis, and aeration [4] |
| 6 | Disinfection, carbon, coagulation/filtration, reverse osmosis, and decay [5, 6] |
| 7 | Ion exchange, lime softening, reverse osmosis, and enhanced coagulation/filtration [7] |
| 8 | Disinfection, coagulation/filtration, membranes, and activated carbon [8, 9] |
| 9 | Disinfection, coagulation/filtration, membranes, and activated carbon [8, 9] |
| 10 | Membrane, disinfection, coagulation/filtration, lime softening, and boiling [2, 10] |
| 11 | Membrane, disinfection, coagulation/filtration, lime softening, and boiling [2, 10] |
| 12 | Ion exchange, membrane, granular activated carbon, and coagulation/filtration [2] |

boil their water prior to consumption. This process is suggested only for microbial problems and recommended only when boiling is thought to be the desired treatment (Table 2).

## 3 FUTURE RESEARCH

At present, the US EPA's National Homeland Security Research Center (NHSRC) is evaluating specific water treatment and decontamination technologies for various drinking water contaminants. The list of contaminants includes those not normally found in drinking water system and those that could be used in an intentional attack. The information gathered in these projects will be made available to water utilities and those that assist water utilities during an emergency. The data that are considered nonsensitive will be published in peer journals or on EPA's website. For data that are considered sensitive, secure publications and access will be available.

Future research will also be necessary on newly created chemicals and mutated or genetically altered microorganisms. Much of that work will be long-term research projects as the specific contaminant is identified.

## REFERENCES

1. USEPA (2005). *WaterSentinel System Architecture Draft, Version 1.0*. U.S. Environmental Protection Agency, Washington, DC.
2. AWWA, Ed (1999). *Water Quality and Treatment*. McGraw Hill, Denver, CO.
3. Noonan, D. C., and Curtis, J. T. (1990). *Groundwater Remediation and Petroleum: A Guide for Underground Storage Tanks*. CRC Press, Boca Raton, FL.
4. USEPA (2003). Water treatment technology feasibility support document for chemical contaminants. *Support of EPA Six-Year Review of National Primary Drinking Water Regulations*. U.S. Environmental Protection Agency, Washington, DC.
5. Marrs, T. C., Maynard, R. L. and Sidell, F. R., Eds. (2007). *Chemical Warfare Agents: Toxicology and Treatment*. Wiley, West Sussex.
6. Teter, D. M., and Brady, P. V. (2003). *Biological and Chemical Sabotage of Public Water Systems: A Threat Analysis (FOUO).* Sandia National Laboratories, Albuquerque, NM.
7. USEPA (2002). *Implementation Guidance for Radionuclides*. U.S. Environmental Protection Agency, Washington, DC.
8. Keijola, A. M., and Himberg, K., Esala, A. L., Sivonen, K., and Hiss-Virta, L. (2006). Removal of cyanobacterial toxins in water treatment processes: laboratory and pilot-scale experiments. *Environ. Toxicol. Water Qual.* **3**(5), 643–656.
9. Notermans, S., and Havelaar, A. H. (1980). Removal and inactivation of botulinum toxins during production of drinking water from surface water. *Antonie van Leeuwenhoek* **46**(5), 511–514.
10. Fox, K. R. (1992). Removal of cryptosporidium in laboratory and pilot plant studies. *Advances in Filtration and Separation*. Gulf Publishing Company, Atlanta, GA.

# DECONTAMINATION METHODS FOR DRINKING WATER TREATMENT AND DISTRIBUTION SYSTEMS

JOHN MCFEE
*Grand Lake Consulting LLC, Inc., Grand Lake, Colorado*
RADHA KRISHNAN
*Shaw Environmental & Infrastructure, Inc., Cincinnati, Ohio*
HAISHAN PIAO
*Greater Cincinnati Water Works, Cincinnati, Ohio*
PAUL RANDALL
*U.S. Environmental Protection Agency, Cincinnati, Ohio*

## 1 INTRODUCTION

Returning a water system to complete operation after a contamination event requires *ex situ* treatment of the contaminated water and *in situ* decontamination of the water system equipment and distribution system piping. The technologies and actions implemented will be a function of a large number of variables. Current research is discussed in the next section. Subsequently, applicable treatment/decontamination technologies are presented in a tabular form. That table includes technologies currently employed by water systems as well as applicable decontamination technologies employed in the nuclear industry.

## 2 SCIENTIFIC OVERVIEW

This article presents an assessment of developing and developed technologies for decontaminating municipal water system equipment, the distribution system itself, and contaminated water after a contamination event. The technology assessment is qualified by recognition of the substantial unpredictability of a purposeful contamination and the complexities surrounding returning the system to safe operation. Those complexities and uncertainties are discussed in the following Problem Definition section and reflected in the later Research Direction recommendations.

### 2.1 Problem Definition

The range of potential contaminants found in a purposeful or inadvertent contamination of a water system includes biological, chemical and radiological agents. This range is only one of the uncertainties to be addressed in dealing with and responding to such an event. Some of the needed information includes:

- *Nature of the contaminants.* The classification of the chemical/biological contaminants (inorganic chemicals, organic chemicals, microorganisms) is one of the parameters that dictate the decontamination approach to be employed for decontamination. For instance, disinfection agents are powerful decontamination approaches for microbial contaminants and some organic contaminants. However, they have little or no effect on removal of inorganic contaminants. The potential for agents to adsorb/absorb (generically described as adherence in this article) on distribution system materials, scale, or sediment vastly complicates decontamination. Radiological contaminants, generally a subset of inorganic contaminants, present unique decontamination issues. Radiological contaminants also present a unique biological and public response problem. Radiological hazards are likely to be present in very small mass quantities. These small mass quantities will be difficult to decontaminate and completely remove from the system.
- *Extent of the contamination.* Isolation of the contamination to a pressure zone or distribution system area is highly desirable, as it limits the subsequent decontamination and treatment effort. If isolation is not possible, then decontamination of a major portion of the system will be a costly and very time-consuming operation.
- *Materials of construction and age of the water distribution system.* Aggressive decontamination approaches can expedite return to normal operations, but these approaches may be limited by the robustness of the system itself. Older highly scaled distribution systems, in which agent adherence is likely, may require more aggressive treatment to remove the contaminants, but these systems are also susceptible to structural failure under aggressive treatment.
- *Cleanup standard.* Whether the system must be decontaminated to meet drinking water standards [1] or less stringent requirements, such as the US Department of Homeland Security's proposed Protective Action Guides [2], would significantly impact the decontamination approach. With some contaminants, compliance with drinking water standards will require implementation of multiple technologies.

Simply stated, the decontamination approach will be dictated by the characteristics of the contaminant and the system to be decontaminated. An additional factor for consideration is the public acceptance of any decontamination approach and the resulting "end state" or cleanup standard. The environmental remediation industry has experienced stakeholder rejection of cleanup approaches that meet all technical requirements.

## 2.2 Research and Development Status

The American Water Works Association Research Foundation (AwwaRF) sponsored a bench-scale study for decontamination of drinking water system infrastructure, during the period 2004–2006 [3]. The objective of this research program was "to provide a basis for developing standard operating procedures (SOPs) that can be adopted for use by water utilities for remediation of contaminated water infrastructure in the event of a major contamination incident" [3]. The study investigated various decontamination methods for their effectiveness in removal of particular types of contaminants from drinking water distribution system pipe surfaces.

The contaminants examined in the study included the following:

- *Inorganic chemicals.* Cyanide, arsenic, mercury, and surrogates of radioactive isotopes (cesium, strontium, cobalt, and thallium).
- *Organic chemicals.* Chlordane and para dichlorobenzene (p-DCB).
- *Microbial contaminants. Bacillus thuringiensis* and MS2 bacteriophage.

In these bench-scale experiments, AwwaRF used 12-in. lengths of pipe sections of various materials. The diameter of the pipe sections varied from 0.75 to 3 in. During the water matrix testing and contaminant adherence tests, the pipe sections were filled with the contaminant mixtures and the pipe surfaces were exposed to contaminants for a period of 7 days.

***2.2.1 Phase 1a: Water Matrix Test.*** The objective of the water matrix test was to determine whether the water matrix had a substantial impact on the adherence of contaminants to the pipe surface. The following water matrix parameters were examined: temperature, pH, alkalinity, and total organic carbon (TOC). Only two types of pipes were tested in the water matrix test: chlorinated polyvinyl chloride (cPVC) and iron pipes. There was no significant or consistent impact of water matrix variables (i.e. temperature, pH, alkalinity, and total organic carbon) on the attachment of microbes, inorganic metals, or organic contaminants to cPVC or iron pipe surfaces.

***2.2.2 Phase 1b: Contaminant Adherence Tests.*** Contaminant adherence tests were performed on various pipe materials, including the combinations of biofilm on cPVC and iron pipe, polyethylene, new and heavily tuberculated (used) galvanized pipe surfaces, epoxy-coated steel pipe, and cement-lined ductile iron pipe with and without the asphalt seal coat. Following were the results:

- Greater than 5% of cesium, strontium, cobalt, and thallium were attached to iron, new galvanized, or iron/used galvanized biofilm pipes.
- Chlordane adsorbed to all pipe surfaces, except the cement-lined ductile iron and polyethylene pipes.
- The adsorption of p-DCB was not as strong as chlordane; however, greater than 5% of p-DCB adsorbed to iron-biofilm, new galvanized, used galvanized, cement-lined ductile iron (with asphalt seal coat), and epoxy-coated steel pipe.
- Bacillus spores attached best to iron-biofilm pipe. No substantial adsorption (less than 5%) of cyanide, arsenic, mercury, or MS2 bacteriophage was observed on any of the pipe materials tested.

***2.2.3 Phase 2: Examination of Decontamination Procedures.*** AwwaRF's bench-scale decontamination test was focused on the contaminants that showed adsorption capacity of greater than 5% on various pipe materials. For the examination of decontamination procedures, decontamination agents were applied to the contaminated pipe sections for 24 h. The pipe surfaces were then rinsed with one-water wash and a final "getter-wash". The effectiveness of the decontamination procedures was calculated by determining the amount of contaminant in the final "getter-wash" compared to the final "getter-wash" from nondecontaminated pipes. The decontamination agents tested included common

surfactants, chelating agents, pure industrial surfactants, commercial surfactant combinations, and chlorine/hypochlorite.

***2.2.4 Decontamination of Bacillus Spores.*** Decontamination tests with Bacillus spores were conducted using chlorine as the decontamination agent at different levels of concentration–time (CT) values (ranging from 300 to 30,000 mg/l/min) to remove Bacillus spores from heavily tuberculated galvanized pipe and iron-biofilm pipe surfaces. Inactivation of Bacillus spores attached to tuberculated galvanized pipe was not pronounced for various chlorine contact times tested. The highest removal efficiency obtained was 84% with a CT application of 30,000 mg/l/min. Results from the Bacillus spores on iron-biofilm pipe were not conclusive due to the very low level of attached spores. The significantly high CT value with lower removal of Bacillus species in the AwwaRF study demonstrates the challenge associated with decontamination of microbial contaminants from the pipe surfaces as compared to removal from bulk water [4].

***2.2.5 Decontamination of Inorganic Contaminants.*** Decontamination techniques tested for inorganic contaminants, cesium, and strontium (radionuclide surrogates) included chlorination, treatment using Simple Green, a commercial decontamination agent (1 and 10%), NaEDTA disodium ethylenediaminetetraacetic acid (1%), and sodium citrate (1%) on two types of pipe surfaces: heavily tuberculated (bulb-like scale adhering to pipe walls) galvanized pipe and cement-lined ductile iron pipe (without asphalt seal coat). Decontamination tests of cobalt and thallium, also radionuclide surrogates, on new iron or galvanized pipes were conducted with chlorination and treatment using Simple Green (1 and 10%). The decontamination results were as follows:

- Chlorination resulted in the removal of cesium on used galvanized and cement-lined ductile iron pipes at 23% and 26%, respectively.
- Strontium was minimally removed by chlorination on cement-lined ductile iron pipe.
- The 10% Simple Green resulted in removal of cesium and strontium with efficiencies ranging between 18 and 56%.
- None of the decontamination agents successfully removed cobalt and thallium from new iron pipes or galvanized pipes.

***2.2.6 Decontamination of Organic Contaminants.*** Three commercial surfactants, Surfonic N-60, Surfonic TDA-6, and Empicol LZV, were evaluated as decontamination reagents at three concentration levels (0.05, 0.5, and 5%) for organic contaminants (chlordane and p-DCB) on cPVC, used galvanized, and epoxy-coated steel pipe surfaces. The results, tabulated in Table 1, were highly variable depending on the contaminant and pipe material.

In 2004, Battelle Science and Technologies initiated a bench-scale drinking water pipe decontamination study under the funding of EPA's National Homeland Security Research Center [5]. The objective of this study was to understand adherence/attachment of various contaminants on pipes commonly used for drinking water distribution.

This study examined several kinds of chemical contaminants, including three kinds of organophosphates (mevinphos, dichlorvos, and dicrotophos), diacetylmorphine (heroin), gasoline, mercuric chloride, strychnine, sodium fluoroacetate, and sodium cyanide. The

**TABLE 1 AwwaRF's Decontamination Study Results**

| Pipe Type | Contaminant[a] | Surfactant | | |
|---|---|---|---|---|
| | | Surfonic N-60 | Surfonic TDA-6 | Empicol LZV |
| cPVC | Chlordane | Good removal | Good removal | Average removal |
| | p-DCB | Poor removal | Poor removal | Poor removal |
| Used galvanized | Chlordane | Good Removal | Good Removal | Average removal |
| | p-DCB | Average removal | Average removal | Poor removal |
| Epoxy-coated steel | Chlordane | Average removal | Average removal | Average removal |
| | p-DCB | Poor removal | Poor removal | Poor removal |

[a]The qualitative performance ratings are defined in terms of percent as follows:

| | |
|---|---|
| <20% | poor removal |
| 20–50% | average removal |
| 50–80% | good removal |
| >80% | excellent removal |

bacterial contaminants examined included *Bacillus anthracis* Sterne (anthrax), *Burkholderia thailandensis* ATCC 700388 (glanders), *Vibrio cholerae* ATCC 25870 (cholera), and *Salmonella choleraesuis* typhi ATCC 6539 (typhoid). Two neurotoxins (Brevetoxin PbTx-3 and botulinum type A) and one mycotoxin (aflatoxin B1 [sigma]) were also studied.

In this study, the pipe housings were filled with contaminated water to maximize the surface area contacted, with very little oxygen present. Test pipe segments were sealed by covering the liquid with a Teflon sheet at both ends. The pipe materials evaluated included the following:

- Polyvinyl chloride (PVC) Schedule 40
- Aged black iron
- Copper
- High density polyethylene (HDPE)
- Cement-lined ductile iron with or without seal coat
- Steel pipe with high solids epoxy.

Contaminants were sealed in the test pipe materials for 1-day and 7-day hold tests at room temperature as well as at 2–8 °C for 7-day hold tests. Battelle subsequently evaluated decontaminant effectiveness, but those results are not available.

Primary results of the adherence results are qualitatively described in Table 2. Note that not all contaminants were evaluated in all pipe types. Related observations include the following:

- Most of the chemical contaminants adsorbed on cement-lined ductile iron pipes.
- Copper and mercury formed an amalgam on the pipe surface, and this type of mercury slowly leached back into the distribution systems.
- There was no difference between contaminant adherence to various types of iron pipes, whether they were cement-lined or not.

**TABLE 2 Battelle Adherence Study Results**

| Contaminant | Pipe Type | | | | | |
|---|---|---|---|---|---|---|
| | PVC | Aged Black Iron | Copper | HDPE | Cement-lined Ductile Iron | Epoxy- Lined Steel |
| Mevinphos | Adsorbed | | Adsorbed | | | |
| Dichlorvos | | | Adsorbed | | | |
| Gasoline | Adsorbed | | | | | |
| Mercury chloride | | | Adsorbed | | | |
| Strychnine | Adsorbed | | | | | |
| Sodium fluoroacetate | | | | | Significant Adherence | |
| Anthrax | High adherence | Moderate adherence | High adherence | High adherence | Moderate adherence | High adherence |
| Glanders | High adherence | | | High adherence | | Moderate adherence |
| Typhoid | Moderate adherence | Moderate adherence | Bactericidal action | Low adherence | Bactericidal action | Moderate adherence |
| Aflatoxin B1 | Adheres | | Less adherence | Adheres | | |

- Fluoroacetate showed significant adherence to ductile iron pipe surfaces, though it was found to be very soluble in water.
- Strychnine and diacetylmorphine dissociated into morphine within a few minutes.
- Botulinum toxin was found to be unstable in water.

A pilot-scale experimental test program was conducted during the period 2005–2007 by Shaw Environmental, Inc. under the sponsorship of EPA's National Homeland Security Research Center [6]. The primary objectives of this decontamination research were to quantitatively determine the potential of target contaminants for persistence in dynamic drinking water distribution systems and to perform quantitative determination of the efficacy of various decontamination methods for removing contaminants from drinking water distribution systems. This effort differs from the AwwaRF and Battelle studies in that this project examined a pilot-scale dynamic system rather than a bench-scale static unit.

A pilot-scale drinking water distribution system simulator (DSS) was constructed from a 6-in. diameter clear PVC pipe. To quantify the extent of adherence of the contaminants to the surface of real-world pipe materials, 10 small rings (coupons) from real-world pipe sections were integrated into the PVC DSS. The real-world pipe coupons used for the study were made of used cement-lined ductile iron pipe sections taken from a pipe that had been in service for 5 years. A set of PVC coupons was included to serve as "control" coupons. Each coupon measures 1 in. in width. At the end of each run, the coupons were removed from the system and analyzed for specific contaminants. An accelerated biofilm cultivation protocol was developed and applied in the DSS for 2–3 weeks prior to the injection of contaminants. A heterotrophic plate count (HPC) of $10^4$ colony forming units (CFU)per square centimeter or higher was considered to adequately represent a viable biofilm population in the pipe-loop system.

A complete decontamination test included evaluation of the contaminant adherence to the pipe surface followed by an evaluation of a specific decontamination procedure. During the adherence test, contaminants were injected into the pilot-scale pipe-loop system. For these contaminants, appropriate decontamination technologies were selected and their effectiveness was determined. Table 3 presents a list of primary experimental design parameters for conducting the pilot-scale adherence/decontamination studies.

Results from experiments studying the effects of flow rates on the adherence of contaminants to the pipe surfaces are tabulated in Table 4. In summary, all tested contaminants have a strong tendency to adhere to cement-lined ductile iron pipe surfaces, and the adherence capacity of target contaminants to the clear PVC pipe surfaces varied significantly.

Table 5 presents a summary of the performance of various decontamination techniques for the target contaminants tested in this study. The variability in the decontamination effectiveness was assessed by the different coupons employed within the pipe-loop system. Therefore, only qualitative ratings of the various decontamination methods are indicated in Table 5.

## 3 CURRENT DECONTAMINATION AND TREATMENT PRACTICES

The previous subsection presented research results from ongoing adherence and decontamination studies. This section describes available decontamination technologies and

**TABLE 3 Experimental Design Parameters for EPA/Shaw Pilot-Scale Decontamination Study**

| Parameters | Selected Materials/Conditions |
|---|---|
| Target contaminants | Sodium arsenite, mercuric chloride, *Bacillus subtilis*, diesel fuel (No. 2), chlordane |
| Pipe material evaluated | Cement-lined ductile iron (from 5-year-old T&E facility pipe-loop system), clear PVC |
| Biofilm | Biofilm cultivated on pipe wall (target HPC: $10^4$ CFU/cm$^2$) |
| Distribution system simulator operating parameters | Flow mode: recirculation |
| | Flow rates: 1, 15, 60 ga/min |
| | Temperature: ambient high bay temperature |
| | pH: pH of Cincinnati tap water ~8.5 |
| | Free chlorine at start of study: ~1.0 mg/l |
| Contact time for contaminant adherence study | 2 d after injection of contaminant into pipe-loop system |
| Concentration of target contaminant | 10 mg/l of mercury, arsenic, and diesel fuel (No. 2), chlordane (as alpha+gamma chlordane, 40 mg/l as technical chlordane) |
| | $10^4$ cells/ml of *B. subtilis* |
| Decontamination approaches evaluated | **Arsenic**: Baseline water flushing |
| | Low pH (i.e. pH 4) flushing |
| | Phosphate buffer flushing |
| | Acidified potassium permanganate flushing |
| | NSF Standard 60 Products flushing: |
| | *NW-310/NW-400 flushing* |
| | *Floran Biogrowth Remover/Catalyst flushing* |
| | *Floran Top Ultra/Catalyst flushing* |
| | **Mercury:** Baseline water flushing |
| | Low pH (i.e. pH 4) flushing |
| | Acidified potassium permanganate flushing |
| | ***B. subtilis***: Baseline water flushing |
| | Shock chlorination |
| | **Diesel fuel:** Baseline water flushing |
| | Surfonic TDA-6 flushing |
| | **Chlordane**: Surfonic TDA-6 flushing |

provides a brief description of these technologies. Note that many of these technologies are considered "available", but have not necessarily been deployed in real municipal water systems. They are included here for consideration in responding to an unpredictable contamination event.

### 3.1 Available Decontamination Technologies

Table 6 is a compilation of decontamination technologies applicable to removal of microbial, organic, and inorganic (including radiological) contaminants. Table 6 also includes a qualitative assessment of the applicability, the effectiveness, and limitations of the decontamination technologies. Table 6 is divided into three sections. The first section lists

**TABLE 4 Shaw Adherence Study Results**

| Contaminant | Pipe Type | |
|---|---|---|
| | Cement-lined Ductile Iron | Clear PVC |
| Arsenic | Strongly adheres | Adheres |
| Mercury | Very strongly adheres | Adheres |
| Bacillus subtilis | Strongly adheres | Strongly adheres |
| Diesel, No. 2 | Strongly adheres | Adheres |
| Chlordane | Strongly adheres | Adheres |

**TABLE 5 Performance of Decontamination Techniques for Various Target Contaminants from EPA/Shaw Pilot-Scale Decontamination Study**

| Contaminants | Decontamination Method | Qualitative Performance Rating[a] |
|---|---|---|
| | Water flushing | Average |
| | Low pH | Average |
| | Phosphate buffer | Poor |
| Arsenic | Acidified potassium permanganate | Good |
| | NW-310/NW-400 | Good |
| | Floran Biogrowth Remover/Catalyst | Good |
| | Floran Top Ultra / Catalyst | Average |
| | Water flushing | Average |
| | Low pH | Average |
| Mercury | Acidified potassium permanganate | Excellent |
| *Bacillus subtilis* | Water flushing | Poor |
| | Shock chlorination | Average |
| Diesel fuel, No. 2 | Water flushing | Average |
| | | Good |
| | Surfonic TDA-6 | Excellent |
| | | Good |
| Chlordane | Surfonic TDA-6 | Excellent |
| | | Excellent |

[a]The qualitative performance ratings are defined in terms of percent/log removal are as follows:

| For chemical contaminants | | For microbiological contaminants |
|---|---|---|
| <20% | Poor | <1 log removal* Poor |
| 20–50% | Average | 1–2 log removal Average |
| 50–80% | Good | 2–3 log removal Good |
| <80% | Excellent | <3 log removal Excellent |

$$^{*}\text{Log removal} = \text{Log}\left[\frac{\text{count of microbes adhered on coupon before decontamination}}{\text{count of microbes remained on coupon after decontamination}}\right]$$

**TABLE 6 Decontamination Technologies Applicable to Contamination of Municipal Water Systems**

| Decontamination Technology | Applicability | Effectiveness | Limitations |
|---|---|---|---|
| | | **Water Treatment System/Equipment Decontamination Technologies** | |
| Grit/Shot Blasting (also dry ice blasting and other potential blast media) [7–9] | Applicable to all contaminants in tanks, very large diameter piping, and accessible equipment | Removes scale and controllable quantities of base material. Therefore, very effective at removing contaminants | Generally a manual access. Some remote systems can be applied. Blast media must be removed as the contaminants will be contained in the media |
| High pressure spray [7] | Applicable to all contaminants in tanks, very large diameter piping and accessible equipment | Depending on the pressures used, some as high as 20,000 psi, scale can be removed very effectively. Lower pressure sprays may not remove tightly adhered scale | Generally requires manual access. Some remote systems can be applied. Safety considerations must be addressed |
| Chemical treatment [10] | Applicable to all contaminants in tanks, piping, pumps and accessible equipment. Chemicals are selected to address particular contaminants and materials of construction. | Aggressive chemical systems can be very effective in removing scale and some base metal. Foams may be used to apply chemicals to improve effectiveness | Aggressive chemical systems must be carefully monitored to avoid equipment damage. Captured treatment chemicals may require management as hazardous waste. Chemicals must be effectively neutralized prior to reuse of the equipment; only ingestion-safe chemicals may be used. Safe handling of the chemicals must be addressed |
| | | **Distribution System Decontamination Technologies** | |
| Flushing/unidirectional flushing/back flushing [11] | Applicable to microbial, organic and inorganic contamination. Current method of choice by utilities to deal with water distribution system contamination | Flushing can remove loose sediments deposited in the pipe and scouring some biofilm from the surface | Typically not effective in pipes larger than 12 in. in diameter. Limited effectiveness in microbial contamination due to biofilm attachment. Large volumes of flushings must be treated |

(*continued overleaf*)

**TABLE 6** (*Continued*)

| Decontamination Technology | Applicability | Effectiveness | Limitations |
|---|---|---|---|
| Air scouring [11] | Applicable to microbial, organic and inorganic contamination. Current method of choice by utilities for water distribution system contamination | Air scouring can remove sediments in the pipe, soft scales, biofilm, and other adhered materials. Very effective for sediment removal. Fairly effective in removal of biofilm | Typically not effective in pipes larger than 12 in. in diameter. Flushings must be treated |
| Pigging/swabbing [11] | Applicable to microbial, organic, and inorganic contamination. Current method of choice by utilities to deal with water distribution system contamination | Effective at removing sediments, biofilm, and friable scales in larger pipe diameters | More effective in larger pipes. Can be used in smaller 4–6 in. diameter pipes by introducing and recovery through fire hydrants. Flushings must be treated |
| Chlorination/shock chlorination [11] | Applicable to microbial contamination. Chlorination is the most frequently used form of halogen disinfection for drinking water in the United States. Chlorine can be applied for the deactivation of most microorganisms and it is relatively cheap | Chlorination is effective for removal of *Escherichia coli*, spores, and other bacteria from water. The effectiveness depends on the proper dose and contact time of the disinfection agent. Chlorination is not very effective for crypto and Giardia removal<br>Chlorination can remove part of bacteria from pipe surfaces, but the effectiveness is not as promising as that for water. High CT value is required for removal of bacteria from pipe surfaces and tuberculated pipes | Formation of disinfection by-products (DBP); odor and taste [12] |

| | | | |
|---|---|---|---|
| Chloramination [11] | Applicable to microbial contamination. Chloramines are the second most commonly used final disinfectant in drinking water treatment next to free chlorine. Chloramines are applied more and more often in the United States as an alternative for chlorine during secondary disinfection of drinking water | Chloramines are effective for the deactivation of bacteria, spores, and other microorganisms; however, the reaction mechanism is slower than chlorine. Monochloramine is the most effective disinfectant. Little to no trihalo methanes (THM) and other DBPs are formed during chloramine disinfection. Chloramines remain actively within the plumbing much longer, because it takes long for chloramines to be broken down | Less reactive than chlorine<br>The efficacy of chloramine disinfection is pH dependent and increases with decreasing pH values |
| Chlorine dioxide [13] | Applicable to microbial contamination. Chlorine dioxide has been used for years in potable water disinfection (United States since 1944) | Chlorine dioxide is superior to chlorine in the destruction of spores, bacteria, viruses, and other pathogen organisms on an equal residual base (even Cryptosporidium and Giardia), at lower concentrations. The required contact time for $ClO_2$ is lower. It destroys THM precursors, and little to no THM and other DBPs are formed during chlorine dioxide disinfection. Relatively stable and in less likely to react with oxidant demand substances than free chlorine. Chlorine dioxide removes biofilm from water systems and prevents it from forming when dosed at a continuous low level. Chlorination, on the other hand, has been proved to have little effect on biofilms | Disadvantage is the presence of chlorite and chlorate resulting from chlorine dioxide treatment. Chlorine dioxide exists as an undissociated gas dissolved in water in the pH range from 6 to 9. The disinfection efficiency increases within this range with increasing pH. It is more vulnerable to volatilization than free chlorine or monochloramine |



(*continued overleaf*)

**TABLE 6** (*Continued*)

| Decontamination Technology | Applicability | Effectiveness | Limitations |
|---|---|---|---|
| Ozonation [13] | Applicable to microbial contamination. Ozone is widely used for drinking water treatment, because of its excellent disinfection and oxidation qualities. Ozone has been used for disinfection of drinking water in the municipal water industry in Europe for over 100 y | Ozone is a more effective disinfectant than chlorine, chloramines, and even chlorine dioxide. No DBP formation. Ozone, unlike chlorine products, can deactivate resistant microorganisms such Cryptosporidium and Giardia. Ozone is relatively unaffected by pH within the range normally encountered in water treatment. | Ozone results in the formation of biodegradable organic matter. Ozone rapidly decomposes in water; its life span in aqueous solutions is very short (less than one hour). Therefore ozone is less suitable for residual disinfection, but can be used in short distribution systems. |
| UV disinfection [13] | Applicable to microbial contamination. It is one of alternative methods to conventional chlorine disinfection | UV can deactivate resistant microorganisms such as Crypto and Giardia. It can be combined with ozonation to improve the disinfection effectiveness | UV cannot provide residual disinfection. This technology has been deployed in groundwater treatment, but would have to be adapted to large volumes of drinking water |
| Surfactant treatment | Applicable to organic and inorganic contamination. Currently, it's not a common practice used by water utilities in the United States. | Surfactants are effective in removal of organics and inorganics from pipe surfaces. The removal efficiency depends on the types of contaminants and surfactants used. Pilot-scale tests indicate that some commercial products are effective in removal of highly adsorptive organic contaminants, such as diesel fuel and chlordane from various pipe surfaces | After removing target contaminants from distribution systems, the cleaning agents (i.e. surfactants) must be flushed from the distribution systems |

| | | | |
|---|---|---|---|
| Hydrochloric acid and other strong acids (low pH flushing) [11] | Applicable to inorganic contaminants. Although readily applied, the danger to decontamination workers and inadvertent contact by users make it undesirable in anything by restricted areas of the distribution system | Effective in removing scale and deposits following flushing | Does not remove all deposits. Flushings must be captured and treated. Requires neutralization after treatment. Distribution system damage can result from residual acids |
| Phosphoric acid (low pH flushing) [11] | Applicable to inorganic contaminants. Sequesters some inorganics. Easily applied in the distribution system | Somewhat effective to very effective, depending on the contaminant and the distribution system materials. The phosphate radical may be particularly effective for some contaminants | As a weak acid, it would require long-term exposure to dissolve scale. The acceptability of food-grade phosphoric acid will require approval in the distribution system |
| Acetic acid (low pH flushing) | Applicable to inorganic contaminants. Sequesters some inorganics. Easily applied in the distribution system | Somewhat effective to very effective, depending on the contaminant and the distribution system materials. The acetate radical may be particularly effective for some contaminants | As a weak acid, it would require long-term exposure to dissolve scale. The acceptability of food-grade acetic acid will require approval in the distribution system |
| Citric acid/Na Citrate (low pH flushing) | Applicable to organic contaminants. Easily applied in the distribution system | Somewhat effective to very effective, depending on the contaminant and the distribution system materials. The citrate radical may be particularly effective in removing some contaminants | As a weak acid, it would require long-term exposure to dissolve scale |
| Acidified potassium permanganate [14] | Applicable to inorganic and some biological contaminants. This is a low pH flush supplemented with permanganate, which oxidizes the inorganics into a soluble form | Some effectiveness as a disinfectant. Effective in dissolution of some metals (iron and manganese) | Brown precipitate must be removed |
| NaEDTA and other chemical sequesterants [14] | Applicable to inorganic contaminants. Sequesterants selected to address contaminants | Selectively effective for contaminants targeted | Questionable acceptability in public water systems due to toxicity |
| Relining [15] | Applicable for all contaminants as a last resort. Applicability is limited by the age, materials, and configuration of the system | Highly effective if applicable | Slow to implement and generally limited to simple configurations |



(*continued overleaf*)

**TABLE 6** (*Continued*)

| Decontamination Technology | Applicability | Effectiveness | Limitations |
|---|---|---|---|
| System replacement | Applicable for all contaminants as a last resort. Very expensive, but for some highly toxic contaminants, may be applicable | Totally effective | Very slow to implement, particularly if large areas of the distribution system are involved |
| **Water Treatment Technologies (Addressing Cleanup of Water Flushings)** | | | |
| Precipitation/coagulation /filtration [13] | Applicable to microbial, organic, and inorganic contaminants. Precipitation, coagulation, and filtration are common steps of water treatment process used in water treatment plants in the United States | Filtration process is effective in removing some microorganisms, but the removal efficiency depends on the operation of the process<br><br>Crypto causes larger problems than Giardia, because of the size. Crypto is 4–5 μm in size, which makes it difficult to remove by conventional filtration [6]. Giardia is 8–14 $\mu$m in size, which makes it easier to remove by conventional filtration than crypto [30]. Effectiveness of direction filtration ranges from 90 to 99% for virus removal, and from 10–99.99% for Giardia removal. The most effective direct filtration configurations for Giardia removal muse include coagulation | Direct filtration is only applicable for systems with high quality and seasonally consistent influent supplies. The removal efficiency depends on the filtration operation. Temperature is another factor that affects the removal |

| | | | |
|---|---|---|---|
| | | | Although coagulation reduces the concentrations of DBP precursors from organic contamination, coagulation shifts the distribution of the DBPs formed by chlorination toward the more brominated species |
| | | Coagulation/filtration can remove some of organics including pesticides, herbicides, and insecticides, volatile organic carbons (VOCs), DBP precursors, and other organics | |
| | | | For inorganic contaminants, the effectiveness is limited by solubility of precipitated species |
| | | Coagulation/filtration (assisted by pH adjustment) can remove many inorganic contaminants | |
| Sand filtration [13] | Applicable to microbial contamination. Low cost, simple operation, and reliable water filtration process. | Sand filtration effectively removes microorganisms, including *Giardia lamblia* that cannot be killed by traditional chlorination. Able to achieve greater than 99.9% Giardia removal | Not suitable for water with high turbidity. Extensive land is required. Filters in cold climates freeze, which reduce cleaning efficiency during cold weather |
| Cartridge filtration [13] | Applicable to microbial contamination. Emerging technology suitable for removing microbes and turbidity in small systems | *Cartridge filtration is effective for removal of some microorganisms* | Cartridge filtration systems require raw water with low turbidity. Polypropylene cartridges become fouled relatively quickly and must be replaced with new units. Although these filter systems are operationally simple, they are not automated and can require relatively large operating budgets |



(*continued overleaf*)

**TABLE 6** (*Continued*)

| Decontamination Technology | Applicability | Effectiveness | Limitations |
|---|---|---|---|
| Adsorption/ion exchange [13, 16] | Applicable to organic and inorganic contaminant removal. Activated carbon treatment is one of the common practices of water treatment in the United States | Activated carbon is an effective process for removing organics including pesticides, herbicides, insecticides, volatile organic carbons (VOCs), DBPs precursors, and other organics | Organics that are poorly adsorbed by activated carbon include: alcohols; low molecular weight ketones, acids, and aldehydes sugars and starches; very high molecular weight or colloidal organics; and low molecular weight aliphatics. Activated carbon is not effective in removing vinyl chloride from water. Bacterial growth on the carbon is another potential problem. Excessive bacterial growth may cause clogging and higher bacterial counts in the treated water |
| | | For inorganic contaminants ion-specific adsorbents can be utilized | Ion exchange can be a polishing step in removing low concentration residuals from treated water |
| Evaporation/ distillation | Typically a polishing step following primary treatment | Highly effective | Energy intensive and requires specialized equipment |
| Membrane filtration [13] | Applicable to organic and inorganic contaminants. Membrane filtration can be an attractive option for small systems because of its small size and automated operation. Membrane processes are increasingly employed for removal of bacteria and other microorganisms, particulate material, and natural organic material, which can impart color, taste, and odor to water | Membrane technologies are effective processes for removing pesticides, herbicides, insecticides, VOCs, DBP precursors, and other organics | Requires specialized equipment and pretreatment to avoid fouling of the membranes. Potentially a large "rejects" stream to be managed with a secondary treatment technology |

| | | | |
|---|---|---|---|
| | | Residual concentrations are a function of membrane effectiveness and quantity of "rejects" (concentrated waste) stream | |
| Oxidation technologies [13] | Applicable to organic and microbial contamination. Advanced oxidation processes have limited applications in the area of drinking water | Advanced oxidation processes can remove both organic and oxidizable inorganic components. The processes can completely oxidize organic materials to carbon dioxide and water. | Advanced oxidation processes often have higher capital and operating costs compared with biological treatment. This method requires the addition of chemicals, such as ozone, hydrogen peroxide, hypochlorite, permanganate, etc. |
| Air stripping [13] | Applicable to high volatility organics contaminants | Effective in removing volatile organics including volatile pesticides and fuels | Low volatility organics such as polychlorinated biphenyls (PCB) are not separated. Stripping columns can be fouled by organism growth |

technologies that can be applied to contaminated large equipment, representing equipment that can be manually entered and physically treated. Tanks and large distribution system piping are some examples. The second section of Table 6 tabulates technologies applicable to the distribution system piping. There are some physical decontamination options such as pigging, but most of the distribution system options are chemical in nature. Note that the applicability of these technologies is constrained by the materials of construction of the distribution system, its age, and complexity. A previously mentioned decontamination issue mentioned previously is scaling and biofilm in the distribution system. Adherence of contaminants on the distribution system may at first minimize the impact of a contamination event by removing the contaminant from the water stream, but will make ultimate cleanup very difficult due to slow leaching (desorption) of adhering species. The last section of Table 6 includes technologies applicable to *ex situ* treatment of the contaminated water flushings. These flushings could result from a straightforward system flush, or they could contain materials scraped outby pigging, or residual chemicals from the chemical treatment. In a large-scale contamination event, capture and storage of these flushings could be difficult.

## 3.2 Technology Descriptions

***3.2.1 Decontamination Methods Appropriate for Tanks and Equipment with Access.*** Decontamination for tanks and equipment accessible to personnel with tools pose an addressable decontamination challenge. Structures can be cleaned by conventional cleaning techniques as listed below and then rinsed before being returned to service:

- *Grit/shot blasting.* Grit/shot blasting uses sand or metal shot propelled against a contaminated surface using compressed air. It is a common industrial process with inexpensive equipment readily available. It is effective in the decontamination of all surfaces [7–9]. Variations of grit/shot blasting include dry ice blasting and soft media (abrasive impregnated sponge) blasting.
- *High pressure spray.* Ultra-high-pressure wash uses a pressure booster to produce a very high pressure stream of water capable of cutting through hard materials [7]. It is used in the nuclear decontamination industry to spall a layer of concrete and is capable of removing corrosion products.
- *Chemical cleaning.* Some decontamination surfactants were cited in the ongoing research discussions. Chemical decontamination methods used by the nuclear industry use very aggressive chemicals that can remove radionuclides tightly bonded to contaminated surfaces [7, 10]. Foam can be used to increase chemical contact time with the contaminated surface.

***3.2.2 Decontamination Methods Appropriate for Distribution System.*** Pipe cleaning systems of municipal water system are capable of decontamination of some agents and in some configurations. The decontamination system must be able to address contamination in sediment, biofilm, friable scale, and hard scale.

- *Flushing/unidirectional flushing.* Conventional flushing is widely used in water systems to respond to water quality issues. It involves simply opening one or more

fire hydrants and allowing water to flow until sediment or other contaminants are removed [11]. Unidirectional flushing is an improvement on conventional flushing in that valves are closed and hydrants opened in a systematic fashion that maximizes water velocities.

- *Air scouring.* Air scouring is currently deployed and uses pulses of water and air to clean pipelines [11]. It may be combined with decontamination agents to enhance decontamination. Alternatively, it may reduce contact time of the decontamination agent and limit effectiveness.
- *Pigging/swabbing.* Pigging is also a currently used technology where water pressure is used to push a swab or polyurethane cylinder, or a bullet-shaped or dumb bell-shaped pig through the line [11]. Pigging removes layers of sediments, biofilm, soft scale and hard scale. Abrasive pigging uses a pig with abrasive materials such as Velcro, carbide straps, plastic brushes, or wire brushes embedded in the shell of the pig to more aggressively remove harder scales.
- *Chemical decontamination.* Chemical decontamination removes contaminants from the pipe wall, sediment, biofilm, friable scale, and hard scale by dissolution or desorption. Numerous chemical decontaminants are identified in Table 6. The decontamination agent is injected into an isolated part of the system and recycled through that portion until the objectives are reached. The decontamination is typically followed by neutralization agents and flushing of the system to remove last traces. Common chemical decontamination agents include oxidizers for organics (i.e. hypochlorite, acidified potassium permanganate), strong acids, weak acids, sequestering agents, and surfactants. Commercial cleaning agents are available and frequently include combination of chemical agents [14].
- *Pipeline relining options.* Cleaning or upgrading distribution system piping has been described as *Trenchless Technology* [15]. Trenchless technologies include relining by spray-on concrete linings and insertion of linings. Although this is not a "decontamination" process per se, it is listed here as an option for consideration. This option may be particularly interesting in the case of low levels of nuclear contamination or as a final assurance that contaminant desorption is precluded in the system.

***3.2.3 Decontamination Methods (Treatment Methods) Appropriate for Contaminated Water (Flushings).*** Although it is expected that a portion of the contaminant residual will remain adsorbed or adhered to the distribution system piping and equipment, contaminated water remains a problem to address. In addition, contamination removed from the system through decontamination processes needs to be isolated and treated prior to discharge. There are several water treatment technologies as shown below that could be employed post event to remove contaminants from the flushed water or decontamination flushings.

- *Chlorination/chloramination.* Chlorine gas or hypochlorites are added to water as a gas or liquid [17]. They are strong oxidizers and destroy bacteria and other organisms. Chloramination supplements the chlorine additive with ammonia and extends the stability of the active chlorine oxidizer.

- *Precipitation/coagulation/filtration.* Water treatment facilities commonly use combinations of precipitation, coagulation, and filtration for water purification. Contaminant-specific chemicals chosen to precipitate (floc) the contaminant allow for contaminant removal as settled solids or in a filter. The clarified liquid is commonly filtered in sand filters or mechanical systems to remove residual solids.
- *Adsorption/ion exchange.* Adsorbents are materials whose makeup and internal pore surfaces physically trap or bond with the contaminants. Ion exchange media (water softeners) are a common application of adsorbents. Typical adsorbent materials include granular activated carbon (GAC), zeolite, bentonite clay, activated alumina, silica gel, porous polymer, and ferric media. Zeolite media have been proved to be highly selective scavengers for metal cations. GAC is primarily used for removal of organic substances [18].
- *Evaporation/distillation.* Contaminants are separated from water by vaporization and subsequent condensation of the purified water. Solids and nonvolatiles are left behind and concentrated, separating the solid contaminants from the water vapor. The capital and operating costs to construct an evaporation system is significant.
- *Membrane processes.* Membrane processes apply pressure on one side of a semipermeable membrane that forces a separation of the solute from the solvent. The membrane rejects ions on the basis of their size and charge. Variations of membrane processes "reject" smaller and smaller contaminants. The ranking of these processes from coarsest to finest separation is microfiltration, nanofiltration, ultrafiltration, and reverse osmosis (RO). RO is the tightest possible membrane process in liquid–liquid separation. Essentially, all dissolved and suspended solids are rejected. RO systems can be configured in "cascades" or series systems that minimize reject volumes or raise permeate quality, or both [18].
- *Oxidation technologies.* Oxidation technologies destroy organic contaminants by attacking carbonaceous compounds (chemical or pathogens) and converting them to simple oxidation products. Typical oxidation technologies employ hydrogen peroxide or ozone, sometimes supplemented by ultraviolet (UV) light.
- *Air stripping.* Air stripping separates volatile organics from water by vaporizing the organic in air that is bubbled through the water or via contact in countercurrent stripping columns.

## 4 HOW TO SELECT A DECONTAMINATION/TREATMENT TECHNOLOGY

The issues to be addressed by the decontamination technology were introduced in a prior subsection. The decontamination approach must be selected from a number of technology options, each with their own applicability and effectiveness. The EPA's water system toolbox outlines the steps involved in technology selection and implementation [13]. The steps are as follows:

1. *Determine the cleanup goal.* The cleanup goal must be established to complete engineering of the decontamination and treatment system.
2. *Select evaluation criteria; effectiveness, implementability, and cost.* EPA recommends that the selection criteria follow the same general approach as those used

in selecting cleanup methods for environmental remediation. Effectiveness is a measure of the technology's ability to meet the cleanup/treatment goals including short-term and long-term protection of the public health and environment, compliance with regulations, and residual generation. Implementability includes the requirements of safety of the involved workers as well as cleanup schedule issues. Lastly, cost is included as a criterion in addition to the other criteria.

3. *Do treatability testing, if required.* Treatability testing involves either bench-scale or pilot-scale confirmation that the selected decontamination technology meets cleanup criteria. Even more importantly, secondary waste treatment/disposal approaches should be evaluated to ensure that the decontamination is not impeded by secondary issues.
4. *Cost the cleanup.* Having selected the decontamination approach, the complete decontamination and recovery to normal operation can be estimated with some accuracy for either the selected approach, or multiple approaches, as required.
5. *Downselect.* Completion of the testing procedures and costing efforts will facilitate a final selection of the decontamination approach. It is also noted that abbreviation of this ordered recovery procedure may well be considered in a significant event. However, recognition of these steps is warranted.

## 5 RESEARCH DIRECTIONS

The EPA's Water Security and Research Action Plan identified the needed research in 2004 [19]. Recovery from any contamination event, intentional or unintentional, requires knowledge of the contaminated system and the specific contaminant, but identification of the fate and transport potential of the contaminant in the system is a significant need. Three general research needs can be as listed below:

- Methods to quickly identify a contamination event and the extent of contamination.
- Determination of the fate and transport of contaminants in the distribution system. This modeling must include the effects of adsorption/desorption characteristics of organic chemicals, inorganic chemicals, and microbes on various materials and biofilm in the contaminated system.
- Continued evaluation of existing and emerging decontamination agents for their effectiveness and ability to reach the "cleanup" goal.

## REFERENCES

1. US Environmental Protection Agency (2002). *National Primary Drinking Water Regulations*, Code of Federal Regulations, Title 40, part 141.
2. US Department of Homeland Security (2006). *Preparedness Directorate; Protective Action guides for Radiological dispersal Device (RDD) and Improvised Nuclear Device (IND) Incidents*, Federal Register, Tuesday January 3, 2006.
3. Welter, G., Lechevallier, M., Cotruvo, J., Moser, R., and Spangler, S. (2006). *Guidance for Decontamination of Water System Infrastructure*, Awwa Research Foundation, Denver, CO.

4. Whitney, E. A. S. et al. (2003). Inactivation of Bacillus anthracis spores. *Emerg. infect. Dis.* **9**(6).
5. Chattopadhyay, S., and Fox, K. (2006). Adherence and decontamination chemicals and biologicals, *American Institute of Chemical Engineering (AIChE) 2006 Annual Meeting*, San Francisco, California.
6. Shaw Environmental, Inc (2007). *Pilot-Scale Tests and Systems Evaluation for the Containment, Treatment, and Decontamination of Selected Materials from T&E Building Pipe Loop Equipment*, Shaw Environmental & Infrastructure, Inc, Cincinnati, OH.
7. International Atomic Energy Agency (IAEA) (2001). *Methods for the Minimization of Radioactive Waste from Decontamination and Decommissioning of Nuclear Facilities*, IAEA Technical Reports Series No. 401, Vienna, Austria.
8. US Department of Energy (DOE), Office of Environmental Management. (1998). *Innovative Technology Summary Report*, Advanced Recyclable Media System.
9. US Department of Energy (DOE), Office of Environmental Management (1999). *Innovative Technology Summary Report*, Soft Media Blast Cleaning.
10. United Nations Environment Program (UNEP) (2001). *SIDS Initial Assessment Report*. Citric Acid. CAS No: 77-92-9.
11. Ellison, D., Duranceau, S., Ancel, S., Deagle, G., and McCoy, R. (2002). *Investigation of Pipe Cleaning Methods*, Awwa Research Foundation and American Water Works Association, Denver, CO.
12. Clark, R., and Boutin B. (2001). *Controlling Disinfection by Products and Microbial Contaminants in Drinking Water*, U.S. EPA, Office of Research and Development, USA, EPA/600/R-01/110.
13. US Environmental Protection Agency (2004). *Response Protocol Toolbox; Planning for and Responding to Drinking Water Contamination Threats and Incidents (Module 6; Remediation and Recovery Guide)*, Available at epa.gov/safewater/watersecurity.
14. International Atomic Energy Agency (IAEA) (1999). *State of the Art Technology for Decontamination and Dismantling of Nuclear Facilities*, IAEA Technical Reports Series No. 395, Vienna Austria.
15. Najafi, M., and Gokhale, S. (2005). *Trenchless Technology Pipeline and utility Design, Construction and Renewal*, McGraw Hill.
16. New Hampshire Department of Environmental Services (2002). Environmental Fact Sheet; Organics in Drinking Water WD-WSEB-3-10.
17. American Water Works Association (AWWA) (1999). *Water Quality and Treatment, A Handbook of Community Water Supplies*, McGraw-Hill, Inc, Denver, CO.
18. National Environmental Service Center (2007). http://www.nesc.wvu.edu/ndwc/pdf/OT/TB/TB5_organic.pdf.
19. US Environmental Protection Agency (2004). *Water Security Research and Technical Support Action Plan*, Office of Research and Development, USA, EPA/600/R-04/063.

## FURTHER READING

EPA Water Security website; epa.gov/safewater/watersecurity This website includes documents and references relevant to ongoing research and recommendations for response to contamination events. AWWA website; http://www.awwa.org/ This website provides access to numerous water treatment publications addressing water treatment and decontamination technologies.

# DECONTAMINATION METHODS FOR WASTEWATER AND STORMWATER COLLECTION AND TREATMENT SYSTEMS

BRUCE M. BIWER, S.Y. CHEN, AND FREDERICK A. MONETTE
*Argonne National Laboratory, Argonne, Illinois*

JOHN MACKINNEY*
*U.S. Environmental Protection Agency, Washington, D.C.*

ROBERT JANKE
*U.S. Environmental Protection Agency, Cincinnati, Ohio*

## 1 CONTAMINATION AND DECONTAMINATION OVERVIEW

This article focuses on the decontamination of the internal workings (e.g. pipes, pumps, and tanks) of wastewater and stormwater systems contaminated as a result of a terrorist event involving chemical, biological, or radioactive agents. The decontamination of the external aspects of these systems (e.g. the interior walls and floors of a wastewater treatment plant that may be contaminated from open tanks or ponds) would be similar to that conducted for industrial operations.

### 1.1 System Contamination

Stormwater systems can be contaminated during precipitation events following a chemical, biological, or radioactive release or if contaminated runoff from decontamination activities is not collected. Contaminants can attach to the internal pipe walls of a stormwater system as well as follow any stormwater through leaks into the surrounding soil. If the stormwater system is not part of a combined sewer system, in which stormwater and sanitary wastes are collected and conveyed in the same pipe to a wastewater treatment plant, the contamination would be discharged directly into the environment, such as into streams, unlined detention/retention ponds, or other open waters.

The distribution of contamination is affected by the condition of a water pipeline system prior to an event. Pipe roughness, corrosion, sediment, and biofilms in a pipeline

*John MacKinney currently works for the US Department of Homeland Security

system serve to chemically and/or physically trap material. Similar traps also exist in drinking water systems. Even pipes that are not corroded and have no sediment or biofilm buildup can become contaminated, depending on the chemical and physical nature of the contaminant and the pipe itself. Solid waste and debris also serve as "sinks" (reservoirs) for any contaminant material in a combined sewer or a separate sewer system. In the latter case, infiltration into the system through pipe leaks could lead to contamination in the system. Restoration of such pipelines might require only routine cleaning (with the methods discussed in the following section), with any fixed contamination allowed to remain unless residual concentrations in the water were above acceptable levels.

Depending on the nature of the contaminant, it could become isolated, removed, or attached to the internal walls of a wastewater treatment plant (within piping, pumps, tanks, and equipment) as it moves through the treatment train. The contamination could also become isolated in sediments (sludges) collected in the primary settling tanks and generated during secondary treatment or adsorbed to dirt or biofilm on internal system walls. Advanced (tertiary) treatment methods, if used, might lead to precipitation of dissolved agents (within the sludge) or filter out agents, depending on the agent and the methods used.

Contamination of external surfaces within a treatment plant could occur from contact with material that has had previous contact with contaminated water and possibly from deposition of nonvolatile aerosolized agents. Aerosolization of contaminants may occur where the water surface in tanks is agitated, possibly during treatment processes such as aeration and skimming operations. Volatile agents, if still present in the water, may be released to the air by these types of operations and pose an immediate hazard in confined areas.

## 1.2 Decontamination

Decontamination is the removal of the potential hazard posed by radioactive, chemical, or biological agents, either through actual removal or rendering such agents inactive. In general, decontamination of an affected stormwater or sewer system consists of first removing any contaminated water, debris, and sludge from the system followed by treatment of residual contamination on the interior surfaces of the system. The greatest challenge in such systems is the delivery of an effective treatment to interior pipe walls deep within the system, especially where access is limited. This article focuses on removal of contamination from the system and treatment of residual contamination within the system itself.

For all threats (radioactive, chemical, and biological), physical removal of the hazardous material or agent ensures a reduction in the hazard. Unlike radioactive material, chemical and biological agents can be rendered harmless to humans (neutralized) through chemical and/or physical means. Thus, the discussion of decontamination options is presented separately for radioactive material and chemical and biological agents. Figure 1 presents a decision tree with decontamination options that may be used for cleanup of contaminated systems.

## 1.3 Radioactive Decontamination

Because radioactivity is an inherent property of radioactive isotopes, such contamination cannot be neutralized; decontamination of affected systems requires removal of the radioactive material. For pipelines, standard cleaning technologies can be used to

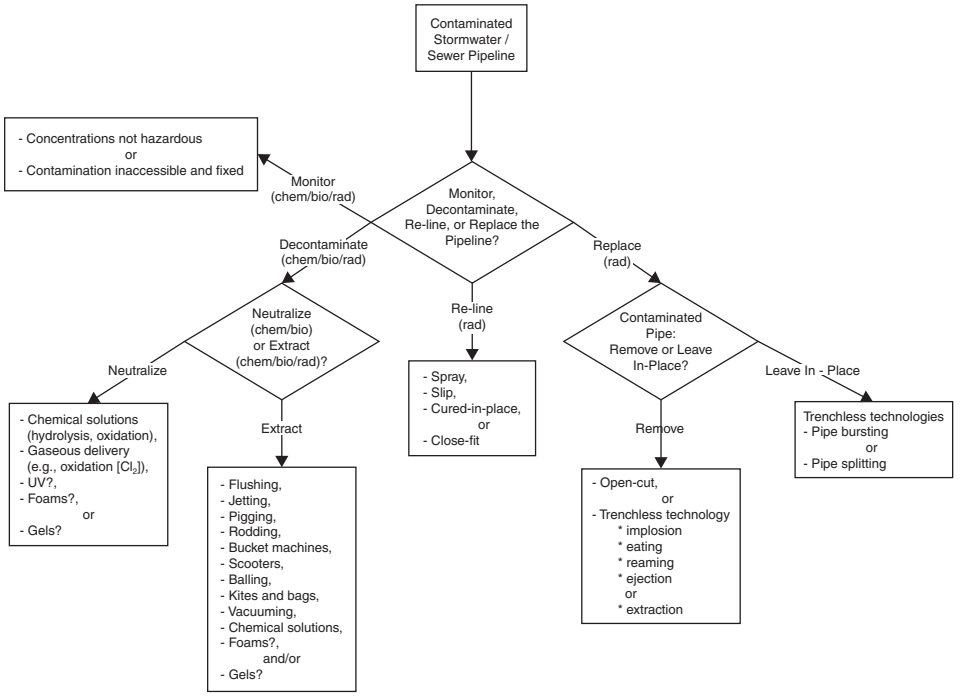



**FIGURE 1** Cleanup technology options for contaminated pipelines.

remove the contamination along with the detritus and debris normally found in sewer and stormwater systems. Such technologies are mostly physical removal processes. Because these technologies were not designed for radioactive decontamination, a pipeline that is cleaned in this way may have residual contamination on or within cracks and crevices in the pipe walls. The effectiveness of standard methods at radioactive decontamination will depend on particular site conditions and need to be tested. Care must be taken to properly protect workers and equipment from any removed material. A proper worker health and safety plan and disposition path for this radioactive waste material must also be in place.

Although sewer and stormwater systems are not pressurized (with the exception of force mains) as are drinking water systems, the operations used for cleaning and maintaining stormwater and sewer pipelines are similar in many respects to those used with water distribution systems. Cleaning operations in stormwater and wastewater systems, however, must also address solid wastes, grease, oils, detergents, roots, debris, rodents, and insects, in addition to a larger sediment buildup problem. Thus, mechanical cleaning methods, such as rodding and the use of bucket machines, are used as well as hydraulic methods, such as scooters or balling, kites and bags, flushing, jetting, and pigging methods [1, 2]. However, the use of hydraulic methods for cleaning sewers should be used only where the potential for backup into connected buildings can be averted.

Chemicals are often used to control a variety of problems such as roots, grease, odors, concrete corrosion, rodents, and insects. The generation of hydrogen sulfide by bacteria found in biofilms under anaerobic conditions in sewer systems creates two major problems: odor and the destruction of sewer pipes and other wastewater system components

[3]. While such applications of chemicals are preventative and not intended to remove material from these systems, chemicals can be used to aid removal (as discussed later in the section on potential technologies).

Radioactive contamination that is tightly bound (fixed) to pipe walls through processes such as chemical reaction or diffusion into the wall would not usually pose an immediate threat to human safety or the environment for smaller diameter pipelines because of its isolation within the system. That is, direct human exposure is unlikely because the pipelines are too small for humans to physically access. It is also possible, although usually not desirable, to fix in-place or isolate radioactive contaminants if contaminant removal is particularly difficult. If it is determined that any later release of this contamination would be insignificant (i.e. contaminant concentrations in effluent wastewater or stormwater would be below acceptable levels), cleanup may not be warranted. In such a case, cleanup might not be justified because of disruption (may be collocated with or in close proximity to utilities or under major thoroughfares and buildings), cost (removal, replacement, and disposal), and the risks of human exposure. Finally, it is reasonable, in cases where the half-life is short, to make use of radioactive decay in a decontamination strategy, but this may not be the case in terrorism incidents.

### 1.4 Chemical and Biological Decontamination

Chemical agents are toxic chemical compounds that may be of common industrial origin, or they may be engineered military chemical weapons. Chemical agents can be neutralized (also referred to as *detoxified*) through destruction of the compound through bond-breaking reactions or they may degrade naturally or volatilize. Biological agents are living bacteria and viruses (naturally occurring or engineered military biological weapons) that can be neutralized through processes such as sterilization and disinfection. Sterilization results in the elimination of all living microorganisms and viruses, while disinfection is a less complete elimination of such entities, especially those in the form of spores.

For chemical agents, of particular concern in stormwater and wastewater systems is those agents that are not readily hydrolyzed (subject to bond-breaking reactions with water) to harmless degradation by-products when in contact with water (e.g. hydrogen cyanide) or those that have hazardous degradation products that do not readily hydrolyze (e.g. Agent VX [4]). An excellent review of chemical agent persistence and degradation in the environment is provided in Munro et al. [5]. A number of biological agents that may persist in water include *Bacillus anthracis* (anthrax) and *Cryptosporidium* [6].

Chemical and biological agents can be removed from contaminated systems with standard cleaning technologies as discussed in the previous section for radioactive contamination. However, disposition of residual wastes from standard cleaning technologies would still require neutralization of the agents once removed. The most efficient process overall would be one that neutralizes the agents while they are within a system.

Most agents can be neutralized in alkaline solutions. For example, VX and the G agents can be hydrolyzed by alkaline hypochlorite solutions [7]. Thus, a standard chemical cleaning method using such a solution could theoretically be used to decontaminate a system. Detoxification of VX can also be achieved through acidic oxidation [8].

Oxidation remains one of the most effective methods of both chemical and biological agent neutralization. Chemical oxidation is already used for a variety of purposes throughout water treatment plants. It is often used to control biological growth such

as algae and other microorganisms that can hinder plant operations; remove inorganic and organic compounds; remove color; decrease odors, primarily from certain organic and sulfur compounds; improve coagulation and filtration processes; and disinfect. Many reactions involving oxidation result in precipitates that settle out of solution or can be filtered out [9].

The principal oxidants used in water treatment plants are chlorine ($Cl_2$), chloramines, chlorine dioxide ($ClO_2$), potassium permanganate ($KMnO_4$), and ozone ($O_3$). A final treatment stage in a number of wastewater treatment plants before discharge to the environment is disinfection with an oxidant such as chlorine. Chloramines are weak oxidants. Their primary role in drinking water treatment is for disinfection of water in distribution systems [10, 11].

## 2 POTENTIAL DECONTAMINATION TECHNOLOGIES

Stormwater and wastewater systems must be physically robust to handle the pressures exerted by running water on various scales and pressures. As discussed previously, cleaning methods range from physical, abrasive methods (e.g. scraping) for scale and root problems to chemical methods for odor and biofilm problems. With the exception of the large, open tanks in a wastewater treatment system, the major problem faced in decontamination as well as in cleaning is one of access. Access is required for monitoring, problem assessment, and problem resolution. Some newer emerging technologies combine methods for enhanced cleaning performance. Other industries face similar challenges with pipeline systems; their technical solutions may have potential application to stormwater and wastewater system decontamination (crossover technologies). If contamination cleanup is not feasible, methods to immobilize the contamination, where it is (pipe rehabilitation, e.g. pipe lining or in-place pipe replacement), may be an option.

### 2.1 Emerging Technologies

In culverts, which are used in some stormwater systems, silt often accumulates, providing a sink for contamination. A recent technological development allows for the removal of large amounts of soil and debris without structural damage [12]. The method employs a barrel reamer attachment, a round tool with fins and water jets, which rotates through the pipe, mixing water with dirt and debris. It is capable of cutting through roots and moving large rocks. Push or pull buckets may then be used to remove the debris from the pipe. Rotating wire brush and directional drilling attachments are also available. A controlled environment is maintained for optimum performance and handling of debris, especially if it is contaminated.

Another technology in the development stage uses dual rotating nozzles and variably sized cleaning tools as part of a vacuum unit that is extended into a pipe [12]. Debris is sucked into a holding tank as cleaning progresses.

Systems designed for sewer flushing are under constant development. Different systems that cause a flushing wave to pass through a sewer pipeline have been developed and used in France, Germany, and Switzerland [2].

### 2.2 Crossover Technologies

Chemicals are already used to control a variety of problems in wastewater systems. Expertise in the use of chemical solutions to clean pipe systems in other industries can

be brought to bear on the decontamination of stormwater and wastewater systems. The technology behind chemical cleaning to remove scale buildup in pipelines has been developed over time in a number of areas. Chemical cleaning of boilers and heat exchangers has been used for decades. Pipe cleaning has also evolved based on experience with marine vessels (waste pipelines, evaporators, and other equipment) and fire protection systems (stagnant water breeds biofilm and scale; many elbows, tees, and valves make other processes difficult) [13]. The chemical solution used is custom-tailored to the specific problem on the basis of the chemical nature of the scale and the type of pipe material. The solution is designed to penetrate, disperse, and dissolve the scale, while minimizing damage to the metallic components of a system.

In the closely allied area of drinking water systems, where compatibility with potable water is required, hydrochloric acid is typically used with weaker organic acids to bind dissolved metals. It is used with inhibitors to protect any base metal. The process involves a hydrant-to-hydrant recirculation system based on trailer-mounted equipment [13]. The length of pipe to be cleaned at one time is determined by the pipe's diameter, because the trailer-mounted holding tank must be large enough to contain the requisite volume of cleaning solution. Likewise, in the food industry, processing and delivery systems (e.g. equipment, pipes, tanks, and valves) must be periodically cleaned to eliminate chemical and biological contamination. Depending on the scenario, such methods and techniques may be translated for use in stormwater and wastewater systems.

In the nuclear industry, the use of chemical solvents for radioactive contamination of equipment and facilities is widespread. However, the primary application of these solutions is for metal surfaces. The use of chemical solvents on porous surfaces such as concrete is generally ineffective [14, 15]. Chemical decontamination is often a multistep process that involves either or both dilute and concentrated chemical reagents. Mild reagents are used primarily in an attempt to remove the contaminant material without attacking the base material. Such reagents require longer contact times with the contaminated material, but cause fewer problems with the treatment of secondary waste than do more-concentrated reagents [16].

## 2.3 Pipe Refurbishment or Replacement

Contamination firmly adhered to the inner wall of a pipeline, far removed from human contact, may not pose an immediate human health risk. In the case of biological or chemical agents, rinsing the pipeline with a neutralizing chemical solution may be the most expedient decontamination process. This option is not available for radioactive contamination. However, if effluent contamination levels are low and there is no concern about accumulation of higher concentrations in hot spots easily accessible to humans, no further action may be required.

Where cleaning methods are not effective (e.g. a heavily corroded sewer pipeline), pipe relining or replacement may be necessary if contaminant accumulation has occurred and/or the release of contaminants is likely in the future. Relining will not remove the contamination, but it will isolate the contamination in place between the inner wall of the pipe and the outer side of the new lining. Pipe cleaning and scraping will be necessary in order to reline a pipe, dislodging and removing some of the remaining radioactive material. Different relining methods include spray, slip, cured-in-place, and close-fit [12, 17].

Traditional pipe replacement (open cut [i.e. excavation]) is costly and disruptive to above-ground features and activities. Newer, less costly alternatives have been developed. Trenchless technologies such as pipe implosion, eating, reaming, ejection, and extraction result in pipe removal with concurrent installation of new pipe [18]. In such cases, any contamination could be removed with the old pipe and would have to be handled, treated, and disposed of properly. The most popular form of trenchless pipe replacement is pipe bursting in which the old pipe is fractured and the resulting pipe fragments are pushed outward as the new pipe is pulled in. This method works well with brittle materials such as cast iron, concrete, or clay. A newer method gaining popularity for use with more flexible pipe materials such as steel, ductile iron, and plastic is pipe splitting. In this case, the old pipe is slit with a series of cutting wheels and slightly expanded as the new pipe is pulled through. As a result, the new pipe is encased by the old pipe, providing some additional physical protection [19]. With pipe bursting or splitting, the old pipe is not removed, which means soil and groundwater may be exposed to any contamination. Thus, these methods should be used only if the contamination is expected to remain immobile.

## 3 CRITICAL NEEDS ANALYSIS

Wastewater and stormwater systems provide an infrastructure for carrying water away from most areas within an urban setting. Thus, they provide a readily available avenue for contaminated runoff and water-based decontamination activities. To best leverage this resource, reliable operational procedures (emergency options) and decontamination measures must be available to enable the use of these systems to full advantage.

### 3.1 Emergency Options

The location, nature, timing, and extent of a terrorist attack will determine what emergency response options are possible and reasonable. Depending on the circumstances, one approach could be to quickly contain the contamination in as small an area as possible, with the primary objective of keeping contaminated water out of the stormwater or wastewater systems (e.g. to keep contamination from reaching critical areas near stormwater drains). In this case, capture/management technologies and temporary, local water storage would need to be available to handle runoff from precipitation or decontamination water, if either is likely. The disposition of this contaminated water would require prior planning.

On the other hand, decontamination water may be directed to the stormwater system if contamination of the stormwater system is a minor concern. For example, the objective may be to clear the area of as much contamination as possible in the shortest amount of time to reduce human exposure or to remediate the contaminated area as soon as possible to restore public utilities or for economic reasons. However, once contaminated water is in the system pipeline, another set of options must be considered.

Whether the pipeline system contains stormwater or wastewater, the contaminated water may be allowed to take its regular course, diverted along an alternate path, and/or be sent to a temporary storage area. For stormwater systems, the sensitivity of the

normal outfall locations to the contaminant and the level of contamination must be weighed against potential diversion options, if any. For wastewater systems, it may be possible to remove the contamination in the treatment plant through standard or slightly modified treatment processes with little impact on continued operation, including decontamination of equipment if necessary. If time is needed to modify treatment processes or contamination of the treatment plant is a concern, contaminated water could be diverted to temporary storage, if available, or diverted directly to the environment.

### 3.2 Decontamination Measures

The selected option for handling contaminated water should come from an informed decision based on knowledge of the ramifications of a given choice versus its alternatives. Informed decision making requires that, for each option, an understanding of the contamination pathway, potential impacts, and the ensuing costs (health, environmental, and socioeconomic) be considered.

The widespread presence of stormwater and wastewater systems in urban areas makes them a useful asset in an emergency if low-cost, easily implemented decontamination methods for their remediation are available. Appropriate methods and their efficiencies will depend on the location of the contamination within the system, its adherence or incorporation into debris or pipe material, and its concentrations. Contamination levels in a pipeline and at the final destination of the pipeline will depend on a number of factors, including length of pipe traveled, pipe condition (material composition, extent of corrosion, and debris content), water flow, and contaminant properties (physical and chemical). Successful decontamination depends on the desired residual concentration levels and the effectiveness of the selected decontamination method. Complications that may arise include concentration of the contaminant in hot spots (before and during decontamination efforts) and methods for capture and treatment of the solid and liquid wastes.

Pipelines may be treated on a section-by-section basis while other sections remain operational. However, decontamination of a portion of a wastewater treatment plant, if not conducted properly, may lead to shutdown of the entire treatment system. Thus, work is needed to assess the effects of potential decontamination methods and their applicability to contamination at various locations along the treatment train. For example, if chlorine is used at the pretreatment stage to kill a biological agent or neutralize a chemical agent in the route of the incoming wastewater, it can be carried further along and eventually kill beneficial organisms in the secondary treatment stage.

The ability to successfully decontaminate a wastewater treatment plant also gives emergency planners and managers the option to treat any contaminated water at the plant, halting the spread of further contamination, if a viable water treatment methodology can be implemented.

## 4 RESEARCH DIRECTIONS

For effective decontamination of wastewater and stormwater systems, solutions that are compatible with existing equipment and that can be deployed rapidly and cost effectively

are required. Simple technologies minimize the need for highly specialized training and large capital investments for dedicated equipment with limited or no use beyond their designed purpose. For many agents, some treatment methods are available. However, understanding the complex interactions of terrorist's agents of concern with the urban environment and the real-world efficacy of proposed decontamination technologies is necessary to support decisions and actions involving the various options discussed in the previous section.

Future work is necessary in a number of areas. A potential threat must be understood within the environment in which it could be pursued before an effective countermeasure can be applied. Thus, conceptual system models need to be developed and exercised under a range of attack scenarios to determine the key aspects of contaminant fate and transport as well as potential mitigative measures (a system sensitivity analysis). The agents that pose the greatest threat and where they are likely to be found must be identified. The effectiveness of decontamination or mitigation technologies needs to be known for each type of threat (chemical, biological, or radioactive), crossover technologies should be exploited, and common treatment technologies need to be identified.

### 4.1 System Threat

To properly prepare for system decontamination prior to an unknown terrorist attack, it is necessary to identify which agents pose the greatest threat in wastewater and stormwater systems and where the greatest threat will be. A number of chemical and biological agents are readily hydrolyzed, and thereby neutralized, when they come into contact with water. Thus, carried by water flow, they pose little or no threat as they enter the system (see hhs192). Work is needed to identify those agents that remain a hazard once they are in the system.

Once contaminants are in a system, it is necessary to know where they are likely to distribute themselves so that decontamination efforts will focus on the high-concentration areas and response workers can take the proper precautions against exposure. Transport within the system will depend on the chemical and physical properties of the contaminants. Questions that need to be answered include how water is distributed within the system, how much contamination is expected to be trapped in the pipeline system, and how much is expected to enter wastewater treatment plants or the environment (e.g. retention/detention ponds). Common hot spots may be where debris collects at irregularities in the pipelines, such as catch basins in stormwater systems and manhole locations in wastewater systems. Such hot spots may act as an initial sink for contamination immediately following a release and act as a source as time passes.

Individual systems will need to be independently studied for consideration of system extent (e.g. length of pipe in use, cross-connections, and number and location of collection and discharge points), age (e.g. extent of biofilm, corrosion, and silt buildup), pipe characteristics (material, shape, and diameter), pipe elevations, and typical water flows. Initial work in this area would be served by system flow model development and could involve case studies of representative systems using tracers to help identify hot spots in individual systems from which some generalizations may be made for different contaminant types in wastewater and stormwater systems.

### 4.2 Decontamination Technology Effectiveness

A number of effective methods to clean wastewater and stormwater systems are available. Because contaminants were in a form that allowed them to enter the system as did dirt (particulates), hazardous chemical, biological, and radioactive materials are likely to be removed with standard cleaning methods. However, some fixed contamination may remain. For full-scale testing of traditional wastewater and stormwater system cleaning procedures, tracers or harmless contaminant surrogates could be used to determine if desired decontamination levels can be achieved.

The effectiveness of decontamination technologies will also depend on pipe or tank material (e.g. cast iron, concrete, and plastic). As aging systems are replaced, decontamination research should focus on the materials being used in replacement hardware and new construction. Finally, decontamination technology development must consider the potential for hazardous by-products, treatability of liquid and solid wastes, waste disposal implications, and the time and cost constraints for employing a technology.

### 4.3 Crosswalk between Disciplines and Industries

The neutralization and destruction of biological agents have been extensively studied and used in medical research, the health care industry (e.g. hospitals), and military programs. Likewise, the neutralization and destruction of chemical agents have been extensively studied in military programs [7, 20]. For radioactive contamination, a large amount of information has been generated by the nuclear industry from operations involving routine maintenance and decontamination and decommissioning activities during site cleanup [14, 15, 21]. Information is also available from the oil and gas industry, which contends with naturally occurring radioactive material buildup in pipes. In addition, data on the maintenance and cleaning of other pipeline systems (e.g. boiler and heat exchangers, marine vessels, fire protection, and food processing) can be exploited. This wealth of information can be combined with some traditional wastewater and stormwater cleaning methods to deliver chemical cleaning solutions to contamination within pipelines.

If the pipelines are not completely pressurized (to minimize secondary decontamination waste streams), sufficient solution-pipe contact time may be difficult to achieve. Increased contact times can be enhanced by the use of foams or gels, but delivery systems for interior pipe walls would need to be developed for this application. Spray lining larger-diameter pipes with epoxies or cementitious materials is an established pipeline rehabilitation method [12]. Modification of equipment for the handling of foams or gels may be a reasonable option. Ultraviolet (UV) radiation is a common neutralization technology used for the destruction of chemical and biological agents. Again, this technology may be viable for inside pipelines if a delivery system could be developed, perhaps coupled with remote technologies already used by contractors who specialize in stormwater or wastewater pipeline cleaning and maintenance.

Technologies in development to neutralize chemical and biological agents within a building environment may be applicable to pipelines. The use of gaseous hydrogen peroxide or chlorine dioxide as fumigants has been studied for use in contaminated rooms and ductwork [22]. Gas-phase delivery would enable contact with the entire internal wall of the contaminated pipe.

### 4.4 Common Treatment Technologies

The ideal decontamination technology for wastewater and stormwater systems would handle most potential threats from all three types of contamination—chemical, biological, and radiological. Many current cleaning methods for pipelines hold the promise as universal cleaning technologies because they are designed to physically remove all contamination. Research in this area is important to minimize the infrastructure necessary to support readiness and to respond to combined attacks (e.g. chemical and radiological).

Many oxidation methods have widespread application for a range of chemical and biological agents. Incorporation of these methods into a decontamination technology could leverage existing processes used in the drinking water and wastewater industries, relying on existing institutional knowledge and technology (e.g. the use of chlorine as a disinfectant). For example, hypochlorite solutions (at different strengths) have been recommended for use against both chemical and biological agents in military applications in the field [7, 20].

## 5 GENERAL CONSIDERATIONS AND SUMMARY

Although methods for the decontamination of wastewater and stormwater systems are available, they may not remove or neutralize agents to acceptable levels. Cost and time considerations may also drive better technology development. Table 1 summarizes available and potential technologies. Research is necessary to determine the most expedient methods for different situations and to develop a reliable suite of decontamination technologies ready to deploy in any metropolitan area. New or enhanced decontamination technologies should

- leverage existing methods;
- minimize exposure to response workers;
- minimize impact to the system and the environment; and
- minimize cost.

One way to reduce impacts is to focus on technologies that minimize the amount of secondary contaminated wastes generated. Less secondary waste reduces the amount of subsequent waste treatment and disposal. In two studies of radioactive contamination at sewage treatment plants, proper disposal of contaminated sludge was a significant cost incurred for those sites where cleanup was conducted [23, 24].

Decontamination of wastewater and stormwater systems is complicated by the inaccessibility of interior pipe walls. Flushing operations are simple, but will generate large amounts of secondary waste, especially for larger pipes. Methods such as jetting reduce the amount of water needed, but still require significant amounts of water compared to technologies that use foams or gels. Delivery of UV radiation or gaseous neutralization compounds to chemical or biological contamination is a possibility. Delivery systems for large-diameter pipes should be an important area of research.

**TABLE 1 Summary of Available and Potential Technologies for Pipeline Decontamination**

| Technology | Applicability[a] | | | | Comments |
|---|---|---|---|---|---|
| | Rad | Chem | Bio | Available[b] | |
| Contaminant Removal | | | | | |
| Physical processes | Y | Y | Y | Y | Includes traditional mechanical pipe cleaning methods that are designed for removal of dirt and debris; some residual contamination may be left on interior pipe walls |
| Chemical solutions | Y | Y | Y | Y | Solutions need to be tailored to contaminant and pipe material |
| Foams and gels | Y | Y | Y | N | Technology and delivery systems need improvement |
| Pipe removal | Y | NR | NR | Y | Recommended only for extreme case of radiological contamination |
| Agent Neutralization | | | | | |
| Chemical solutions | N | Y | Y | Y | Solutions need to be tailored to contaminant and pipe material |
| UV radiation | N | Y | Y | N | Development of delivery systems required |
| Chemical gases | N | Y | Y | N | Development of delivery systems required |
| Leave in-Place | | | | | |
| Fix in-place (pipe rehab) | Y | NR | NR | Y | Recommended only for extreme case of radiological contamination |
| Pipe bursting or splitting (pipe replacement) | Y | NR | NR | Y | Recommended only for extreme case of radiological contamination |

Y, yes; N, no; NR, not recommended, other methods are more cost effective.
[a]Applicability indicates a technology's suitability for decontamination of stormwater and wastewater system pipelines (e.g. cost and efficiency).
[b]Indicates if the technology is currently available for use. Further development may be required to reach its full potential as a decontamination technology.

## REFERENCES


1. U.S. Environmental Protection Agency (1999). *Collection systems O&M fact sheet, sewer cleaning and inspection, EPA 832-F-99-031*, Office of Water, Washington, DC.
2. Fan, C. Y. (2004). *Sewer sediment and control, a management practices reference guide, EPA/600/R-04/059*. Office of Research and Development, National Risk Management Research Laboratory, Cincinnati, Ohio.
3. U.S. Environmental Protection Agency (1991). *Hydrogen sulfide corrosion in wastewater collection and treatment systems, EPA 430/09-91-010*, Office of Water, Washington, DC.
4. U.S. Environmental Protection Agency (2005). *Handbook on the Management of Munitions Response Actions, Interim Final, EPA 505-B-01-001*, Office of Solid Waste and Emergency Response, Washington, DC.

5. Munro, N. B., Talmage, S. S., Griffin, G. D., Waters, L. C., Watson, A. P., King, J. F., and Hauschild, V. (1999). The sources, fate, and toxicity of chemical warfare agent degradation products. *Env. Health Perspec*. **107**(12), 933–973.
6. Khan, A. S., Swerdlow, D. L., and Juranek, D. D. (2001). Precautions against biological and chemical terrorism directed at food and water supplies. *Public Health Rep*. **116**(1), 3-14.
7. Hurst, C. G. (1997). Decontamination. Chapter 15 in *Medical Aspects of Chemical and Biological Warfare. Office of the Surgeon General at TMM Publications*, F. R., Sidell, E. T., Takafuji, and D. R., Franz, Eds. Walter Reed Army Medical Center, Washington, DC.
8. McGuire, R. and Raber, E. (2001). *Oxidative decontamination of chemical and biological agents using L-gel, UCRL-AR-143212*, Lawrence Livermore National Laboratory, Livermore, California.
9. Spellman, F. R. (2003). *Handbook of water and wastewater treatment plant operations*, Lewis Publishers, New York.
10. HDR Engineering Inc. (2001). *Handbook of Public Water Systems*, 2nd ed., John Wiley & Sons, New York.
11. Pizzi, N. G. (2002). *Water Treatment Operator Handbook*, American Water Works Association, Denver, Colorado.
12. U.S. Environmental Protection Agency. 2006. *Emerging technologies for conveyance systems, new installations and rehabilitation methods, EPA 832-R-06-004*, Office of Wastewater Management, Washington, DC.
13. Ellison, D. (2003). *Investigation of pipe cleaning methods*, Awwa Research Foundation and American Water Works Association, Denver, Colorado.
14. U.S. Department of Energy. (1994). *Decommissioning Handbook*, Office of Environmental Restoration, Washington, DC, March.
15. Taboas, A. L., Moghissi, A. A., LaGuardia, T. S. (eds.). 2004. *The Decommissioning Handbook*, ASME Press, New York, New York.
16. International Atomic Energy Association. (2001). *Methods for the minimization of radioactive waste from decontamination and decommissioning of nuclear facilities*, Technical Reports Series No. 401, IAEA, Vienna, Austria.
17. United Nations Environment Program (Division of Technology, Industry, and Economics, International Environmental Technology Center) and the International Society for Trenchless Technology. (2001). *Trenchless technology systems, an environmentally sound approach for underground services*, Japan/United Kingdom. UNEP-DTIE-IETC/ISTT.
18. Simicevic, J., Sterling, R. L. (2001). *Guidelines for pipe bursting, TTC Technical* Report #2001.02, prepared by the Trenchless Technology Center, Louisiana Tech University, Ruston, Louisiana, for the U.S. Army Corps of Engineers, Engineering and Development Center, Vicksburg, Mississippi.
19. Chapman, D. N., Ng, P. C. F., Karri, R. S. (2004). Research needs for on-line replacement techniques, prepared for presentation at the *Fifth NETTWORK Workshop, University of Birmingham*, Birmingham, England.
20. Yang, Y.-C., Baker, J. A., Ward, J. R. Decontamination of chemical warfare agents. *Chem. Rev*. **92**: 1729–1743.
21. U.S. Environmental Protection Agency. (2006). *Technology reference guide for radiologically contaminated surfaces, EPA-402-R-06-003*, Office of Air and Radiation, Washington, DC.
22. U.S. Environmental Protection Agency (2007). *Report on the 2006 workshop on decontamination, cleanup and associated issues for sites contaminated with chemical, biological, or*

*radiological materials*, EPA/600/R-06/121, Office of Research and Development, National Homeland Security Research Center, Cincinnati, Ohio.

23. U.S. General Accounting Office (1994). *Nuclear regulation, action needed to control radioactive contamination at sewage treatment plants*, GAO/RCED-94-133.
24. Interagency Steering Committee on Radiation Standards (2005). *ISCORS assessment of radioactivity in sewage sludge: recommendations on management of radioactive materials in sewage sludge and ash at publicly owned treatment works*, ISCORS Technical Report 2004-04; DOE/EH-0668; EPA-8-32-03-002B, USA.

## FURTHER READING

Bell, C.G. Jr., Thomas, H.A. Jr., Rosenthal, B.L. (1954). *Passage of nuclear detonation debris through municipal waste treatment plants . in Sanitary Engineering Conference*. Baltimore, Maryland, WASH-275, U.S. Atomic Energy Commission, Division of Reactor Development, Washington, DC.

Crittenden, J.C., Trussell, R.R., Hand, D.W., Howe, K.J., and Tchobanoglous, G. (2005). *Water treatment: principles and design*, 2nd ed., John Wiley and Sons, New York.

Fox, K.R. (2004). Water treatment and equipment decontamination techniques. *J. Contem. Water Res. Educ*. **129**, 18–21.

Gafvert, T, Ellmark, C, Holm, E. (2002). Removal of radionuclides at a waterworks. *J. Environ. Radioact*. **63**, 105–115.

Glymph, T. (2005). *Wastewater microbiology, a handbook for operators*, American Water Works Association, Denver, CO.

Goossens, R, Delville, A, Genot, J, Halleux, R, Masschelein, W.J. (1989). Removal of the typical isotopes of the Chernobyl fall-out by conventional water treatment. *Water Res*. **23** (6), 693–697.

Gowser, K.E, Tamura, T. (1963). Significant results in low-level waste treatments at ORNL. *Health Phys*. **9**(7), 687–696.

Hammer, M.J. (1977). *Water and wastewater technology*, John Wiley and Sons, New York.

Hickey, E.E, Strom, D.J. (2005). *Technical basis for radiological emergency plan annex for WTD emergency response plan: West Point treatment plant*. PNNL-15163 Vol. 3. Pacific Northwest National Laboratory, Richland, Washington.

Metcalf and Eddy, Inc. 1987. *Wastewater engineering: treatment, disposal, reuse*. Tata McGraw Hill Publishing Company, New Delhi, India.

National Association of Clean Water Agencies. (2005). *Planning for decontamination wastewater: a guide for utilities*. National Association of Clean Water Agencies, Washington, DC.

Pacific Northwest Laboratory. (1994). *Reconcentration of radioactive material released to sanitary sewers in accordance with 10 CFR Part 20*. NUREG/CR-6289, Richland, Washington.

Sarai, D.S. (2005). *Basic chemistry for water and wastewater operators*. American Water Works Association, US Nuclear Regulatory Commission, Denver, CO.

Stetar, E.A, Boston, H.L, Larsen, I.L, Mobley, M.H. (1993). The removal of radioactive cobalt, cesium, and iodine in a conventional municipal wastewater treatment plant. *Water Environ. Res*. **65**(5), 630–639.

Straub, C.P. (1955). Limitations of water treatment methods for removing radioactive contaminants. *Public Health Rep*. **70**(9), 897–904.

U.S. Environmental Protection Agency. (1999). *Combined sewer overflow O&M fact sheet, EPA 832-F-99-039*, Office of Water, Washington, DC.

U.S. Environmental Protection Agency. (2004). *Primer for municipal wastewater treatment systems, EPA-832-R-04-001*, Office of Water, Office of Wastewater Management, Washington, DC.

# PREVENTION OF CONTAMINATION OF DRINKING WATER IN BUILDINGS AND LARGE VENUES

WILLIAM B. SAMUELS AND RAKESH BAHADUR
*Science Applications International Corporation, McLean, Virginia*
WALTER M. GRAYMAN
*W. M. Grayman Consulting Engineer, Cincinnati, Ohio*
RICARDO P. BORJA
*Malcolm Pirnie, Inc., White Plains, New York*

## 1 INTRODUCTION

According to an article in the Engineering News-Record [1]:

> "simple measures that can protect the inhabitants of a building or users of critical infrastructure from chemical and biological attack are becoming routine since the September 11 terrorist attacks and the subsequent anthrax outbreaks. Many building owners and developers are demanding that design criteria for their projects include security master plans. And those in charge of protecting infrastructure are working out protocols to protect water, wastewater, and other systems. These include risk assessments to determine how much security is truly needed."

As quoted in the article [1], Keith Henson, director of security services for Lockwood Greene, Spartanburg, South Carolina reported on "four basic methods of protecting assets: modifying daily routines of building facilities and maintenance personnel; changing the security force; installing physical barriers; and adding electronic surveillance systems. Often, the simplest protection from any threat is distance."

Lessons can be learned from the experience of the US military in protecting buildings. As reported in the Engineering News-Record [1]:

> the US Army Corps of Engineers is charged with protecting the armed forces, including civilian employees, from chemical, biological and nuclear attacks in military buildings. Each military installation is responsible for designing its own buildings. The Corps' Construction and Engineering Research Laboratory in Champaign, Illionois, is developing a software tool to ensure that architects can understand the threats and design buildings to a certain threshold of protection. The Corps expects the software to familiarize designers with various materials as well. Some building materials are almost impossible to clean while others only need to be wiped down. Other high tech materials, such as carpet that can neutralize contaminants,

are under investigation. The laboratory is participating in a program run by the Defense Advanced Research Program Agency to develop buildings that are immune to chemical, biological, and radiological attacks.

City building codes typically require the owner or agent of a dwelling building to supply potable, safe, drinking water to the occupants. In addition, water supply systems need to be designed and installed so as to provide at all times, a supply of water to plumbing fixtures, devices and appurtenances in sufficient volumes and at adequate pressures to enable them to function satisfactorily under normal conditions of use. In addition, building codes typically require all users of a public water system to prevent cross-connections between the potable water piping system and any other piping system within the premises. This means that there must be a procedure or protocol in place at these buildings that is acceptable to a municipality, and that fully describes how these venues plan to manage their building in protecting and securing the drinking water system for the building and all appurtenances associated with the water system. In addition, the facility management must be aware of all employees, maintenance personnel, and contractors that come in contact directly or indirectly with the water system for the buildings under their control or portion therein.

An unscrupulous person using very simple tools or equipment, could compromise the drinking water system for any building or potentially, for a full city block or more. This could potentially result in the illness or death of the occupants of the affected building or area. Appropriate steps must be taken by building management to prevent such potentially problematic actions from occurring.

There must be a reassurance that the occupants of "high profile" buildings, either permanent or temporary, have a protected, safe, and secure drinking water system, and the employees or contractors working within these buildings are screened to reduce the potential to tamper or compromise the buildings' water supply system, or other critical mechanical systems (heating, ventilating, and air conditioning [HVAC], sprinklers) in these buildings. Also, that the drinking water in adjacent buildings is not affected by any terrorist act. There is a general attitude in the water industry that dilution keeps chemical contamination from being much of a threat to water systems; however, according to Ed Wetzel (Montgomery Watson Harza), as quoted in the Engineering News-Record [1] "there is no way to guarantee that a water system is 100% safe. As with buildings, the beginning point for protection is assessing the vulnerability of the system."

## 2 BUILDING AND PLUMBING ASSESSMENT

This assessment identified equipment and components of typical domestic water distribution systems in large buildings and venues such as in low rise and in high rise, commercial and residential buildings. Components of these systems include typical water service connections, associated piping, valves, tanks, pumps, water flow, and pressure characteristics. This information is essential in analyzing the vulnerability of such domestic water distribution systems to possible injection of contaminants.

### 2.1 Typical High Rise Configuration

Although exact configurations and designs of internal plumbing systems may vary from building to building, the potable water systems in high rise buildings are typically divided

into vertical zones. The zones are designed so that they can be served by a gravity or booster pump system while ensuring adequate (but not too high) pressure throughout the zone. Building codes vary from city to city; however, each zone typically encompasses about 25 floors but may not exceed 370 ft. For buildings larger than 370 ft, additional zones must be constructed. Furthermore, zones supplied by pumps may not exceed 300 ft.

Figure 1 shows an example of a schematic diagram of a domestic water distribution scheme in a 43-story high rise building, using a gravity tank supplying the upper zone of the building and a pump system supplying the lower zone of the building. This scheme is used when space for an intermediate gravity house tank is not available. Frequently, a tank is located above the bottom zone and water is pumped to that tank and then fed by gravity to the bottom zone.

### 2.2 Typical Low Rise Configuration

Similar to high rise buildings, the domestic water distribution system in a low rise may vary slightly in design from building to building, but they are typically one-zone systems supplied directly from the street main or via a booster pump system. A booster pump system normally supplies the higher portion of the building to achieve the minimum pressure required to operate a plumbing fixture or equipment. The lower portion of the building, like the ground and sublevels, are normally fed using the available street pressure. A suction tank may be required in a booster pump system.

Figure 2 shows an example of a schematic diagram of a low rise domestic water distribution system represented by a 10-story low rise building. In this example, a booster pump system combined with two large hydropneumatic tanks is being utilized. The hydropneumatic tanks primarily provide a constant boosted pressure in the distribution system and secondarily serve as storage.

Generic computer models of the water supply systems of a two-zone high rise and a low rise building have been constructed based on the general diagrams shown in Figures 1 and 2 respectively and on information gained from site visits to various buildings. These models were used to study, assess, and visualize various contamination scenarios. These modeling results are discussed further on in this article.

## 3 WATER SYSTEM COMPONENTS ASSOCIATED WITH LARGE VENUES

Water systems in large venue buildings typically include the following types of components: piping, pumps, storage tanks, backflow prevention devices and valves. Each of these components can serve a role in the potential introduction of a contaminant into the water system. In the following sections, a range of each type of component is described.

### 3.1 Piping Systems

Internal piping within commercial buildings generally range from 6-in. diameter for transmission pipes serving zones, down to 3/4-in. diameter or less for pipes serving individual fixtures. Typical pipe materials for service connections and domestic water distribution systems are cement-lined ductile iron for piping 4 in. and larger, and copper or red brass for piping smaller then 4 in. Pressure in pipes can range from around 28 psi at fixtures to 200 psi in some transmission piping within a building.

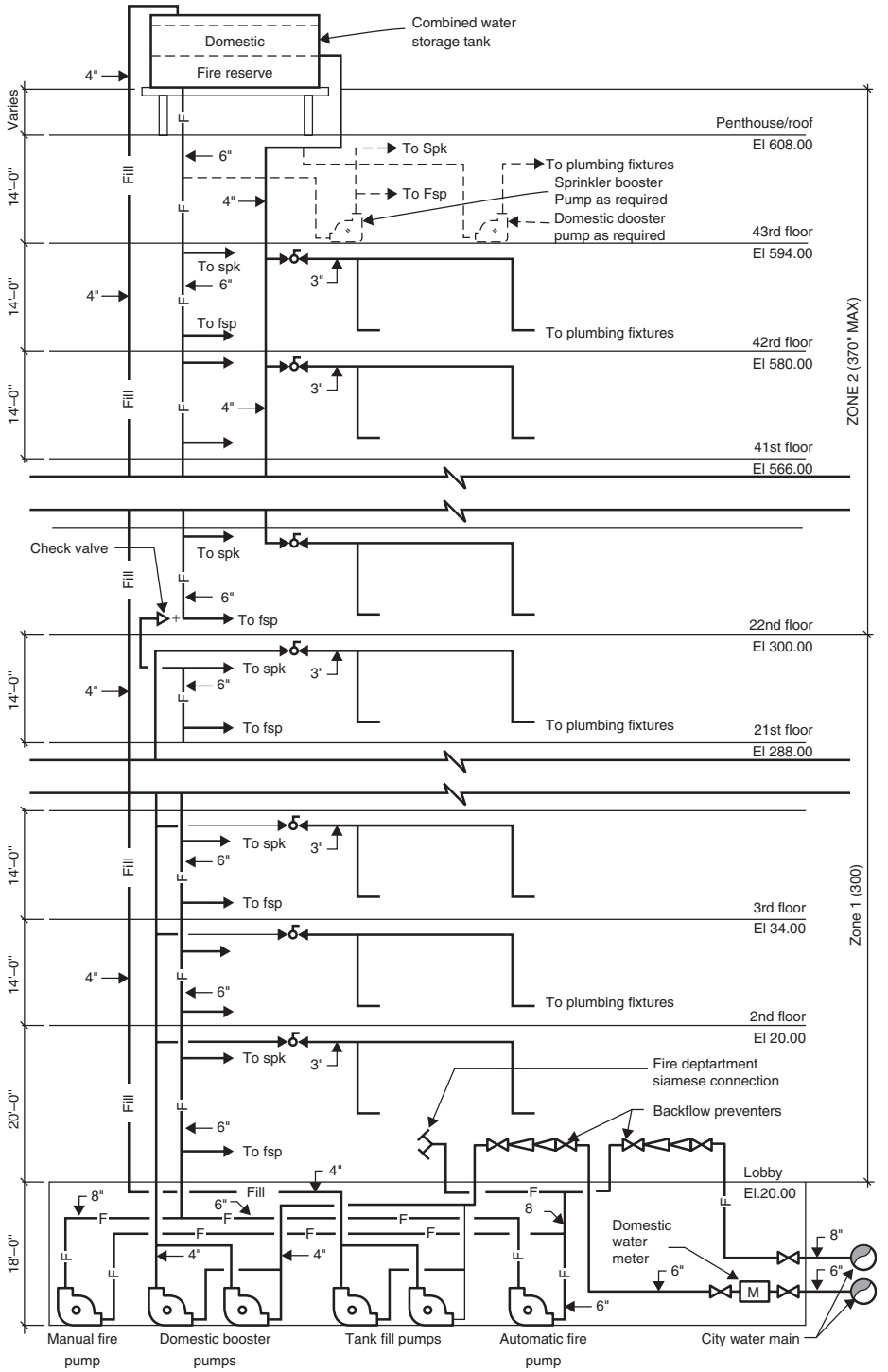



**FIGURE 1** Typical high rise building with gravity tank and pump zones.

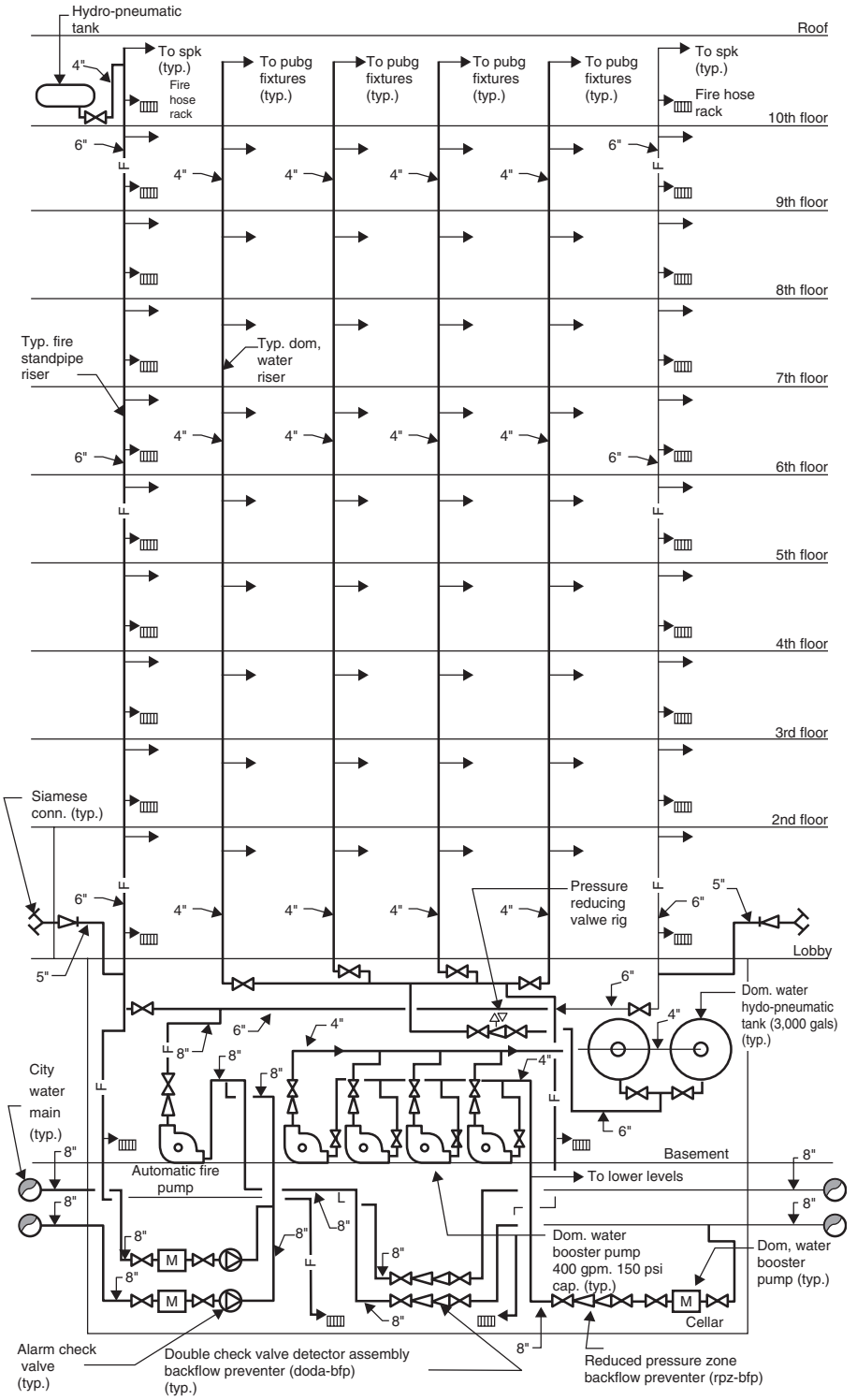



**FIGURE 2** Typical low rise building with a booster pump system.

### 3.2 Pumps

In most buildings, large, electrically driven, positive displacement pumps located in the basement are used to pump water to elevated tanks and/or to directly pump water for use throughout the building. A contaminant injected on the suction side of such pumps would be spread throughout the zone or area served by the pump. Additionally, there are numerous types of temporary pumps that are widely used in buildings for pressure testing of sprinkler and plumbing piping systems.

### 3.3 Storage Tanks

There are several water storage tank designs associated with a typical domestic water distribution system in large venue buildings. All are potentially quite susceptible to injection of contamination. Hot-water storage tanks and thermal expansion tanks are normally sealed and provided with backflow prevention devices at the water connection to protect the domestic water system from potential contamination. Therefore they are considered low risk for such contamination. The various types of storage tanks are described below.

Gravity house tanks serve as the main water supply of typical high-rise buildings. Due to excessive heights of high rise buildings, it became a disadvantage to use a pump to supply and maintain the pressure and flow required for domestic water distribution. This is especially true in very tall buildings, where the use of gravity storage tanks started and has become very popular. Gravity tanks are atmospheric type tanks and are normally built of wood, steel, or equivalent materials. Except for wooden tanks, they are lined with food grade rubber linings or other approved nontoxic coatings. Wooden tanks are always cylindrical in shape while steel and other tanks can be rectangular or cylindrical. The most popular and widely used gravity tanks in high rise buildings are wooden tanks because they are very reliable, easy to maintain and replace. The two types of wood used for wooden tanks are yellow cedar and redwood. Durability-wise, these tanks can last for 20 to 30 years and can withstand most harsh weather conditions. In a typical high rise application, gravity house tanks are used for combined service, in which the domestic water and fire water reserve are stored in the same tank. Typical capacities for gravity house tanks are from 10,000 to 16,000 gal per zone. Gravity tanks are susceptible to contamination because they are atmospheric tanks and have accessible openings for servicing and open-ended pipe trim such as the overflow pipe and drain pipe.

Suction tanks are atmospheric type tanks and have similar trim and components to gravity house tanks except for the discharge piping, which is directly connected to a pump or series of pumps. These tanks are auxiliary equipment to the domestic water system and that may be required if any power pump or booster pump supplying the domestic water system or portion of the system cannot be directly connected to the city water main. These tanks are mostly made of steel, and come in rectangular or cylindrical shapes. Typical capacities for these tanks are 7500 gal with pump capacity of 400–500 gpm and 10,000 gal with pump capacity of 501 gpm or more.

Hydropneumatic tanks are closed, pressure type tanks and are used with water booster pump systems to boost and maintain a constant pressure in a water distribution system. Although the sole purpose of a hydropneumatic tank is to boost inadequate pressure and properly cycle pumps, it has also been widely used as a storage tank until the early 1970s. This resulted in oversized tanks that require large mechanical spaces in a building. The erroneous idea that a reserve water capacity is available, similar to a gravity tank system, has been a major contributing factor to the misapplication of these systems. The design

is flawed because when the low pressure limit is reached, the remaining water in the tank is absolutely useless to satisfy any system demand. Nowadays, hydropneumatic tanks are smaller and are being used solely to boost inadequate pressure in a water system. These tanks although closed and pressurized, are also susceptible to intentional contamination because they are provided with drain valves and air charging fittings, where a pump can be connected easily to inject contamination.

### 3.4 Backflow Prevention Devices

Backflow preventers are devices designed to prevent back-siphoning and back-pressure from adding contaminated fluids into a potable water supply due to cross-connection in building plumbing systems. Cross-connections are actual or potential connections between a potable and nonpotable water supply that constitute a serious public health hazard. The backflow preventer device described below is used in typical service connections of high rise buildings or large venues to protect the city water supply.

A reduced pressure zone (RPZ) Backflow preventer device provides the maximum protection against back-siphoning and back-pressure condition, and is normally used in high hazard applications. It consists of two check valves and a differential zone with a relief valve between the two checks. The relief valve normally stays closed due to the pressure exerted by the zone. The zone is always maintained at least 2 lb less than the supply pressure. When the supply pressure drops, the pressure in the zone will also drop and cause the relief valve to open and discharge the water from the system side of the water system to the atmosphere. This device is furnished with test cocks and gate valves to enable testing.

### 3.5 Valves

System valves include meter test tees, drain valves, and strainers. A meter test tee consists of a shut-off valve (normally a gate valve) joined with a piece of pipe or nipple that has a cap at the outlet. This test tee is connected to the main pipe downstream of a water meter and used to test and calibrate the flow of water through a meter. Drain valves are used to remove water, partially or totally from the lowest portion of tanks or piping system. These valves are normally gate or ball valves. Other types such as electronic or mechanical automatic drain valves can also be used, depending on the type of application. Strainers are used to separate and collect debris, such as sands, stones, and other foreign materials from water flowing through a piping or tank systems. The two most commonly used strainers in a water distribution system are the basket and “wye-pattern” strainers. These strainers have accessible retainer caps and basket covers that can be easily opened by hand or a simple hand tool for maintenance.

### 3.6 Wall Hydrants

Wall hydrants are devices used for cleaning of building exteriors and miscellaneous irrigation purposes. These valve assemblies are mounted on exterior walls of buildings and equipped with hose end connections. The two most popular types used in buildings are the exposed type, where the valve outlet and key operator are mounted exposed from the exterior wall and the enclosed type, where the valve is in a box, locked and flushed with the exterior wall. These valves are directly connected to the domestic water distribution piping.

### 3.7 Service Connections

Typical design flows for large commercial buildings can range from 65 to 400 gpm per service connection depending on the number of house tanks, booster pumps, and fill pumps in a building. The length of the connection and the presence of appurtenances such as valves and fittings vary depending upon the specific local requirements and conditions. A service connection to a building is typically designed to a maximum working pressure of 200 psi. However, internal plumbing fixtures and equipment are generally designed to a lower working pressure, thus requiring pressure reducing valves (PRVs) to reduce the incoming pressure before supplying plumbing fixtures and equipment. Typical pipe materials for service connections and domestic water distribution system are cement-lined ductile iron for piping 4 in., and larger and copper or red brass for piping smaller then 4 in.

In order to pump a contaminant from within a building into the external water system, the pump must overcome the pressure in the receiving main in addition to losses associated with moving the water from the building to the main. For pipes, the friction losses are based on the pipe diameter, the flow or velocity, and the roughness of the pipe. Additional losses are associated with appurtenances such as bends, valves, meters, and so on. Typical roughness coefficients (C-factor used in the Hazen-Williams equation) for new pipes are in the range of 120–150 depending upon the material. As the pipe ages, a pipe can become pitted or corroded leading to lower roughness factors. More typical C-factors for older, small diameter pipes used as connections would be in the range of 100–120. Minor losses associated with bends, valves, and so on are generally in the range of 0.2–2.

## 4 WATER SUPPLY VULNERABILITY

Under the headline, "Water Utility Officials Fear 'Backflow' From Terrorists - Reservoirs May Be Safe, but House Pipes Can Be Used to Push Toxins Into a Neighborhood," the Wall Street Journal [2] published an article on the vulnerability of households and other buildings to the introduction of contaminants into the water system. Although the article also sensationalized the issue by stating that "the flow of water into a house or business ... can be accomplished with a vacuum cleaner or bicycle pump," it did correctly identify this vulnerability. A Department of Defense Report [3] correctly stated that, "All faucets are vulnerable to an internal release, depending on physical accessibility and line pressure. Agents can be introduced into a building's water distribution system if the water line pressure in its piping, pressure tanks, or water softener treatment system is overcome." Without adequate and secure backflow devices, a contaminant introduced into a building could also be pumped into the distribution system, effectively contaminating parts of the public water system.

Recognizing the potential vulnerability of water distribution systems to intentional contamination, there has been a significant body of work addressing this issue [4]. However, there has been very little published on the subject of the impacts within a building that has been contaminated through the direct introduction of contaminants into the plumbing system. For large buildings, such contamination could potentially impact hundreds or even thousands of people.

### 4.1 Potential Soft Targets in Large Venues

Based on examination of plumbing plans for large venue buildings, and professional experience, the following soft targets were identified as potential entry points for intentional contamination. Although any direct connection to the water system (e.g. sinks, hose bibs, etc.) could serve as an entry point, the following are specific identified targets within most buildings.

1. In a combined system (fire protection and domestic service served from the same system), a pump could be hooked up to the Siamese connection and contaminant pumped directly into the building system or building tank. The Siamese connection is used as an auxiliary water supply designed so that the fire department can hook up their pumper truck and supply water to the internal fire system (e.g. sprinklers). This would not be effective if there is a separate fire and domestic system. Wall hydrants could serve as a similar entry point for a contaminant.
2. A contaminant could be directly introduced into a tank within the building without a pump.
3. From a utility closet (or other fixture), a pump could be hooked up and pumped directly into the water system. If there is a check valve on the tank then the contaminant could not be pumped into the tank in this manner.
4. An RPZ backflow preventer is a port that a pump could be attached to, at a relatively low pressure. There is usually a test connection that is readily available and could be used.
5. There is frequently a test connection (outlet) on the downstream side of a meter. This provides access to the entire system served by that meter.
6. Many large venue buildings have tanks located on their roofs (see Table 1 below). Typically, doors leading to the roof are not locked from the inside since they are used as fire exits (though they may be alarm-fitted). This could allow entry to a tank on the roof.
7. Direct injection into a hydropneumatic tank.

**TABLE 1 Potential Scope for Contamination through Alternative Entry Points**

| Entry Point | Contamination Potential |
|---|---|
| Siamese connection/ wall hydrant | Entire building |
| Tank | Zone |
| Fixture | Part of zone or building |
| RPZ port | Entire building |
| Meter connection | Entire building |
| Roof access | Zone |
| Hydropneumatic tank | Zone or entire building |

The entry points for potential contamination in buildings can be grouped as follows:

1. Entry points that have the potential to contaminate the entire building
2. Entry points that have the potential to contaminate a single zone (in a multizone building) or the entire building in a single zone building
3. Entry points that have the potential to contaminate a part of the building or a zone.

Table 1 describes the potential spatial scope of contamination for the seven entry points previously described.

### 4.2 Hydraulic Models and Contamination Scenarios

In order to test the potential impacts of a contamination event in a building, hydraulic models representing two generic large buildings were constructed. The models are used to investigate the movement and spread of contamination for alternative contamination scenarios. Scenarios investigated include different locations for the injection, different injection quantities, durations, and times.

The first set of model scenarios corresponded to the addition of a contaminant at or near the connection point to a city water system. As indicated in the Table above, this could be achieved through a Siamese connection, wall hydrant or through a tap located in the vicinity of the water meter, RPZ or a pipe on the suction side of the interior pumps. This scenario could also represent the impacts of a contamination event in the city water system. Impacts of the event are greatest when the contaminant is added during the period of highest water usage. For the case of a contaminant injected from midnight to 3 a.m., there are no impacts because the pumps were not operating in this scenario. The greatest impacts occur with the 3-h injection starting at 6 a.m. because of the large amount of water used at the start of the work day.

A second potential pathway for contamination of the water system is the direct injection of a contaminant into one or both of the tanks. Since the tanks are not pressurized, a contaminant can be added by direct insertion into the tank (i.e. pouring a liquid or powder into a hatch or other entry on the top of the tank), rather than through pumping. When a contaminant enters a tank, it is diluted with the clean water that already exists in the tank. In the present example, it is assumed that the tanks are completely and instantly mixed. This is generally a reasonable assumption for a small tank with a small diameter feed line [5]. As water is consumed in the upper half of the building, the contaminated water is drawn from the roof tank and delivered to the fixtures on the effected floors. The progression of floors impacted by the contamination and the resulting concentrations are shown in Figure 3. This figure shows snapshots of the building at 1 p.m., 2 p.m., and 5 p.m. representing 1 h, 2 h, and 5 h after the start of the contamination event. As expected, no contaminated water is delivered to the lower floors served by the mid-level tank. A series of model runs were made in order to study the effect of the time that the tank is contaminated, on the resulting exposure. The same amount of contaminant was added in separate model runs at midnight, 6 a.m., noon, and 6 p.m. and the exposures calculated over the next 24 h. The results are very insensitive to the time of day when the tank is contaminated.

The final set of model runs with the high-rise model looked at the impacts associated with injection of contaminants at various fixtures within the system. In the first scenario, a low head pump is used to inject the contents of the 55-gal drum over a period of 2 h

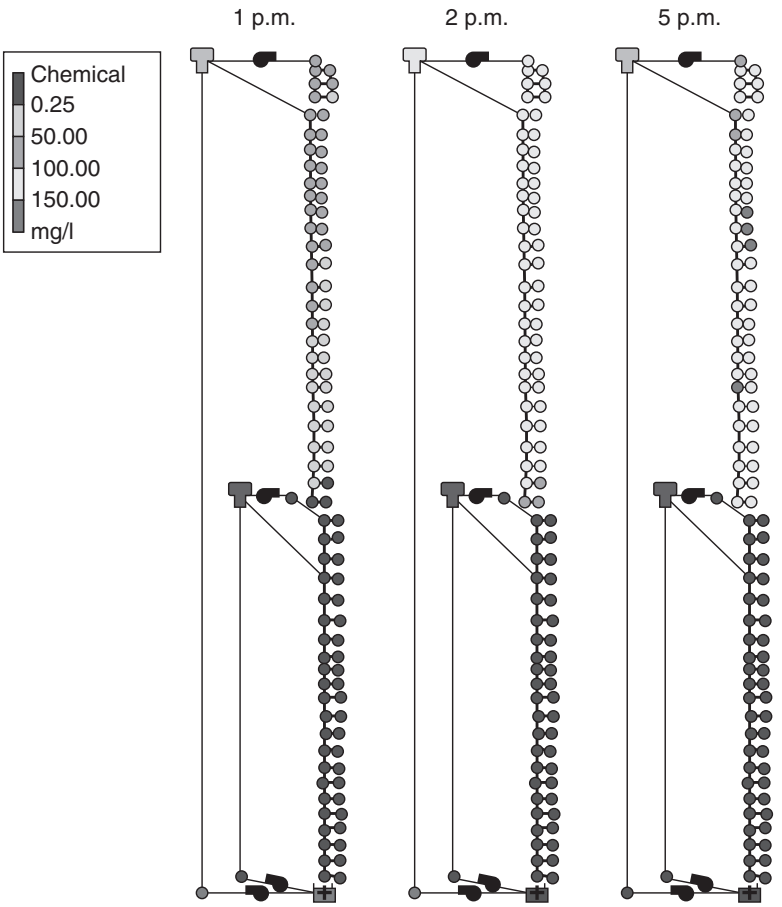



**FIGURE 3** Snapshots of building water system showing contaminant concentration.

starting at noon. The moveable tank/pump is attached to a fixture such as a utility sink on the 27th floor. The pump is capable of overcoming the pressure on the downstream side of the PRV (70 psi) but cannot overcome the pressure on the upstream side (137 psi). As shown in Figure 4, as a result, all of the contamination affects water usage on floors 25, 26, and 27 served by the PRV on floor 27. In the next scenario, a higher head pump is used that is capable of overcoming the pressure on the upstream side of the PRV. However, as long as the demand on the downstream side of the PRV (associated with usage on floors 25, 26, and 27) exceeds the rate at which the contaminant is injected into the fixture, the contaminant will stay within the three-floor zone and not affect other floors. When the water usage on floors 25, 26, and 27 is set to zero, only then will the contaminant move through the PRV in the main riser. As shown in Figure 5, when the contaminant enters the riser, it will mix with the water that is coming from the tank and move with the flow (i.e. toward the lower floors), resulting in contaminated water feeding those floors. Viewing this issue from a building safety perspective, the above analysis suggests that the most vulnerable component of the system is fixtures on high floors (or on a floor near the top of a zone in a multizone building).

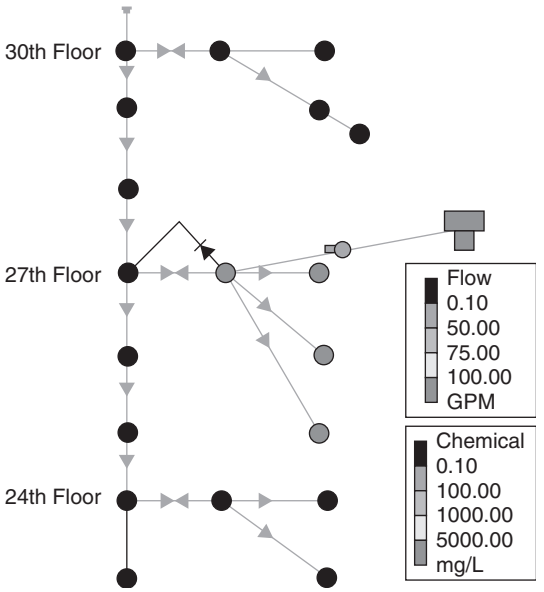



**FIGURE 4** Movement of contaminant introduced by low head pump.

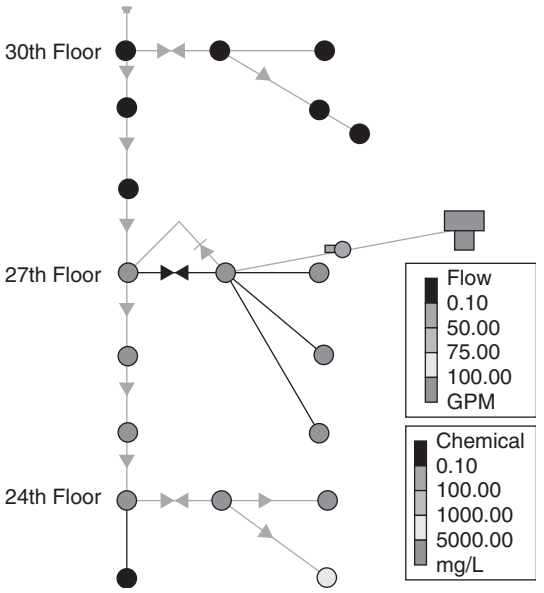



**FIGURE 5** Movement of contaminant introduced by high head pump.

## 5 CONCLUSIONS

This article provides information on the potential threat to a building's domestic and potable water supplies from chemical and biological agents that could potentially be used by terrorists. Distribution systems and piping systems within buildings are potentially susceptible to intentional contamination. In order to introduce a contaminant into a pressurized system, one must only overcome the internal pressure using an appropriate pump. Typically pressures within a system can range from a minimum of about 30 psi to 200 psi. Some components, such as most storage tanks, are not pressurized so material can be added by direct entry without a pump. The quantity of material that would need to be added to a water system in order to result in health or other impacts depends upon the specific contaminant and the flow rate in the entry pipe, or the water volume in the tank.

Based on an examination of plans for typical large venue, high rise and low rise buildings several potential points of vulnerability were identified. Typically these vulnerable points included access points near the entry point for pipes connecting to the city water system and storage tanks within the building. Access to these points could lead to contamination of the entire building or, in the case of multizone buildings, contamination of an entire vertical zone. Tanks are especially vulnerable because typically, they are not pressurized so that a contaminant could be introduced directly without the need of a pump. Although any fixture within the building could serve as a point of contamination by use of a pump capable of overcoming the system pressure, for most cases only that part of the building that is "downstream" of the entry point would be impacted, thus limiting the extent of the contamination.

Hydraulic models proved to be a useful tool for estimating the spread of the contaminant and the resulting human exposures. Several different scenarios were modeled for high-rise and low-rise buildings to demonstrate the likely consequences of various contamination schemes. Impacts depended upon the location of the entry point, duration of the event, time of day of the event, quantity of contaminant introduced into the system, and lethality of the agent. Based on the analysis of a typical high-rise building and a low-rise entertainment venue, it was found that a significant number of people could be impacted by the introduction of a contaminant into the water system.

The primary mechanisms for protecting a building from widespread contamination events are to limit access to key locations within the building. These key locations include: (i) the area in the vicinity of the connection or entry point of water from the city system into the building, (ii) internal tanks, and (iii) potential contamination points such as fixtures on high floors.

## REFERENCES

1. Powers, M. B., Post, N. M., and Roe, A. G. (2002). *Building for a Secure Future: Bioterrorism, Chemical, Biological Threats Pose New Design Challenges, Engineering News-Record*, http://enr.construction.com/features/buildings/archives/020325f.asp.
2. Dreazen, Y. J. (2001). Water utility officials fear 'Backflow' from terrorists. *Wall Street J.* December 27, A14. Available at: http://cryptome.org/backflow-panic.htm.
3. Lory, E., Cannon, S., Hock, V., Van Blaricum, V., and Cooper, S. (2005). *Potable Water CBR Contamination and Countermeasures*, Naval Facilities Engineering Service Center and U. S. Army ERDC. http://www.natick.army.mil/soldier/jocotas/ColPro_Papers/Lory.pdf.

4. Grayman, W. M. (2006). Use of distribution system water quality models in support of water security. In *Security of Water Supply Systems: From Source to Tap*, J. Pollert and B. Dedus, Eds. Springer Press, Netherlands.
5. Grayman, W., Rossman, L., Deininger, R., Smith, C., Arnold, C., and Smith, J. (2004). Mixing and aging of water in distribution system storage facilities. *J. AWWA.* **96**(9), 70–80.

## FURTHER READING

Allman, T. P. and Carlson, K. H. (2005). Modeling intentional distribution system contamination and detection. *J. Am. Water Works Assoc.* **97**(1), 58–61.

Clark, R. A. and Deininger, R. (2001). Minimizing the vulnerability of water supplies to natural and terrorist threats, *AWWA IMTech Conference Proceedings*, Baltimore, MD, p. 10.

Clark, R. M. and Rolf, A. (2000). Deininger protecting the Nation's critical infrastructure: the vulnerability of U.S. water supply system. *J. Contingencies Crisis Manage.* **8**(2), 73–80.

Foran, J. A. and Brosnan, T. M. (2000). Early warning systems for hazardous biological agents in potable water. *Environ. Health Perspect.* **108**(10), 993–995. http://www.ehponline.org/realfiles/docs/2000/108p993-995foran/foran-full.html.

Hickman, D. C. (1999). *A Chemical and Biological Warfare Threat: USAF Water Systems at Risk, Counter Proliferation Paper No. 3*, Future Warfare Series no. 3, Air War College, Maxwell Air Force Base, Alabama.

Hock, V. F. (2005). *Current Research in Fate &Transport of Chemical and Biological Contaminants in Water Distribution Systems, Session 2C, Modeling, Ecological Restoration / Systems Assessment, USA-ERDC-CERL*, www.dtic.mil/ndia/2005triservice/track2/hock.pdf.

Purver, R. (1995). *Chemical and Biological Terrorism: The Threat According to the Open Literature*, The Canadian Security Intelligence Service.

# COMMUNICATIONS AND INFORMATION INFRASTRUCTURE

# CRITICAL INFRASTRUCTURE PROTECTION: TELECOMMUNICATION

TED G. LEWIS

*Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, California*

## 1 INTRODUCTION

The telecommunications sector is a complex adaptive system exhibiting *self-organized criticality* (SOC) suggesting its vulnerability to systemic failure. Over its 100-year history, the architecture of the telecommunications sector in the United States has evolved into a scale-free network with critical nodes located in a small number of major *telecom hotels*, that is, buildings containing a high concentration of switching equipment, storage, and interdependent connections. These *hubs* were formed by economic, regulatory, and technical forces operating over four historical periods: an *unregulated beginning*, the *telecom war* years, the *regulated vertical monopoly* period, and the current deregulated *competitive era*. This article briefly traces the evolution of telecommunications in general and telephony in particular. Using network science theory, we show that hubs and *betweener* nodes are the most critical components in the national system. Furthermore, these critical nodes are the direct result of regulatory forces shaping the industry, which have had major impact on telecommunications. Because of economic, regulatory, and technical forces ever-present in the industry, the telecom sector has evolved into a state of SOC. Although the industry has not experienced a calamity on a scale similar to the 2003 Eastern Power Grid Blackout, I believe that the two networks have evolved to a similar state.

## 2 OVERVIEW

Telecommunications infrastructure became the first *critical infrastructure sector* in the United States following the Cuban Missile Crisis of 1962. The confrontation between President Kennedy and Premier Khrushchev of the former Soviet Union, eventually led to the NCS (National Communications System) and the formation of the NSTAC—*National Security Telecommunications Advisory Committee*—created

by President Reagan (EO12382–1982) to advise the President of the United States on matters pertaining to the security and well-being of telecommunications. The first critical infrastructure sector was renamed the *Communications Sector* by the Department of Homeland Security in 2009 [1]. Regardless of its name, telecommunications security has always been on the forefront of homeland security even before the creation of the US Department of Homeland Security in 2003.

The communications sector, like many other fundamental infrastructure sectors, has a long and rich history of evolutionary change. Generally speaking, power, energy, telecommunications, and other interstate commerce sectors such as transportation have emerged as *complex adaptive systems*, becoming very large, complex, and malleable networks with both strengths and weaknesses. These strengths and weaknesses are a by-product of technical, economic, social, and regulatory policies of the United States, which have shaped these industries for over 100 years. Generally, it is believed that these forces are responsible for the current state of SOC for this sector.

This article develops a framework for understanding this complex adaptive system. Note that it is a *system*, which is more than merely a collection of components. Network modeling is a natural way to simplify and understand the rudiments of complex systems, and in particular the *architecture* of such systems. A network represents a system as a collection of *nodes* connected by *links*. For example, a social network is a collection of people, represented by nodes, and their associations, represented by links. A telecommunications network may be modeled at several levels: the physical level model uses nodes to represent switches and links to represent wires. A telecommunications network model might also equate nodes with buildings containing thousands of switches, and links with thousands of fiber optical cables. Networks are abstract mathematical objects that serve only to represent what is of most interest to the study of a system.

Determination of *individual* asset security has very little payoff for homeland security. For one thing, it is too expensive to protect every asset, and for another thing, it is not necessary. Knowing that a transformer in a power grid or a telephone pole in a telecommunication system is vulnerable to a terrorist attack or natural disaster such as a hurricane, tells us very little about the vulnerability of the larger system. Because of the complexity, interdependencies, and varying criticalities of large and complex systems that span the entire nation—or major portions of it—we must understand the system's architecture. Network models allow us to study large and complex system architectures as *evolving systems* so we can understand *system vulnerabilities* and derive strategies to deal with them. The immediate objective, then, is to protect the entire telecommunications infrastructure by judicious selection of critical components. A longer term, more ambitious objective is to suggest measures that cause wholesale restructuring of the telecommunications sector such that it is intrinsically more secure.

## 3 EVOLUTIONARY FORCES THAT SHAPE THE SECTOR

In some sense the communications sector has come full circle: from digital to analog, and then back to digital. Its creators envisioned a system somewhat like today's Internet, that is, a global broadcast network that connected everyone to everyone else. But their vision was limited by available technology going back over 200 years ago. Samuel Morse (1791–1872) perfected the first commercially successful digital system called the *Telegraph*, and demonstrated it in 1844 by transmitting *Morse Code* (dots and dashes are

equivalent to the binary 1s and 0s of today) from Washington D.C. to Baltimore. Western Union transmitted digital messages much like today's e-mail from coast to coast in 1861. Thus was born the first electronic communication network for transmitting disembodied messages between a pair of humans. Technology was the limiting factor, but profitability would soon motivate rapid advances in technology, obsolescing digital telephony almost immediately.

Western Union enjoyed a brief monopoly of the electronic communication business until 1876 when Alexander Graham Bell (1847–1922) successfully transmitted his voice over an analog channel to Mr. Watson, his assistant. Bell filed his "telephone patent" only a few hours ahead of Elisha Gray (1835–1901) of Western Electric. (Western Electric made the telephones and switching equipment for exchanges.) He founded the *Bell Telephone Company* and quickly built the first telephone exchange network in Hartford, Connecticut in 1877. Bell later purchased Western Electric from Elisha Gray in 1882, and proceeded to create one of the largest of many *vertical monopolies* of the twentieth century. Bell Telephone linked two cities (New York and Boston) together in 1883, but it would take the company nearly another 60 years to subscribe 50% of the population. The first mobile telephone did not appear until 1946! Compare this to the rate of adoption of the video tape recorder in the 1980s (12 years to reach 50%), and the rapid adoption of most new technologies today, such as the iPod, Internet e-mail, and cellular handsets.

Historically and politically, it is important to note that the first cellular telephone network (1979) was built in Japan rather than the United States. Through most of the twentieth century, communications in the United States consisted mainly of the *public switched telephone network* (PSTN) owned and operated by AT&T. This slow pace of technology innovation by a vertical monopoly led to radical changes in the industry, primarily to stimulate innovation and rapid adoption of new technologies. Slow adoption of new technology would become one of the factors leading to deregulation of the communications industry in 1996.

Patent litigation in 1879 separated voice and data: Justice allowed Bell Telephone to operate voice networks and Western Union to operate data networks (basically stock market quotes). This artificial separation between voice and data would become a barrier to advancement of telephony until invention of the Internet in 1969, and its commercialization in 1998. Even today, the *network neutrality* movement is about content, that is, whether voices, dates, pictures, etc. should be priced separately or not. The network neutrality advocates rightly claim that all information is digital, so how can telephone and telecommunications companies charge separate rates for different encodings of ones and zeros? So far, the network neutrality advocates have won, and this has not become a force shaping the sector.

### 3.1 Unregulated Beginnings

Table 1 lists major events in the evolution and shaping of the telecommunications sector. This timeline has four distinct periods: *Unregulated*, *Telecom War*, *Regulated*, and *Deregulated*. From 1877 to 1898, the industry was mainly unregulated. During this period, a large number of local companies emerged to serve local customers. This produced a large number of isolated and heavily connected networks characterized by dense wiring clustered around a small number of central switching offices. Even after consolidation set in, the resulting networks were clustered and highly focused on local calls. (Highly

**TABLE 1 Major Events in the Evolution of Telecommunications Regulation**

| |
|---|
| 1837–1873 Telegraphy was first digital communication system |
| 1866 Western Union becomes first telecom monopoly |
| 1876 Bell demonstrates first operating telephone |
| 1878 5600 telephones in use |
| 1882 109,000 telephones in use |
| 1885 AT&T incorporated for long-distance service |
| 1894 Bell's patents expire |
| 1898 Telecom War begins . . . through 1934. |
| 1899 AT&T reorganized as an IP holding company |
| 1903 Telephone industry dominated by independents |
| 1907 AT&T reorganized and controlled by J. P. Morgan |
| 1911 AT&T vertically integrated: Western Electric, Long Lines |
| 1913 US DOJ sues AT&T claiming violation of Sherman Antitrust Act. |
| 1924 AT&T owns 223 of 234 independents! |
| 1934 Telecommunications Act of 1934 |
| 1934–1974 Vertical Monopoly Period |
| 1974–1984 DOJ suit leads to breakup of AT&T |
| 1996 Telecommunications Act of 1996 |
| 1996 LECs win court battle establishing states right to set retail prices |

clustered networks are more resilient and less vulnerable to failures and attacks than today's national-scale communication networks).

### 3.2 The Telecom War

A "telecom war" broke out among competitors after Bell's patents expired, prompting the U.S. Department of Justice to step in and enforce the Sherman Antitrust Act of 1890. While the case against AT&T was very similar to the Sherman Antitrust Act case against Microsoft, the action against AT&T was much more severe. The government forced AT&T to stop buying independent telephone companies without their permission; it required AT&T to interoperate with its competitors [the local exchange carriers (LECs), in today's language]; and required AT&T to divest its control of the Western Electric Manufacturing Company whereas Microsoft was merely fined and allowed to remain intact after being found guilty of violating the 1890 Act.

While the action against AT&T may have seemed severe, AT&T owned 223 of the 224 independent companies within a decade of the 1913 ruling! This illustrates one of the primary factors affecting and shaping many infrastructure systems: *increasing returns*. Increasing returns in economics says the more a certain commodity exists, the more valuable it becomes. In this case, increasing returns drove AT&T toward a monopoly: the more customers connected by the AT&T network, the more valuable the network became. The more valuable it became, the more customers wanted to subscribe. This spiral ended up with AT&T in the monopoly catbird seat.

Increasing returns accelerates the adoption of one technology and service over another, because it standardizes the user interface, exhibits the compounding network effect of being able to communicate with more people over a large network versus a small network, and motivates the owner operator to amortize fixed costs over an ever larger customer base.

In network terms, increasing returns is a kind of *preferential attachment* effect. It works like this: as customers randomly select one of many vendors to provide telephone service, they eventually realize that more people are subscribing to one service than another. The benefits of the "more popular" service may be intangible, but if only a few customers decide to switch to the more popular service, this begins a process of preferential attachment. Think of the vendor (competitor) as a node in a network, and the links as subscriptions. The more heavily connected node is preferred over the less connected nodes, which accelerates adoption of the heavily connected node. As more consumers subscribe to the preferred vendor node, more decide to also subscribe, which snowballs into an avalanche of connections. Thus, the popular node becomes a major hub of the network.

Fundamental infrastructure systems such as electric power, water and sewer, and telecommunications systems all exhibit the network effect known as preferential attachment. In the end, the preferred node becomes a monopoly, as Microsoft did in the 1990s. Emergence of a monopoly has little to do with the performance of a certain company or leader, but instead it is a fundamental property of fundamental infrastructure systems. Increasing returns sets in, and the infrastructure becomes the *only* player in the field, that is, a monopoly.

Although the theory of preferential attachment, increasing returns, and network effects were not well-understood in the 1930s, the results were clear: as a consequence of monopolies like AT&T, most customers were happy with their service, but not all. In particular, people living in rural or thinly populated areas were without service. The network effect was inaccessible to them because it was not cost-effective for the owner or operator of the telephone company to serve an isolated customer.

The Congress, in its wisdom, bartered *universal access* for *natural monopoly* of the major means of long-distance communication when it passed the 1934 Telecommunications Act. Universal access means that everyone gains access at a (somewhat) flat fee, regardless of his or her geographical location. Instead of nationalizing AT&T, the Congress provided monopolistic protections for the private enterprise in exchange for universal access. AT&T was required to amortize connection charges across all customers. But this privilege came at a price because innovation would slow to a halt without the incentives provided by competition.

### 3.3 Regulatory Period

The 1934 Telecommunications Act initiated the *regulatory period* of evolution. It provided for the regulation of telecom through the FCC (Federal Communications Commission), which answers only to the Congress. It declared the electromagnetic spectrum within the United States as public property and only the Congress had the right to regulate its use. A license and huge licensing fee was imposed on commercial broadcasts. Finally, the Congress required broadcasters to operate in the best interest of the public.

The 1934 Act had a huge impact on shaping the communications network of the United States. For example, the so-called "long lines" established by AT&T during this period remains a major component of the communications infrastructure today. The protocols and standards of operation established by AT&T remain as legacy systems. Specifically, the SS (switching system) computers designed and built by AT&T/Bell Labs established a global standard for how telecommunications systems operate. (They are legacy systems in the sense that the old analog protocols no longer work with the new digital protocols

of the Internet, and in some cases, the digital protocols have to be made to interoperate with newer digital protocols).

Because AT&T was a closely regulated vertical monopoly, the system operated seamlessly from end-to-end. Equipment interoperated, networks interfaced with one another, and universal access guaranteed safe and secure operation. In many ways the old AT&T system was more resilient and rugged than the cobbled together networks of today. According to Richard Kuhn, "For several decades AT&T has expected its switches to experience not more than two hours of failure in 40 years, a failure rate of $5.7 \times 10^{-6}$." The old regulated system was extremely reliable!

### 3.4 Deregulated Oligopolies

The deregulated period began in 1974 and continues, today. It took 10 years for the US Department of Justice to break up AT&T this time. Breakup led to the "Baby Bells", or LECs which are regional telephone companies licensed to operate as monopolies within geographical areas of the United States. A total of 22 companies were granted seven operating regions, but the infrastructure remained much the same as during the regulated period. The Congress also sought to establish pricing, which was challenged by the LECs, leading to the states having the right to set prices for their citizens, in 1996. Nonetheless, pricing restrictions on both the wholesaler (LEC and, IEC or Interexchange Carrier) as well as the retailer (consumers) had a major impact on performance and reliability of the network. Why build out newer, faster, and more reliable networks when profitability is constrained by regulation?

The Baby Bells continued to be slow adopters of new technology and providers of better service. This period of telecom evolution may have persisted for some time if the Congress and the NTIA had not commercialized the Internet in 1993–1998 (National Telecommunications and Information Administration within the Department of Commerce, created in 1978 EO 12046). The commissioner of the FCC and the Congress justified its major revision of the 1934 Telecommunications Act mainly based on the concept that competition would spur innovation. One goal of the 1996 Telecommunications Act was to encourage universal Internet access for everyone's home and office. The Baby Bells, saddled with their legacy analog systems and voice-only mentality were taking too long to transition to the new digital age. This theme continues to resonate today.

The 1996 Act unbundled services, in other words, no more extra fees for extra services like digital data transmission (VoIP or voice over Internet protocol). It motivated the deployment of faster networks (xDSL), and limited ownership of Cable TV, TV, and radio stations. But most importantly, the 1996 Telecom Act established *peering* as a way of life for competitors. This has led to the number one vulnerability in the communications sector.

Peering is the practice of sharing networks with competitors. Company A may need Company B's network to provide long-distance connections for local customers. Conversely, Company B needs Company A's local connections to gain access to the "last mile" or household/office consumer. LECs typically own and operate local exchanges, while IECs ("long-haul" carriers) typically own and operate long lines (Fig. 1). In today's market both, local access to get onto the long lines and long lines to make long-distance calls, are required.

Peering radically restructured the industry, because it not only allowed, but motivated competitors to co-locate their switching equipment in close proximity to one another.

The consequences were dramatic and unanticipated: a small number (30–40) major switching hubs emerged as the preferred nodes. That is, the law of increasing returns appeared again. Only this time the result was creation of the *number one vulnerability* of the telecommunications sector: the carrier or *telecom hotel*. This phenomenon is explored later.

The telecommunications sector contains more than the wired-only network left over from the days of vertical monopolies and regulation. Even so, all communication networks depend on it. Satellite communication (with small exceptions), cellular telephony, Internet, and to a lesser degree, broadcast TV, Cable TV, and GPS navigation depend on the core capabilities of the wired network. Therefore, a potential threat to the wired network is also a potential threat to the wireless and associated networks. These systems are interdependent as shown in Figure 1.

## 4 MAJOR COMPONENTS OF THE SECTOR

A full discourse on the U.S. telecommunications system could easily fill an entire book, so the discussion here focuses on the top level. Figure 1 is a gross simplification of telecommunications in the United States. It consists of three major layers: the LECs and their customers; the long-distance interexchange carriers (IECs), and the various devices and services feeding into the points-of-presence (POP) gateways provided by the IECs. IECs operate long lines that connect cities and countries to one another.

Figure 1—reading from left to right—shows how a telephone call or e-mail transmission makes its way from one person to another. Suppose an e-mail sender is transmitting from one of the houses shown under the LEC column. The message travels to a *headend switch*, typically located in the neighborhood to serve up to 1,000 homes. The headend

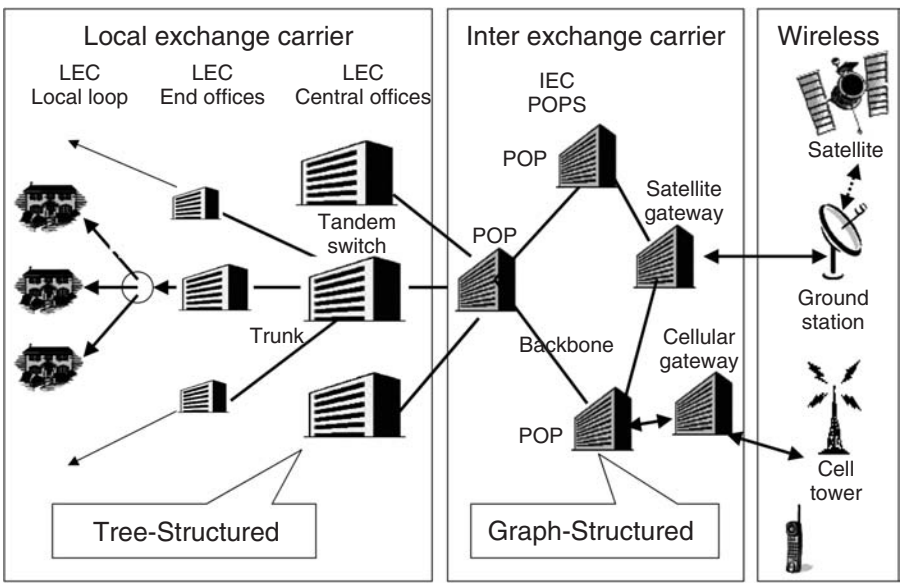



**FIGURE 1** Structure of the communications sector [2].

connects to a central office in the LEC, which forwards the message, locally or through the long-haul IEC network. If the recipient is located within the same network, the message is routed back through the tandem switches to a headend switch and then into the recipient's home. If the recipient is at a long distance, the message travels through a POP or gateway to the IEC network.

Suppose the recipient uses a cell phone from 1,200 miles away. The LEC must forward the message to a POP switch within an IEC network, as shown in the middle column of Figure 1. The IEC's gateway also acts as a bridge across networks that operate at different speeds and protocols (rules for exchanging messages). The sender's message may make its way across several IECs before finding a gateway that connects the sender with the receiver.

When the recipient answers his or her cell phone call the nearest cellular tower transmits the "connection signal" to a gateway within the wired IEC network. A roaming cell phone registers with local towers, so the IEC and LEC switches can find the cell phone regardless of where it is. Eventually, the network makes a connection between the sender and the recipient's local tower. This all happens at nearly the speed of light, so the consumer does not notice a long delay.

The most interesting feature of Figure 1 is this: to work as one integrated communications system, cellular, satellite, and other means of communication depend entirely on the *wired landlines*. The old AT&T long-haul lines (and others) are the backbone of the national system. Cellular transmission has a range of about 3 miles, so cell phones actually connect to land lines via a nearby tower. Transcontinental cell phone calls are not possible without the long lines maintained by the wired IECs. Even satellites depend on the terrestrial wired lines. Ground stations often provide feeds to television and other broadcast media, but they need a stable and reliable wired landline network to operate. These systems are interdependent and together they form a very large and complex system.

The logical structure of Figure 1 shows that the telecommunications sector is a *system*, rather than a loose collection of local components and unrelated assets. As such, this system's resiliency is dependent on its "architecture" more than the resiliency of individual components. For example, the highly redundant IEC layer has many POP and gateway switches, so that the failure of one has minor implications for the reliability of the overall system. It begs the question, however, of which components are most *critical*, where criticality means failure of a critical component can lead to failure of the *entire* system.

Security analysts often overlook system analysis of infrastructure, preferring to perform asset analysis because it is easier. Analysts tend to pay more attention to local incidents involving a single asset such as a bridge, building, or computer, because it is easy. In reality, simple components frequently fail without bringing down an entire system. It is well-known that natural disasters are distributed according to a *power law*, whereby inconsequential failures occur with high frequency and high consequence failures occur with much less frequency [3]. However, the telecommunication system is a product of human engineering and Congressional regulation and these forces that have shaped the sector have also made it more vulnerable to targeted attacks than it would be if it were a product of nature. Therefore, it is important to ask, "What is critical in critical infrastructure protection, and in particular, telecom infrastructure?" Criticality is at the core of system analysis.

The answer to this question is found by investigating the architecture of the system, which in turn leads to understanding critical components whose failure might bring down the entire system. Because we cannot afford to protect everything, we opt to protect the

most critical components. This is the strategy called *network analysis* and it borrows heavily from the network science literature [4].

## 5 RESILIENCY OF NETWORKS

To understand the criticality of telecommunication system components we need to understand the fundamentals of network theory, because the structure of large and complex networks has a major impact on their survivability under stress. Ideally we want networks to continue to operate under less-than-perfect conditions. A plausible goal is to operate any infrastructure system as a robust network that is difficult to bring down even when purposely attacked. This analysis is limited to single-node attacks.

The telecommunications network is a bidirectional network because messages flow in both directions. A failure of one switch may or may not halt bidirectional flow because of redundant or alternate paths. However, failure of a switch may reduce the overall network capacity or speed. Resilience can have several definitions: as a measure of the impact of an attack on overall structural integrity of the network, or as a measure of the decline of output from the network (in terms of number of messages per unit time). We study both: the structural integrity of the telecom network due to cascade failure which is a single node outage that ripples through the network taking down affected nodes; and the decrease of output flow from a network in which messages flow from source to sink node. *Cascade failure analysis* determines resilience of the static structure (architecture) of the network, while *flow failure analysis* determines resilience of commodity flow through a network.

More formally, cascade failure resilience is defined as the fraction of nodes that continue to operate following the failure of a single node:

$$R_c = 1 - (I_c/n);$$

where
$R_c$ = cascade resilience,
$I_c$ = "infected" or damages nodes,
$n$ = number of nodes in the network.

Flow resilience, in contrast, is defined as the fraction of commodity flowing into sink nodes after a single node is attacked, compared to beforehand:

$$R_f = F_1/F_0;$$

where
$R_f$ = flow resilience
$F_1$ = flow after an attack
$F_0$ = flow before an attack

We can express both measures as a percentage in the interval (0, 100%). Cascade resilience parameter $I_c$ is estimated by simulating an *epidemic* or a contagion that spreads from the attacked node to adjacent nodes with probability $\gamma$, the infection rate, and repaired in $\tau$ time steps following failure. Once repaired, a node stays repaired, simulating

an SIR (Susceptible-Infected-Recovered) epidemic. $I_c$ is obtained by merely counting the *total* number of nodes infected from onset to recovery of all nodes. (We could also use the peak number infected, but this is left as an exercise for the reader). Flow resilience parameters $F_1$ and $F_2$ are estimated by simulating flows emanating from a single source node to a single sink node. A single source is constructed by aggregating all nodes with zero inputs; similarly, a single sink is constructed by aggregating all nodes with zero outputs. In simulations conducted by the author, link capacities are all the same and flows out of a given node are evenly divided among the outgoing links. Flows into a node are summed; it is possible for nodes to overflow or underflow. We ignore overflows and limit the amount of message flow through a link to the link's maximum capacity. In a telecommunication network, capacity is equivalent to bandwidth.

### 5.1 Hubs, Clusters, and Betweeners

We compare resiliency of three fundamental network structures: random, clustered, and scale-free. A random network is one in which nodes are connected to one another by randomly selecting pairs of nodes and linking them. Clustered networks contain highly connected neighborhoods of nodes that are connected to other nodes in the cluster. That is, if node A is connected to nodes B and C, then connecting nodes B and C forms a triangle. A, B, and C form the simplest possible fully connected network. The cluster coefficient of a single node is the number of triangles it is a part of, relative to the maximum number possible. A metric called the *cluster coefficient* quantifies the amount of clustering in a network, by taking the average of node cluster coefficient across all nodes. Figure 2 illustrates hubs, clusters, and betweenness: Figure 2a shows an unclustered random network. Figure 2b shows a highly clustered network. The central node of Figure 2b has $k = 4$ links connecting it to 4 neighbors. Thus, there are potentially $k(k-1)/2 = 4(3)/2 = 6$ triangular networks that can be formed out of its four neighbors. The central node belongs to 4 triangular networks, so its cluster coefficient is $4/6 = 0.67$.

A scale-free network has a very definite structure: most nodes have only a few link connections, while one or two nodes have a very large number of connections. A node with five connections (and therefore five links) has a *degree* of five. A network's hub is the node with the highest degree. Figure 2c illustrates a scale-free network containing a hub with degree of five.

### 5.2 Betweenness

Figure 2d illustrates another metric that will become useful later in the discussion of networks. *Betweenness* is a measure of *intermediary power* in a network. It is simple, but laborious to calculate. Betweenness is a measure of how many paths go through a node (or link) from all other nodes. To compute it, tally the number of shortest paths passing through a node or link, from and to all other nodes, for all nodes and links. Then scale the tallies to the unit interval (0, 1) by dividing them by the largest tally. The normalized number is the node or link *betweenness*. Figure 2d shows three of the nine paths passing through node 3, from and to all other nodes. Node 3 is a kind of gatekeeper because it indirectly connects other nodes to each other.

A network's *betweener* is the node or link with the highest betweenness value. In a sense, the betweener is a critical traffic node, because more messages can pass through the betweener node or link than any other node or link. This measure is useful in modeling

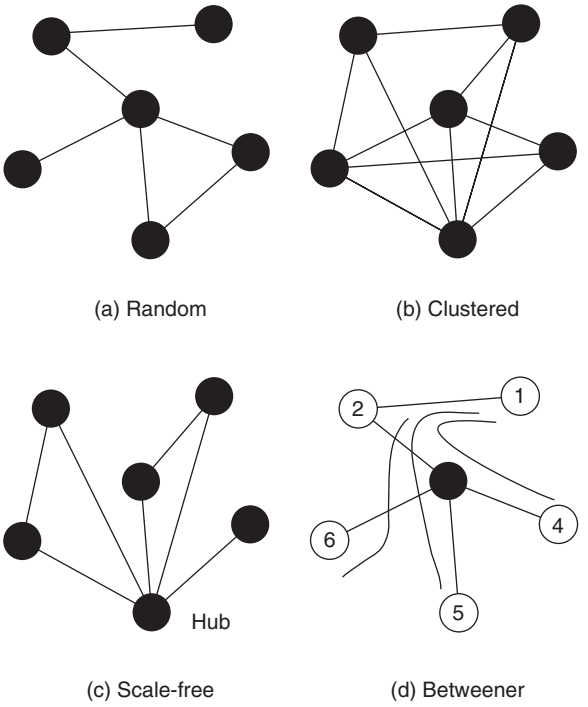



**FIGURE 2** Illustration of network topologies and the betweenness metric.

network flows, because the betweener can control the majority of flow through a network. Therefore, betweenness is an important metric for measuring resilience in flow networks such as a pipeline, transmission, or traffic networks. We want to simulate the impact of taking out the betweener on the flow resiliency of a telecom network.

## 6 RESILIENCE RESULTS

Now we turn to the subject of resiliency of a network. What constitutes "failure" in a network? If a single node or link fails, does it mean the entire network fails? If a "critical node or link" fails, does this equate to network failure? The 2003 Blackout of the Eastern Power Grid, triggered by a single link failure, propagated across the entire network disabling a large portion of it. The 2003 *cascade failure* acted much like an epidemic sweeping through a population. Therefore, experience tells us that epidemics are one form of failure that can bring down an entire network. Are telecommunication networks subject to epidemics? Yes. The spread of computer viruses and worms behaves very much like the spread of a virus in human populations. On a physical level, outage of one node affects adjacent nodes, because continuity depends on predecessor and successor nodes.

### 6.1 Cascade Resiliency

Network epidemics or *network storms* are observed in many infrastructures such as traffic jams, floods, power outages, communication outages, and e-mail congestion. In social

network theory, well-known contagions such as the H1N1 flu spread through human contact (links), and either persist (never go away) or die out. Similarly, an important question for homeland security is, "Do infrastructure epidemics live forever or eventually die out, once initiated within a network?"

Simulation of attacks on random, cluster, and scale-free networks shows how vulnerable networks are to targeted attacks. We generated networks with 50 nodes and 100 links, and randomly connected node-pairs to obtain a random network. Similarly, we generated cluster networks from random networks by repeatedly rewiring links such that the cluster coefficient of the entire network increased. This emergent process terminated when the overall network cluster coefficient reached 50% [4]. Finally, starting with a random network, we repeatedly rewired links chosen at random, but linked by preferential attachment to a randomly chosen node, until the largest node has degree at least four times the average. This produces a scale-free network with a degree sequence distribution that obeys a *power law*.

In each case, an attack on a single node initiates an epidemic which spreads to its neighbors with an infection rate of $\gamma = 25\%$. Infected nodes are repaired in $\tau = 5$ time steps, and once repaired, remain immune to subsequent infection. This simulates a susceptible-infected-susceptible (SIS) epidemic, producing epidemics that follow a very simple Kermack-McKendrick model [5] of logistic growth of the infection followed by a rapid decline as nodes mend and return to an operative state. As it turns out, the number of nodes infected over the life of the SIS epidemic is a measure of resiliency. Moreover, this number is different for random, clustered, and scale-free networks.

Figure 3 summarizes the results. Attacks on hubs are the most consequential (89% of the nodes are "infected"), while attacks on high cluster coefficient nodes are the least consequential (minimum of 17% for cluster attacks, and only 23% for hub attacks on cluster networks!). Clearly, attack strategy and network topology both bear on resiliency. Cluster networks are more resilient than scale-free or random networks!

A number of investigators have shown that scale-free networks are more tolerant of random attacks, but highly vulnerable to targeted attacks on the network's hub [6]. This

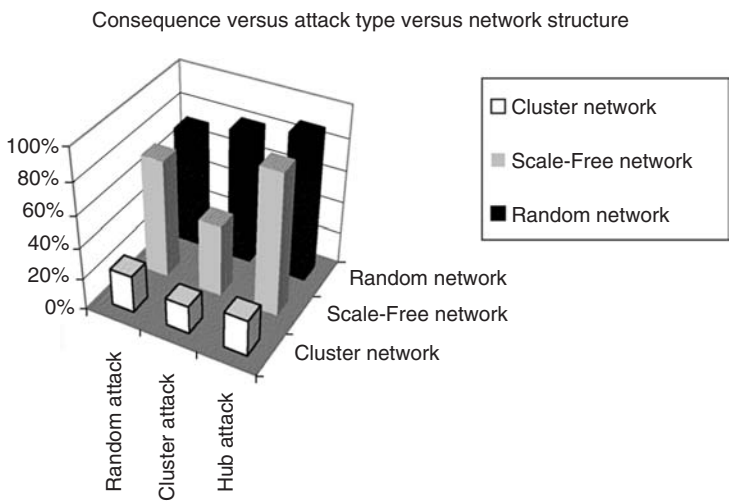



**FIGURE 3** Cascade failure in random, cluster, and scale-Free networks.

makes sense, because hub removal also removes the maximum number of links. It has also been shown that scale-free networks are more likely to sustain persistent epidemics, which is an important result for the telecommunication sector because computer viruses spread like epidemics. In fact, Wang and others confirmed this finding in an elegant and convincing network model that relates topology to persistence [7]. The Wang et al. model says network connectivity, as defined by the *spectral radius* of the network, relates to persistence as follows: $\rho\gamma - \Delta ?0$. If this relation exceeds zero, the contagion persists forever! Otherwise, it eventually dies out. Here $\rho$ is spectral radius, $\gamma$ is infection rate, and $\Delta$ is repair rate. The higher $\rho$, the more likely the epidemic never disappears from the network. And, scale-free networks have higher $\rho$ than equivalent random and cluster networks.

The opposite is true for cluster networks: they are tolerant of random and targeted attacks (because they have no hubs), and they are less likely to sustain recurring epidemics. Telecommunication networks are never clustered; rather they tend to be scale-free, so they are more susceptible to persistent epidemics. Figure 3 suggests that clustering improves resiliency against cascade failures by a factor of 3–4 over targeted attacks on scale-free networks.

Cluster networks are tolerant of both random and targeted attacks because they have more link redundancy than either scale-free or random networks. Interestingly, the Western US Electric Power Grid is a high cluster coefficient network, which means it should be more resilient than the Eastern power grid. According to Kendall [8], the reverse is true: Western grid outages exceeded Eastern and ERCOT outages during the period 1993–1999. This unexpected result is perhaps due to SOC, a topic that is described in more detail below.

Hubs attacks are more consequential than any other kind of attacks. The lesson is clear: protect the most critical nodes and links as defined by degree. An economical strategy with maximal return is to protect hubs and perhaps a few other high-degreed nodes within the telecom sector.

### 6.2 Flow Resiliency

Another form of "failure" in networks has to do with networks that supply some sort of commodity. A supply chain network such as a gas and oil pipeline network, water supply system, or airplane supply chain provide a commodity that flows from source to sink. It is important for sink nodes to keep up with demand, and to do so, flow must be continuous and not interrupted by a failure of a node or link along the way. In a telecommunication network, the commodity is voice, data, e-mail, etc.

Another kind of failure is *denial of service* due to reduction or termination of flow of messages through a network. An arbitrary network likely has many alternative paths from source to sink, along which a commodity can flow. Removal of a single node or link may or may not have much impact. This begs the question, "Does network structure matter to networks that supply a commodity such as e-mail messages or voice streams?" If we treat the telecommunications sector as a flow network, where e-mail, voice mail, and other digital information such as photographs flow from sender to receiver, what constitutes a threat to continuity of flow?

Simulation of attacks on directional random, cluster, and scale-free networks with a single source and single destination node produces much the same results as shown in Figure 3, except the consequences are measured in terms of flow resiliency, $R_f = F_1/F_0$.

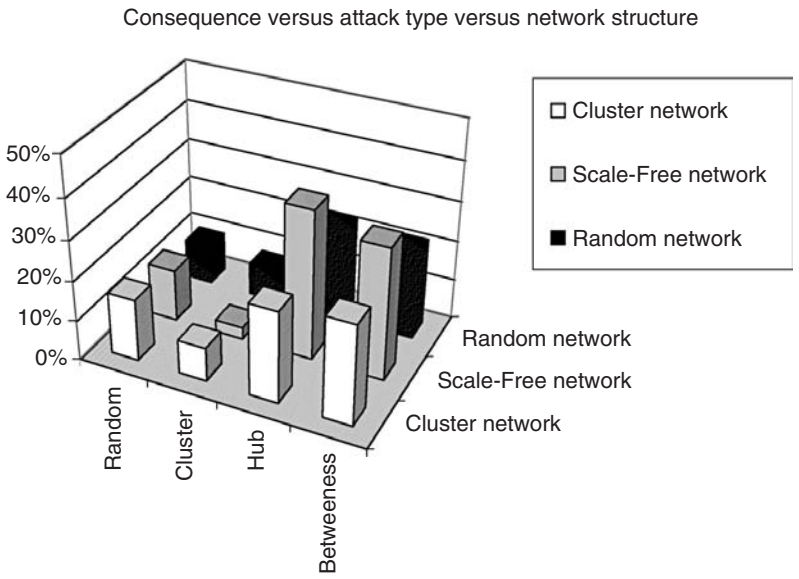



**FIGURE 4** Simulation results for flow networks.

Given an input of say 100 units, and demand of 100 units, what fraction actually reaches the destination node? If a node failure reduces output from 100 to 70 units, then $R_f = 70/100 = 0.7 = 70\%$.

Simulation results confirm that hubs are more critical than all other nodes except for high betweenness nodes (Fig. 4). Random and cluster networks are more resilient, but still suffer relatively high consequences when their hubs and betweeners are attacked. Scale-free networks suffer even more consequences because their hubs are larger. In many cases, the hub is also the betweener. This is why consequences are similar. Betweenness is a measure of the number of paths running through a node. Therefore, telecommunication networks are more vulnerable to hub and betweener attack than random or cluster attacks.

## 7 TELECOMMUNICATIONS CRITICALITY

Has the telecommunications sector reached a state of resilience, or the opposite? After 100 years of evolution, do we have a more or less secure and resilient communication network? This author claims that the sector has become *less resilient* and therefore, more likely to fail than ever before. The argument for loss of resiliency is based on two main observations: (i) after one hundred years of economic, regulatory, and technical pressure to be efficient, profitable, and politically acceptable to the Congress, the system has evolved into a weakened state, culminating with the 1996 Telecommunications Act; (ii) like many massively large and complex infrastructure networks with a long history of evolution, the telecom industry has reached a state of SOC. This claim is supported by the existence of critical nodes in the scale-free shaped sector. These two ideas are partners: evolution from randomness to a state of SOC, resulting in a network with hubs and betweeners.

### 7.1 The Hubs: Telecom Hotels

NSTAC identified *telecom hotels* as the number one vulnerability in the communications sector in 2003 [9] and recommended their protection as the top priority of homeland security. The report defines a telecom hotel:

"*Telecom Hotel*: Conditioned floor space owned and operated by a commercial Landlord for the purpose of hosting multiple service providers. Tenants may include the incumbent ILEC, competitive local exchange carriers (CLEC), Internet service providers (ISP), competitive access providers (CAP), Web hosting operations, or any other non-telecommunications commercial enterprises in need of floor space to support their electronic equipment" [9].

For example, *One Wilshire Boulevard*, a 30-story, 656,000 square foot building in downtown Los Angeles, is the single-most important point of connectivity in the Western United States. It houses over 240 telecommunications companies, provides up to 75 watts of power per square foot, and connects the United States with most of Asia. Backup power of 8 megawatts and 11,000 gallons of diesel provide resilience in case of power outages.

Details of telecom hotels are openly advertised over the Web along with security and resiliency provisions ( www.carrierhotels.com). Thus they are not only critical, but in the open. Their vulnerability, however, is perhaps low, because their importance to the entire sector is widely known, leading to exceptional security measures. Nonetheless, the high concentration of LEC and IEC switching equipment in one location raises concern. The first line of the NSTAC report says, "The Administration has expressed concern that the concentration of multiple entities' telecommunications assets in specific locations may have implications for the security and reliability of the telecommunications infrastructure" [9].

### 7.2 Self-Organized Criticality

The mere existence of telecom hotels is no accident. In fact, these highly concentrated assets are a direct consequence of evolutionary forces described above, leading up to and including the 1996 Telecommunications Act, which created telecom hotels in its wake. Specifically, the 1996 Act promotes peering and allows for sharing of facilities among competitors. Technically, it is better to peer with one's competitors by co-locating switches and routers in the same building, because it reduces time delays in transmission. Economically, the costs of housing, powering, and servicing an aggregated collection of equipment is lower, because they can be amortized over many companies. Politically, the Congress sought to increase innovation by encouraging collaboration between competitors. These forces set into motion the famous *preferential attachment*, leading to highly connected nodes housed under one roof. Telecom hotels are the most connected hubs of the communications sector.

Regulation leads to increasing returns, which leads to hubs, which in turn leads to SOC. SOC is a property of a complex adaptive system that operates near or at its *tipping point* [10]. Originally studied by Turcotte and colleagues [11, 12], definitions of SOC vary across fields of study. More formally, SOC is a property of a system that operates at or near a critical point dividing chaos and stability. Consequently, a slight change in system state tips the system in either direction, from stability into instability or the reverse.

Asset concentration in the telecommunications sector has been building for over 100 years. Initially, telephone companies were local and isolated. The telecom wars produced consolidation under AT&T. The breakup of AT&T into Baby Bells had little

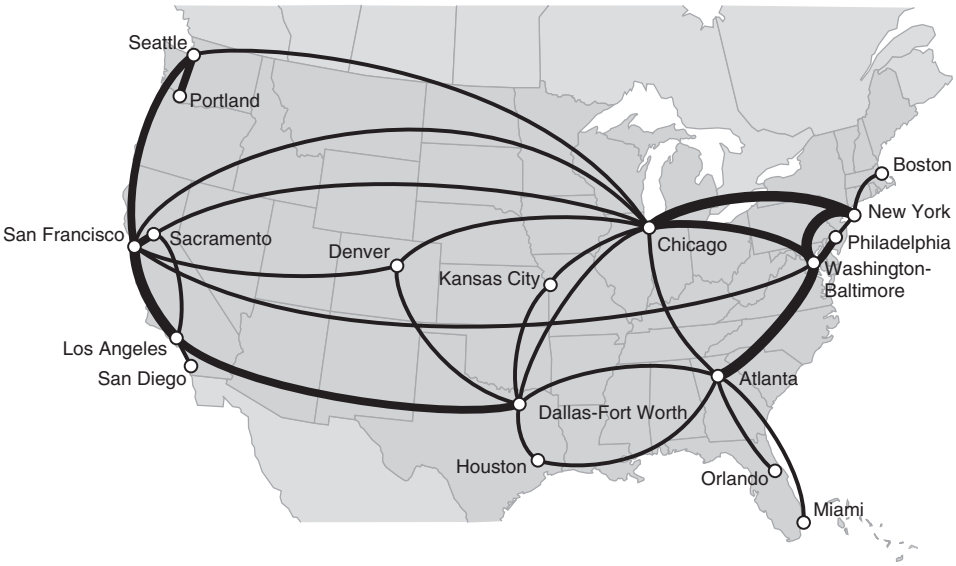



**FIGURE 5** Network of the top 30 telecom routes. [2002 Telegeography Research, www.telegeography.com].

effect on the communications network, because the separate companies used the same telephone lines and switches. During this period of asset consolidation the communication sector was perhaps a cluster network, rather resilient against hub and betweener attacks. Then the 1996 Telecom Act accelerated increasing returns; leading to fewer than 20 major hubs among the top 30 routes (Fig.5). Note that Chicago is both the hub and the betweener of this network.

A similar analysis (not shown here) confirms this theory for the top dozen AS-level Internet service providers, the *Tier-1 ISP network*. These major hubs handle e-mail, web, and voice-over-IP traffic and inevitably process everyone's Internet transactions. Their Autonomous System number identifies them, such as AS#1234. The large ISP located in Reston, VA. (AS#1239) is both betweener and hub of the top-level peers. Montreal (AS#6453) and Broomfield, CO (AS#3356) rank second. No one has studied in detail the system-wide consequences of a targeted attack on these ASs, so it is unknown how vulnerable the Internet is to removal of these critical nodes.

For a variety of reasons, the national telecommunications sector is optimized for high performance and low cost. Peering and the 1996 Telecom Act have moved the sector closer to its SOC, as evidenced by a few heavily connected hubs, highly concentrated in a handful of large telecom hotels, connected by thousands of links. As a result, vulnerability to cascade and perhaps flow attacks has increased since deregulation. Removal of a small proportion of highly connected nodes could result in major telecommunication outages.

While the conclusion drawn here has not been verified in practice, because we have no historical precedent for such a calamity, a similar SOC state exists for the electric power grid [13]. Dobson et al. extensively analyzed electrical power grids from around the world and made a strong case for SOC. Historical data supports Dobson's results, but such data is lacking in the telecommunications sector. Clearly, the power grid is different from

the telecommunications network, but it suffers from similar regulatory forces. Without similar analysis, SOC of the communications infrastructure remains speculative.

## 8 FINAL ANALYSIS

The telecommunications sector is an example of a scale-free network containing hubs (telecom hotels). This topography is a direct result of economic, regulatory, and technical forces that have shaped the sector over a period of 100 years. Perhaps the most dramatic step toward SOC occurred after the 1996 Telecommunications Act, which created the telecom hotels. Whether or not these will turn out to be the Achilles Heel of the sector remains to be seen. Currently, there is no historical data to support the conjecture that telecom hotel failure will lead to a telecommunications Pearl Harbor.

The components of the telecommunications sector in need of protection are the telecom hotels, major POP, network access points (NAP), and root servers. This adds up to perhaps 100–200 sites at the high end, and as few as 26 sites at the lower end. While the 13 root servers of the Internet have gone into hiding, there are 26 widely known NAP servers around the world that are critical to the security of the Internet. A full simulation of the effects of a cascade failure caused by a virus or physical attack on one of these critical nodes has yet to be carried out. This remains an open research question.

On a longer time scale, the telecommunications sector may evolve even closer to its SOC, unless policies are changed. Congressional regulation and economic forces have shaped the sector, so they can also be employed to reshape it. If Congress were to enact legislation that resulted in the dissipation of telecom hotels, increased redundancy, fewer betweeners, and perhaps increased path redundancy, the sector would remove its tipping point. Under this scenario, the network architecture would revert to a clustered or random network. In other words, an alternative strategy is to restructure the network instead of hardening critical nodes.

## REFERENCES

1. The National Infrastructure Protection Plan, Department of Homeland Security. (2006). www.dhs.gov.
2. Lewis, T. G. (2006). *Critical Infrastructure Protection: Defending a Networked Nation*. John Wiley & Sons, Hoboken, NJ, p. 500.
3. Malamud, B. D., and Turcotte, D. L. (2006). The applicability of power-law frequency statistics to floods. *J. Hydrol.* **322**, 168–180. www.elesevier.com/jhydrol.
4. Lewis, T. G. (2009). *Network Science: Theory and Applications*. John Wiley & Sons, Hoboken, NJ, p. 450.
5. Kermack, W. O., and McKendrick, A. G. (1927). A contribution to the mathematical theory of epidemics. *Proc. R. Soc. London, Ser. A* **115**, 700–721.
6. Albert, R., Jeong, H., and Barabasi, A. (2000). The Internet's Achilles' heel: error and attack tolerance of complex networks. *Nature* **406**, 378–382.
7. Wang, Z., Chakrabarti, D., Wang, C., and Faloutsos, C. (2003). Epidemic spreading in real networks: an eigenvalue viewpoint. *Proceedings of 22nd International Symposium on Reliable Distributed Systems, ISBN 1060-9857.*
8. Kendall, G. (2001). Power outages during market deregulation. *IEEE Control Syst. Mag.*, **21**, 33–39.

9. *NSTAC Task Force on Concentration of Assets: Telecom Hotels, February 12, 2003, National Security Telecommunications Advisory Committee*, www.ncs.gov/nstac/reports/2003/Telecom%20Hotels.pdf.
10. Gladwell, M. (2002). *The Tipping Point*. Little, Brown and Company, New York, p. 301.
11. Turcotte, D. L., Smalley, R. F., and Solla, S. A. (1985). Collapse of loaded fractal "Trees". *Nature* **313**, 6004.
12. Turcotte, D. L. (1999). Self-organized criticality. *Rep. Prog. Phys.* **62**, 1377–1429. DOI: 10.1088/0034-4885/62/10/201.
13. Dobson, I., Carreras, B. A., Lynch, V. E., and Newman, D. E. (2007). *Complex Systems Analysis of Series of Blackouts: Cascading Failure, Critical Points, and Self-organization*, Madison, Wisconsin, Vol. 17(2). CHAOS, p. 15.

## FURTHER READING

Barabasi, A.-L. (2003). Scale-free networks. *Sci. Am.* **288**(5), 60–69.

Kuhn, D. R. (1997). Sources of failure in the public switched telephone network. *IEEE Comput.* **30**(4), 31–36.

# STRATEGIES FOR PROTECTING THE TELECOMMUNICATIONS SECTOR

JOHN SULLIVANT

*$S^3E$–Sisters Three Entrepreneurs Security Consultants Company, West Hollywood, California and Magallanes Associates International (MAI), Thousand Oaks, California*

## 1 INTRODUCTION

To provide for the economic and national security of America, it is essential that we establish and maintain a telecommunications capability adequate to satisfy the needs of the nation during and after any national emergency. We now live in a world that is increasingly more dependent on information and the technology that allows us to communicate and do business globally, at the speed of light. Information has always been time-dependent but is more so today than ever. The composition of the telecommunications sector evolves continuously due to technology advances, business and competitive pressures, and changes in the marketplace and regulatory environment. Despite its dynamic nature, the sector has consistently provided robust and reliable communications and processes to meet the needs of businesses and governments [1].

## 2 BACKGROUND

### 2.1 A Historical Perspective

The Telecommunications Sector has evolved from a predominantly closed and secure wire-line telecommunications network focused on providing equipment and voice services, into a diverse, open, technologically sophisticated, highly interconnected, and complex industry with a wide array of infrastructure that spans critical aspects of the US government, economy, and society.

Three distinct policy events have shaped the course of the modern-day telecommunications industry. The first event was the 1984 court-ordered breakup of AT&T [2], a company that controlled the majority of the local and long distance markets. The second event was the passage of the Telecommunications Act of 1996 [3], which opened local PSTN (public switched telephone network) service to competition. It required incumbent carriers to allow their competitors to have open access to their networks. As a result, carriers began to concentrate their assets in collection facilities and other buildings known as telecom hotels, collection sites, or peering points instead of laying down new cable. Internet Service Providers (ISPs) also gravitated to these facilities to reduce the costs of exchanging traffic with other ISPs. Open competition has caused the operation of the PSTN and the Internet to become increasingly interconnected, software-driven, and remotely managed, while the industry's physical assets are increasingly concentrated in shared facilities. The third event was the horrific attacks of 2001, which led to sweeping changes in the reorganization of the US government with the creation of the US Department of Homeland Security (DHS), the realignment of security responsibilities of several government agencies under this new entity, and a wave of laws and national actions aimed at redefining the importance of the telecommunications and other sectors, and their threat environment. Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur [4].

In response to the attacks of 2001, the DHS issued a National Infrastructure Protection Plan (NIPP) in June 2006. This plan establishes a bold, comprehensive unifying structure and overall framework for the integration of national critical infrastructures and key resources protection efforts, into a single National Security Program. It requires designated lead federal agencies to work with the private sectors to address how sector stakeholders should implement the national strategy and protection measures, and how they can improve the security of their assets, systems, networks and functions [5].

The telecommunications sector, the theme of this article, is one of the 18 major industries identified in the NIPP as a National Critical Infrastructure. These sectors are diverse, operate in every State and affect every citizen, private and public entity, and the government at every level. The National Telecommunications Sector-Specific Plan augments the NIPP and describes the collaborate efforts between state, local, and tribal governments; nongovernmental organizations; and the federal government to secure the sector from a terrorist attack or other disaster. The plan offers a road map to prioritizing protection initiatives within and across the sector to ensure risk mitigation by lowering vulnerabilities, deterring threats, and minimizing the consequences of attacks and other incidents [1].

## 2.2 What Makes Up The Telecommunications Sector?

The Communications Sector is integrally linked with the Information Technology (IT) Sector. In general usage they are often referred to and incorporated under the common name "Telecommunications Sector." Driven by twenty-first century technology transformation and convergence, the Communications and the IT Sectors are becoming more closely aligned with telecommunications and eventually will merge into one entity. For the purposes of this article we will consider that merging to have taken place. The Telecommunications Infrastructure Sector [6] is a complex system of systems that incorporates multiple technologies and services with diverse ownership. More than 85 percent of telecommunications-related assets, systems, and networks are owned and operated by the private sector. Some owners and operators are government or quasi-government entities.

The infrastructure includes wire-line, wireless, satellite, cable and broadcasting, and the transport networks that support the Internet and other information systems. The sector provides voice and data service to public and private users through a complex and diverse public network infrastructure encompassing the PSTN, the Internet, and private enterprise networks. The PSTN provides switched circuits for telephone, data, and leased point-to-point services. It consists of physical facilities, access tandems and other equipment. The physical PSTN remains the backbone of the infrastructure with cellular, microwave, and satellite technologies providing extended gateways to the wireline network for mobile users. The Internet and private enterprise networks are key resources, comprising the domestic and international assets within both the IT and Communications Sectors, and are used by all other sectors to varying degrees.

## 2.3 How Do We Secure the Telecommunications Sector?

Much of the expertise required for planning and taking action to protect telecommunications assets lies outside the federal government, including precise knowledge of what needs to be protected [7]. The sector has historically factored natural disasters and accidental disruptions into network resiliency architecture, business continuity, and emergency preparedness planning strategies. The interconnected and interdependent nature of these service provider networks has fostered information sharing, cooperative response, and recovery relationships for decades. Since one service provider network problem nearly always impacts the networks owned and operated by other network providers, the community has a long-standing tradition of cooperation and trust, even in today's highly competitive business environment. Owners and operators have always been responsible for protecting their physical assets against unauthorized intruders. These measures, however conventionally effective in the past, generally have not been designed to cope with significant military or terrorist threats or the cascading economic and psychological impacts they may entail [8]. Such planning to defend against a terrorist attack is a relatively new phenomenon for the industry. With the wide range of operators and owners, companies, technologies, and government interests that make up the telecommunications community, it is important to find common ground in establishing sector security goals. Despite any initial variances in agreeing on a single strategic security vision, much headway has been made and new security enhancement initiatives continue to emerge as new technologies are developed and employed. Moreover, the telecommunications sector recognizes that other critical infrastructures are highly dependent on its services for basic operations. In this respect, interconnection, interoperability, and security are achieved

through technology standards, regulations, carrier agreements, and inter-carrier cooperation, enabling the infrastructure to operate effectively and rapidly restore networks after a disaster. Resiliency is achieved through the technology, redundancy, and diversity employed in the network design and by customers who plan for and employ diverse and resilient primary and backup communications capabilities [9]. Although industry partners maintain and protect the core backbone of the network and share assets and systems, and the facilities connecting these assets to the customer premises, customers are largely responsible for developing and employing mitigation strategies for access to their portion of the network through continuity of operations planning [10].

### 2.4 What are Critical Telecommunications Infrastructure Systems and Assets?

The U. S. Patriot Act defines *critical infrastructure* as "systems and assets, physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health and safety, or any combination of these matters." Telecommunications, IT, and cyber space systems, functions and assets fall under this definition [11].

### 2.5 What is the U.S. Policy on Protecting National Critical Telecommunications Services and Computer-Driven Systems?

The Telecommunication Infrastructure and its computer-driven systems are essential to the nation's security, public health and safety, economic vitality, and way of life. Within the government these systems process and communicate classified national security information concerning the vital interests of the United States. This is necessary to gather intelligence, conduct diplomacy, command and control military forces, provide continuity of essential functions of government, and to reconstitute the political, economic, and social structure of the nation. A survivable communications system is a vital component of our deterrent posture for national defense. Within the private sector these systems process and communicate sensitive business, financial, and other competitive information vital to the interests of specific enterprises. Computer-driven systems monitor, operate, and maintain prime systems in all commerce activity: Banking and Finance; Busing and Ocean Liners; Chemical; Civil Aviation; Commercial Real Estate; Defense Industrial Base; Drinking Water and Water Treatment; Education and Research; Emergency Services; Energy (electric, oil, gas, and nuclear); Food and Agriculture; Manufacturing and Construction; Postal and Shipping; Public Health and Healthcare; Seaports and Staging Areas; and Trucking and Distribution Terminals. These services provide for the economic stability and survivability of the nation.

The national policy [12] to protect telecommunications has evolved from experiences and events stemming from previous national security incidents, natural disasters, and industrial mishaps. A family of policy directives and federal laws now formulate the policy of the United States to protect these systems. The overarching goals [13] of the US policy are as follows:

1. Build a safer, more secure, and more resilient America by enhancing the protection of telecommunication assets, operations, functions, and systems.
2. Prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them.

3. Ensure that disruption, interruption, or manipulation of critical functions that do occur are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States.
4. Strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or industrial mishap.

The national policy to secure cyberspace [14] further articulates five national priorities: (i) the establishment of a security response system, (ii) a threat and vulnerability reduction program, (iii) an awareness and training program, (iv) efforts to secure government cyberspace, and (v) international cooperation. The policy emphasizes that cyber elements should have the following characteristics:

- Be robust enough to withstand attacks without incurring catastrophic damage;
- Be resilient enough to sustain nationally critical operations;
- Be responsive enough to recover from attacks in a timely manner.

The US policy focuses on protection measures that ensure essential government operations, public services, and economic functions are maintained in the event of a terrorist attack, natural disaster or other type of incident, and that elements of the telecommunication sector are not exploited for use as weapons of mass destruction.

## 3 THREATS, CHALLENGES, AND CONTINUOUS IMPROVEMENT

### 3.1 The General Threat Assessment

The threat to the telecommunications sector did not emerge on September 11, 2001. Long before that day, the nation's electronic systems had been targets of interception and disruption during times of war and armed conflicts, and from those who engaged in economic espionage and other criminal activity.

In less than one generation, the information revolution and the introduction of the computer into virtually every dimension of our society has changed how our economy works, how we provide for our national security, and how we structure our everyday lives. In the future, computer-related technologies will continue to open new vistas of opportunity for the American people. Yet this new age of promise carries within it peril. All computer-driven systems are vulnerable to intrusion and destruction. A concerted attack on the computers of any one of our critical infrastructures could have catastrophic affects on the economy [15].

The telecommunications sector faces both natural and man-made threats. It is susceptible to cyber threats such as interception, unauthorized electronic access, related forms of technical exploitation, as well as the hostile intelligence threat. The technology to exploit these electronic systems is widespread and used extensively by foreign nations, terrorist groups, and criminal elements. Other threats confronting the sector include: natural threats; cyber threats; workforce threats; explosive, chemical, and biological terrorist threats; and supply chain threats. The sector also is vulnerable to unintentional human error because of its high reliance on human interaction. It is important to mention that the threat assessment performed by the Homeland Infrastructure Threat and Risk Analysis

Center (HITRAC) on the Telecommunication Sector identified only a few direct threats, giving the sector a *low* threat rating. However, the risk for the sector as a residual target is *moderate to high* due to its interdependencies on other critical infrastructure and the significant consequences of loss that could materialize from collateral damaged sustained to sector assets and services, resulting from a direct attack upon the assets of another sector [16].

### 3.2 The Threat to America's Telecommunications Components

Attacks on telecommunications assets can produce cascading collateral damage for other sectors, far beyond the targeted asset and physical location of the incident. Natural, man-made or technological hazards could produce catastrophic losses in terms of human casualties, property destruction, and economic effects, as well as profound damage to public morale and confidence. Conversely, an attack on another sector could affect telecommunications assets. During the 2001 attacks, the telecommunications sector was not a direct target but nonetheless, significant damage impaired telecommunications facilities, lines, and equipment in the northeastern part of the nation. Much of the disruption to voice and data communications services throughout lower Manhattan occurred when a building at the World Trade Center complex collapsed into an adjacent Verizon communications center, which served as a major local communications hub within the public network. Approximately 34,000 businesses and residences in the surrounding area lost services for extended periods. Several critical government operations, among them the Federal Aviation Administration, NY City services, NY/NJ Port Authority, US Customs, FBI and US Secret Service activities were affected. Disruptions to other government and private customers in other service areas also occurred, as various carriers had equipment collocated at the site that linked their networks to Verizon. In addition, a considerable amount of telecommunications traffic that originated and terminated in other areas also passed through this location and was disrupted. AT&T's local network service in lower Manhattan was significantly disrupted following the attacks, which directly affected the operations of the World Financial District, the Stock Exchange, and international banking operations. Conversely, the electric system [17] in New York City remained operational for the island of Manhattan outside of the World Trade Center complex. Furthermore, needed electric service at Ground Zero was quickly and efficiently restored to support rescue and recovery operations.

Although not directly targeted, the telecommunications sector became a victim of significant cascading collateral damage. The loss of telecommunications service, as well as the damage sustained to the energy, water, banking and financial, public health, and transportation infrastructures created significant management challenges for the city of New York during the crisis. Despite this, the telecommunications sector demonstrated remarkable resiliency as the direct damage to its assets and operations was offset by diverse, redundant, and multifaceted communications capabilities—*a key aspect of security for this infrastructure* [18].

### 3.3 The Threat to America's Internet Networks

The Internet threat is not only physical damage to its assets but also stems from an intruder's ability to hack into the system from the outside and be capable of causing

disruption or destruction from within. The most widely reported Internet security problems of the past few years are "denial-of-service", which are designed to "crash" systems. With the explosive growth in broadband services, high-speed Internet access for home users makes it likely that future denial-of-service attacks on home computers will emerge. The misuse of the on-line environment through spam, identity theft, fake websites, and other means threaten to undermine the potential economic and social benefits of the on-line environment by eroding the trust and confidence in its safety and security [19].

Another concern is the potential for an intruder to hijack a user's computer, establishing a "backdoor" that can be activated anytime the computer is on-line, giving the intruder control over the user's system. Ironically, as government and corporate organizations have hardened their networks and become more sophisticated at protecting their systems, they have driven adversaries to pursue other targets of opportunity. Home-users with broadband connections are these new targets of opportunity both for their own computing resources and as an alternative method for attacking and gaining access to government and corporate networks [14].

Every day, in America, thousands of unauthorized attempts are made to intrude into the computer systems that control key defense facilities, power grids, banks, government agencies, telephone systems, nuclear power plants, water treatment plans, and public health and transportation systems. Some attacks are the equivalent of car thief "joy riders," committing a felony as a thrill. Others are committed for industrial espionage, theft, revenge-seeking vandalism, or extortion. Still others are committed for intelligence collection, reconnaissance, or the creation of a future attack capability. The perpetrators range from juveniles to thieves, from organized crime groups to terrorists, and from hostile militaries to intelligence services of foreign governments [20]. What has emerged in the last several years is an increase in the seriousness of the threat and a broadening of infrastructure sector targeting. Cyber crime costs have reached $100 billion a year in business disruptions and damage to systems. As a result, the Justice Department's Computer Crime and Intellectual Property Section, the FBI's Cyber Division, and the US Secret Service Electronic Crimes Task Force all play a central role in tracking crime and offenders, apprehending, and bringing to justice the responsible individuals and organizations [21].

## 4 TELECOMMUNICATIONS CHALLENGES AND CONTINUOUS IMPROVEMENT

Managing threat and reducing vulnerability in the telecommunications sector is a particularly complex challenge. While industry partners have been successful in protecting the core backbone of the telecommunications network, gaps exist in customer user responsibility. Not all customer critical systems and operations are supported by diverse primary and backup telecommunications capabilities or address the issue of single point failure consequences. Developing and employing mitigation strategies for their portion of the network, and mitigating their own risk through continuity of operations planning requires strengthening [22].

Table 1 summarizes a sampling of some of these challenges and potential solutions. The listing by no means is all-inclusive. My goal is to provide a top-level overview of some of the most significant complexities facing the telecommunications sector and what is being done, or should be considered, to narrow the vulnerability gap.

**TABLE 1 Telecommunications Sector Challenges and Continuous Improvements**

| Significant Challenges | Continuous Improvement |
|---|---|
| **1**. *Vagueness and ambiguity of planning*. In 2005, the Government Accountability Office (GAO) [23] reported that sector-specific plans varied significantly in addressing security protection measures. None of the 18 sector-specific plans fully addressed all 30 cyber security-related criteria. The Telecommunications and Information Technology Sector plans fully addressed many of the criteria, but the remaining 16 sector plans were less comprehensive. | • Enterprises that fell short of achieving expectations must adapt to the changing threat and hazard environment to address weaknesses and gaps in protection.<br>• Enterprises must continuously evaluate program weaknesses to reduce risk and introduce reasonable and prudent mitigation solutions.<br>• The emerging terrorist threat requires new approaches focused on intelligence-driven analyses, information sharing, and unprecedented partnership between the government and the private sector. |
| **2**. *Identifying and prioritizing critical assets*. The national security strategy for protecting critical resources recognizes that it is not practical or feasible to protect all assets, systems, and networks against every possible terrorist attack all the time [24]. | • Protection planning must address the full range of plausible threats and hazards, not just those most frequently reported or considered to be the most likely to occur.<br>• A proactive performance-based approach is required to enhance the decision-making processes, provide advance warning to potentially targeted assets and assist owners and operators in taking steps to protect assets in an all-hazards environment.<br>• The approach requires a coordinated and focused effort from our entire society. |
| **3**. *Protecting privacy and civil liberties*. Technologies designed to protect information and systems, if not carefully utilized, could inadvertently undermine civil liberties. Even with the best of intentions, technology that protects against intrusions, when cast too broadly, might profile innocent activity [25]. | • The U.S. Government must continue to do the following:<br>◦ protect the private information of its citizens that resides on its computer systems;<br>◦ partner with the private sector to protect personal information within their systems;<br>◦ consult with communities to define acceptable solutions; conduct legal reviews; and commit to comply with statutory and privacy solutions;<br>◦ develop robust intelligence and law enforcement capabilities to protect information systems, consistent with the law.<br>• Ensure the protection of American citizens' civil liberties, their rights to privacy, and to the protection of proprietary data. |

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| Significant Challenges | Continuous Improvement |
|---|---|
| **4**. *Internet architecture and working remotely*. With many corporations allowing employees to work at home, computer systems used for business purposes outside the official work environment create a challenge for enterprises to safeguard such systems from attack. As organizations increasingly demand remote connectivity to corporate and government networks, the security of these remote endpoints becomes increasingly critical to the overall protection of the network. This increase in interconnectivity exposes the on-line environment to a growing number, and a wider variety, of threats and vulnerabilities [26]. | • A need exists to redesign the national information infrastructure. Initially it was built quickly and without concern for security, without thought that a sophisticated enemy might attack it. Now we must fix it to protect, guard against, or reduce the existing vulnerabilities.<br>• Government and industry must continue to work together to understand vulnerabilities, develop countermeasures, establish policies and procedures, and raise awareness necessary to mitigate risks. This includes the following:<br>◦ defining an appropriate threshold for security;<br>◦ expanding infrastructure diverse-routing capability;<br>◦ understanding the risks associated with vulnerabilities of the telecommunications infrastructure. |
| **5**. *Improving system performance, reliability and efficiency*. Significant challenges are to ensure the diversity of telecommunications services; to improve the reliability and efficiency of networks, telecommunications carriers, and the physical network facilities they use to route circuits; and to support critical government and industry operations to withstand the effects of wide-scale network disruptions [27]. | • Promote collaboration to advance performance, technology, and security. Partnerships and organizations currently available to address security include the Presidents National Critical Infrastructure Board, the Government Network Security Information Exchanges, the Telecommunications Information Sharing Analysis Centers (ISAC), and the National Reliability and Interoperability Council of the Federal Communications Commission (FCC). Other programs include the National Security Telecommunications Advisory Committee, Government Emergency Telecommunications Service, Telecommunications Service Priority and Wireless Priority Service, Special Routing Arrangement Service, Next Generation Priority Service, and the Hotline System. The continued success of these partnerships and programs assures the reliability and interoperability of the government's owned or commercially provided national security and emergency preparedness communications resources. |

- Redundancy within the infrastructure is also critical to ensure that single points of failure in one location will not adversely impact connecting others. Security assessment teams need to characterize this state of diversity and collaborate to understand the topography of the physical components of the architecture in order to establish a foundation for defining a strategy that ensures physical and logical protection diversity.
- Improving business protocols, hardening facilities, building resiliency, incorporating hazard resistance into facility designs, initiating countermeasures, installing security systems, leveraging "self-healing" technologies, promoting workforce surety programs, and implementing cyber security measures will enhance program performance effectiveness.

6. *Consistency in applying evaluation measurement standards*. Although stakeholders share similar objectives, they have different perspectives on what constitutes acceptable risk and how to achieve security and reliability. Therefore, an agreement on a sustainable security threshold and corresponding security requirements remains elusive [28].

- Adapting the measurement and evaluation criteria described in the NIPP will provide uniformity to the analysis process.

7. *Government and private sector cooperation*. There is a growing awareness that confidence and security in the use of the on-line environment cannot be addressed solely as a technology matter, but requires that all users be aware of the security risks and preventive measures, assume responsibility, and take steps to strengthen the security and reliability of information and the networks it travels on [29].

- There is a need for strong leadership between government and the private sector, for outreach to users, and for cooperation across borders.
- Reducing risk requires an unprecedented partnership between our country and our global partners. This includes agency involvement by the:
  - National Coordinating Center for Telecommunications
  - National Counterterrorist Center
  - National Joint Terrorist Task Force
  - US Coast Guard Intelligence Coordination Center
  - National Maritime Intelligence Center
  - International Maritime Intelligence Center

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| Significant Challenges | Continuous Improvement |
|---|---|
| | • No single strategy can eliminate cyberspace vulnerabilities and their associated threats. The nation must continue to work with industry to manage risk and to enhance its ability to minimize the damage that results from attacks that do occur. This includes the following strategies:<br>◦ develop cohesive domestic strategies to ensure a trusted, secure, and sustainable on-line environment;<br>◦ address the threat posed by the misuse, malicious use, and criminal use of the on-line environment;<br>◦ develop watch, warning, and incident response and recovery capabilities to prevent cyber attacks and minimize damage and recovery time;<br>◦ encourage the establishment of mutual assistance programs for cyber security emergencies;<br>◦ raise awareness about the removal of impediments to information sharing about cyber security vulnerabilities between the public and private sectors;<br>◦ encourage software industry to consider promoting more secure "out-of-the-box" installation and implementation of their products;<br>◦ facilitate a national effort to promulgate best practices and methodologies that promote integrity and reliability in software code development, and processes and procedures that diminish the possibilities of erroneous code, malicious code, or trapdoors that could be introduced during development. |

**8**. *International protection*. Telecommunications networks are global in scope and extend beyond US borders. The federal government and private sector corporations also have a significant number of critical facilities located outside the United States. Providing adequate protection measures for these assets and services presents unique challenges [11].

- Industry and the US State Department should continue their involvement in international organizations such as those listed below:
  - G8
  - United Nations
  - NATO
  - European Union
  - Organization of American States
  - Asia-Pacific Economic Cooperation
  - Organization for Economic Cooperation and Development
  - International Maritime Organization
  - International Watch and Warning
- The US State Department should continue to collaborate with other federal agencies and international partners to do the following:
  - identify and prioritize the nation's critical foreign telecommunications dependencies;
  - build and strengthen international partnerships;
  - implement a comprehensive, integrated, international risk management program;
  - implement protection programs and resiliency strategies;
  - share information with international entities;
  - perform outreach to enhance information exchange and management of international agreements.
  - protect assets, systems, and networks that operate across or near the borders of foreign countries or rely on international aspects to enable critical functionality, require continuing coordination, and planning with all stakeholders;

(*continued overleaf*)

**TABLE 1** (*Continued*)

| Significant Challenges | Continuous Improvement |
|---|---|
| | ◦ interact with foreign governments and international organizations to enhance the confidentiality, integrity, and availability of cyber-based infrastructure having an international or global dimension;<br>◦ coordinate the protection of physical assets located on, near, or extending across the borders with Canada and Mexico or those with important economic supply chain implications;<br>◦ coordinate protection needs where the service originates from outside the United States to include US government and corporate facilities located overseas; |
| **9**. *The Technology Revolution and its impact on law enforcement activities*. Rapid changes in the telecommunications and computer industries have blurred the traditional gaps that separated these technologies. While the result of these changes improved our capability, many improvements make it difficult for law enforcement agencies to detect and prevent terrorist acts and inhibit lawfully authorized electronic surveillance. Some advanced technologies that form the backbone of the information superhighway also nullify the effectiveness of traditional methods of carrying out court-authorized wiretaps. Encryption technologies used to protect data are now available lawbreakers, preventing the government from obtaining contents of information it is authorized to intercept [30]. | • Adapt legislation and appropriations to support lawful programs.<br>• Encourage and fund research and development to create capabilities to respond to lawful searches.<br>• Develop new encryption technologies to counter the capabilities of lawbreakers.<br>• Continue to improve surveillance, monitoring, and detection capabilities to discover threats in the making rather than responding to an attack after the fact. |
| **10**. *Trained people*. America is short on training the IT specialists it needs to operate, improve, and secure its new IT-based economy. | • A nationwide initiative to recruit, employ, train, and retain adequate numbers of information security specialists to meet the demands of the industry is in order. |

## 5 CONCLUSIONS

### 5.1 Performance, Reliability and Efficiency

Three national program elements contribute to the stability and survivability of the telecommunications sector. The first is the advancement in micro-electronics technology, which has stimulated an unprecedented growth in the supply of telecommunications and information processing services. The second is the resiliency built into the telecommunications infrastructure that has increased the availability of services to its customers and reduced the impact of outages. The third is the priority service programs that have contributed to the continuance of critical telecommunications services and functions during an emergency [31]. Collectively, these initiatives have directly advanced the US policy on protecting national critical telecommunications services and computer-driven systems.

### 5.2 The Threat to America's Telecommunications Sector

The pace of the technological drive to install computer controls in every one of our nation's critical infrastructures far outstrips our potential to design computer security software, train IT security personnel, or develop and promulgate computer security practices and standards. We have created a gaping vulnerability in our national security and economic stability that affects not only computer-controlled systems, but also the vital databases maintained by public health centers, law enforcement, legal and judicial institutions, educational and research institutions, and proprietary data managed and operated by other sector functions and systems. We are vulnerable to mischief-making hackers, hardware and software failures, cyber criminals and, most alarmingly, to deliberate attack from nation states and terrorists. To complicate matters further, most critical infrastructures interconnect and therefore, depend on the continued availability and operation of other systems and functions. This interconnectivity is provided by the IT and telecommunications sectors, which increasingly control the operations and productivity of the other critical infrastructures. Given the dynamic nature of these interdependent infrastructures and the extent to which our daily lives rely on them, a successful terrorist attack to disrupt or destroy IT and telecommunications critical assets could have a tremendous impact beyond the immediate target and continue to reverberate long after the immediate damage is done [7].

### 5.3 Future Research Direction

The unique characteristics of the telecommunications infrastructure sector, the rapid change in technology, and the significant impediments complicating their protection requires an unprecedented level of public and private sector cooperation and government coordination. The challenge ahead is to develop a coordinated and complementary system that reinforces protection efforts rather than duplicates them, and that meets mutually identified essential requirements. In addition, many telecommunications assets, systems, and functions span national borders and, therefore, must be protected within the context of international cooperation [32].

Several government initiatives [33] have helped keep America safe since the 2001 attacks. The first initiative is the development of partnerships among government,

industry, academics, and others to ensure a trusted, secure, and sustainable telecommunications environment through the development, implementation, and review of guidelines and best practices. These federal programs augment the extensive state, local, tribal, territorial, and private sector protection programs that constitute important efforts already being implemented. The second initiative is the creation of Homeland Security Centers of Expertise, which challenges us to marshal our nation's advantages in the sciences and technology. These Centers are combating terrorism across a wide range of research and development activity and are studying the following:

- the interactions of networks and the need to use models and simulations;
- risk analysis related to the economic consequences of terrorist threats and events;
- potential threats to animals and agriculture and agro-security issues related to postharvest food protection;
- improvement and promotion of the design, development, and implementation of usable security measures in existing and new technologies.

The third initiative is the removal of structural and legal impediments that prevented the collection and sharing of information by our law enforcement and intelligence agencies. The fourth initiative concerns the government's diplomatic outreach and operational capabilities to build global partnerships to combat cyber crime whenever it originates.

### 5.4 The Prospects for the Future

Despite all the hard work accomplished to create new laws and the means to combat telecommunications terrorism, our work is far from complete in both planning and execution. We can expect to see more frequent and escalated planning activity by adversarial groups to attack our critical assets. Future attempts to disrupt or damage our communications capabilities is almost evident and probably a matter of time. The threat is that in a future crisis a criminal cartel, terrorist group, or hostile nation could seek to inflict economic damage, debilitating disruption and death, and degradation of our national response by attacking critical networks. Terrorists are relentless and patient. They are also opportunistic and flexible. Terrorists are inventive and resourceful in terms of target selection, as well as in the selection and use of specific instruments of violence, and intimidation at the time and location of their choosing [34].

In focusing our protection efforts, we must acknowledge three key factors [35]: (i) Given the immense size and scope of potential target sets within the telecommunications sector we cannot protect completely all things, at all times, against all conceivable threats. (ii) The assets, systems and functions that comprise the telecommunications infrastructure are not uniformly "critical" in nature, particularly in a national or regional context. (iii) Given the dynamics of the sector's size and scope, and diversity of mission, we must prioritize protection strategies to reduce vulnerability and threat condition; to maximize program effectiveness, efficiency, resources, and funding allocations; and to maximize returns on our investment.

Despite the tremendous effort we are putting into our planning, no protection strategy can succeed in isolation. It must be a part of a larger strategy that is responsive to economic and national security considerations [36]. We must move forward with the understanding that there are enemies who seek to inflict damage on our way of life.

They have attacked us on our own soil, and they have shown a willingness to use unconventional means to execute those attacks. The attack tools and methodologies they are employing are becoming widely available and, the technical capability and sophistication of users bent on causing havoc or disruption is improving. We now have an opportunity and an obligation to take action to prevent, deter, neutralize, or mitigate the effects of deliberate efforts to disrupt, interrupt, manipulate, destroy, incapacitate, or exploit telecommunications assets. We must renew our resolve to embark upon a program of self-assessment to identify program weaknesses; mitigation analysis and problem-solving to strengthen our security status; advanced research and development to improve technology performance and survivability; and enhance practices whereby we can objectively reduce the risk to telecommunications resources, assets, facilities, systems, and functions.

## REFERENCES


1. Sullivant, J. (2007), *Strategies for Protection National Critical Infrastructure Assets: A Focus on Problem-Solving*. John Wiley & Sons, Hoboken, NJ, p. 500.
2. Communications Infrastructure Plan (2007), p. 9, U.S. Department of Homeland Security, Washington, DC.
3. National Strategy for the Physical Protection of Critical Infrastructure & Key Assets (2003), p. 3, U.S. Department of Homeland Security, Washington, DC.
4. The National Infrastructure Protection Plan (2009), p. 8, U.S. Department of Homeland Security, Washington, DC.
5. Communications Infrastructure Plan (2007), p. 1, U.S. Department of Homeland Security, Washington, DC.
6. National Strategy for the Physical Protection of Critical Infrastructure & Key Assets (2003), p. 8, U.S. Department of Homeland Security, Washington, DC.
7. Ibid. (2003), p. 8, U.S. Department of Homeland Security, Washington, DC.
8. Communications Infrastructure Plan (2007), p. 2, U.S. Department of Homeland Security, Washington, DC.
9. Ibid. pp. 9–11; 21.
10. National Strategy for the Physical Protection of Critical Infrastructure & Key Assets (2003), p. 6, U.S. Department of Homeland Security, Washington, DC.
11. Presidential National Security Directive (NSD): National Policy for the Security of National Security Telecommunications and Information Systems (1990), p. 1–3, Office of the President of the United States, Washington, DC.
12. The National Infrastructure Protection Plan (2009), p. 9, U.S. Department of Homeland Security, Washington, DC.
13. National Strategy to Secure Cyberspace (2003), p. 13–14, U.S. Department of Homeland Security, Washington, DC.
14. Defending America's Cyberspace–National Plan for Information Systems Protection (2006), pp. 6–9, U.S. Department of Homeland Security, Washington, DC.
15. Communications Infrastructure Plan (2007), pp. 35–37, U.S. Department of Homeland Security, Washington, DC.
16. National Strategy for the Physical Protection of Critical Infrastructure & Key Assets (2003), p. 9, U.S. Department of Homeland Security, Washington, DC.

17. Sullivant, J. (2007). *Strategies for Protection National Critical Infrastructure Assets: A Focus on Problem-Solving*. John Wiley & Sons, Hoboken, NJ, p. 502.
18. Ibid. pp. 502–503.
19. Ibid. p. 503.
20. The National Strategy to Secure Cyberspace (2003), p. 28.
21. Ibid. p. 7.
22. GAO. (2005). *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cyber Security Responsibilities.* GAO-05-434, Washington, DC, May 25, 2005.
23. The National Infrastructure Protection Plan (2009), pp. 40–42.
24. Defending America's Cyberspace–National Plan for Information Systems Protection (2006), pp. 11–15.
25. Ibid. (2006), pp. 4–5.
26. Sullivant, J. (2007). *Strategies for Protection National Critical Infrastructure Assets: A Focus on Problem-Solving*. John Wiley & Sons, Hoboken, NJ, p. 523.
27. Ibid. p. 506.
28. Defending America's Cyberspace–National Plan for Information Systems Protection (2006), pp. 21–80.
29. Communications Infrastructure Plan (2007), pp. 11–19.
30. Communications Infrastructure Plan (2007), p. 4.
31. National Strategy for the Physical Protection of Critical Infrastructure & Key Assets (2003), pp. 6–7.
32. The National Infrastructure Protection Plan (2009), pp. 25–26; 49–70; 149–153.
33. National Strategy for the Physical Protection of Critical Infrastructure & Key Assets (2003), p. 7.
34. Ibid. (2003), pp. 2–3.
35. National Strategy to Secure Cyberspace (2003), pp. 5–11.
36. Ibid. pp. 5–11.

## FURTHER READING

*Executive Order 13231: Critical Infrastructure Protection in the Information Age*. (October 16, 2001).

*Executive Order 12382: National Security Telecommunications Advisory Committee*. (February 28, 2003).

*Executive Order 12472: Assignment of Emergency Preparedness Telecommunications Functions*. (April 3, 1984),

Information Technology Infrastructure Plan (2007).

Lewis, T. G. (2006). *Critical Infrastructure Protection in Homeland Security: Defending A Networked Nation*. John Wiley & Sons, New York.

National Response Plan (2008).

National Strategy for Combating Terrorism (2006).

National Strategy for Homeland Security (2002).

National Strategy to Combat Weapons of Mass Destruction (2002).

NSDD 145: National Policy on Telecommunications and Information Systems Security (1984).

# WIRELESS SECURITY

MATTHEW SEXTON, EDWARD SMITH, AND BERNIE EYDT
*Booz Allen Hamilton, McLean, Virginia*

## 1 SCIENTIFIC OVERVIEW

Wireless networks have undoubtedly proliferated into many aspects of daily life, both personal and professional. Although many wireless networks exist, ranging from cellular networks to Wireless Fidelity (Wi-Fi), they can be divided into two primary categories: data-centric and voice-centric. Data-centric wireless networks primarily provide extensions of the existing Internet Protocol (IP)-centric networks and evolved from wired IP-centric networks providing security similar to that of wired networks. Voice-centric wireless networks evolved as extensions of the legacy wireline telephony networks and focus security on end user issues, such as cloning, billing fraud, and other forms of subscriber-based attacks. This end user fraud protection focus, although valid for an extension of the wireline voice network, offers weaker security architecture for data services added to the voice network as enhancements to user services.

### 1.1 Voice-Centric Networks

Security within today's voice-centric networks has advanced well beyond the rudimentary security provided by first-generation mobile phone services that were mere extensions of the public service telephone network (PSTN). User authentication, voice and data privacy, and assurance of transmitted data are becoming the norm in wireless voice services. Security technologies have evolved as voice and data networks have converged with modern cellular networks, which have a mixture of security technologies. Third-generation (3G) cellular networks are poised to enhance security based on lessons learned from current networks and the application of technologies from data-centric networks. The following is a brief summary of the advances and issues with current and future voice-centric wireless networks.

***1.1.1 Network Evolution Path.*** Cellular security is the result of two evolutionary paths taken from first-generation cellular services, which were simple extensions of the PSTN. In the United States, wireless security evolved from the first-generation Advanced Mobile Phone Service (AMPS), which provided limited security. The United States deployment of second-generation cellular (time division multiple access technology and code division multiple access [CDMA] technology) took a more limited approach to security and focused on addressing issues identified with the AMPS service, such as billing fraud resulting from the ability to clone phones and off-air voice intercept.

The first cellular enhancement addressed in the United States was billing fraud resulting from thieves collecting user information from off-air signaling and using that

information to clone phones. The solution was to employ more robust user authentication through a challenge-response method known as the *cellular authentication and voice encryption* (CAVE) algorithm. The CAVE algorithm is a challenge-response method that uses network and user parameters to develop shared secret data (SSD) to form the basis of over-the-air parameter exchanges. The method uses cryptography to create a dynamic authentication response used to verify the identity of the user, thus greatly reducing the possibility of successful phone cloning and fraudulent access.

Another US enhancement was increased voice privacy. This enhancement was made possible by increasing the complexity of the signal modulation and voice coding techniques employed in the digital transmissions, and by adding the optional application of a voice privacy mask to the digital voice. The digital modulation made the possibility of publicly available radiofrequency (RF) intercept systems, such as police scanners, intercepting and decoding the voice extremely unlikely. The application of a voice privacy mask added security from unwanted intercept if the data was intercepted.

Today, 3G cellular communications face many of the same design challenges and constraints as its 2G/2.5G ancestors. Two standards bodies govern the cellular industry; the Universal Mobile Telecommunications System (UMTS) is specified by the Third Generation Partnership Project (3GPP) and the CDMA2000 architecture is specified by 3GPP2 [1]. Both systems face many of the same risks and threats, and therefore share a number of common security elements or traits [2].

Subscriber authentication, session confidentiality, and signaling integrity are the primary goals of secure communications. UMTS and CDMA2000 security protocols such as the authentication and key agreement (AKA) protocol are more robust mechanisms designed to limit the vulnerability of and improve the security stance of cellular communications. A central concept for all wireless communications is access security. Restricting subscriber access to authenticated and authorized devices, coupled with voice and data encryption will reduce an organization's network vulnerability.

The Internet Protocol Multimedia Subsystem (IMS), originally designed by the 3GPP, is a widely accepted open standard effort to define an all IP-based wireless network. Its adoption has been slow, but the technology may help promote a convergent future that will bring cellular networks together with other wireless technologies. IMS promotes the use of employing established, open protocols and commodity equipment. This approach facilitates application access and promotes interoperability between disparate networks by bridging the gap for access technology, that is, IMS networks operate with any endpoint that supports IP capabilities. However, since IMS requires new network infrastructure, many carriers have been slow to implement their rollout plans because of costs and complexity.

***1.1.2 Project 25 Digital Radio.*** Project 25 (P25) is a standard for the manufacturing of interoperable digital two-way wireless communication products. Formed in 1989, P25 began as a joint effort between the National Association of State Telecommunications Directors (NASTD), the Association of Public-Safety Communications Officials-International (APCO), and a group of federal agencies to develop a series of standards to define a digital radio system (conventional and trunked) [3]. The Telecommunications Industry Association (TIA)-102.AAAB standard provides an overview of the security services available in land mobile radio (LMR) [4]. It generalizes security requirements into three categories: (i) confidentiality, (ii) authentication and integrity, and (iii) key

management. Two additional security-related TIA standard documents detail block encryption [5] and over-the-air-rekeying (OTAR) [6].

Either the Data Encryption Standard (DES) or Advanced Encryption Standard (AES) can provide confidentiality. Currently, AES support is required for compliance with the P25 block encryption standard, and DES is optional. Although DES was officially withdrawn (i.e. Federal Information Processing Standards [FIPS] 46-3) by the Secretary of Commerce, many governmental organizations including state and local governments still implement this algorithm. Encryption, chronological message numbers, and message authentication codes provide integrity, as does a device's electronic serial number (ESN). A key management facility (KMF) or a key variable loader (KVL) provides key management. A KMF uses OTAR and is therefore much more scalable than the manual use of KVLs to load subscriber device encryption keys. OTAR distributes traffic encryption keys (TEK) using key encryption keys (KEK) (also known as *shadow keys*) to ensure confidentiality of cryptographic secrets. A critical challenge to today's public safety personnel is secure and interoperable communications. There are many challenges to implement a KMF to KMF interface standard, that is, a shared interoperability key environment. Key generation/distribution between multiple agencies remains a challenge for a number of reasons. For example, agencies that employ OTAR may have the same interop keys, but subscriber unit storage location numbers may not map to the proper key identifier required for voice communications. This has been a problem for many years and is discussed in greater depth later in this technical article. It is also important to note that the key rotation schedule for P25 devices usually exceeds 30 days, compared to other wireless technologies that may rotate their communication key each session. While P25 devices can connect to laptops or other data networks [7], their transmission rates are limited and they cannot support broadband data applications.

## 1.2 Data-Centric Networks

***1.2.1 Radio Frequency Identification Technologies.*** Radio Frequency Identification (RFID) technologies are a form of automatic identification and data capture technology that uses electric or magnetic fields at radio frequencies to transmit information [8]. RFID tags are tiny microchip transponders that constantly listen for a radio signal sent by transceivers. The majority of RFIDs are "passive" or do not require a power source, they get their power from the radio signals themselves. Several common uses of RFID are: asset tracking, manufacturing, retailing, payment systems, security and access control, and even health care patient tracking. RFID has two groups of technical controls: controls to protect the tag, and controls to protect RF communications. Security controls vary by tag generation, and by the power supply and processing capability of the tag. Security is focused on the system as a whole, rather than the RFID tag alone. A comprehensive review of RFID technical, managerial, and operational controls are detailed in National Institute of Standards and Technology (NIST) SP 800-98: Guidance for Securing RFID Systems [8].

***1.2.2 IEEE 802.11 Wireless Local Area Networks.*** Wireless local area network (WLAN) communications offer organizations and users many benefits, such as portability, flexibility, increased productivity, and lower installation costs. The IEEE 802.11 standards working group developed the medium access control (MAC) and physical layer (PHY) specifications for wireless connectivity for fixed and mobile

devices within a local area. The original confidentiality protocol—Wired Equivalent Privacy (WEP)—was intended to provide security comparable to that of wired local area networks (LANs) [9]. Unfortunately, WEP turned out to be susceptible to a variety of attacks [10], and it suffered even more from poor vendor implementations, such as the reuse of initialization vectors [11] and the use of initialization vector of all zeros [12]. To address WEP's problems, IEEE established an IEEE 802.11 security enhancements working group that published the 802.11i specification. The Wi-Fi Alliance, an industry group, also promoted this effort through interoperability testing of equipment designed to the IEEE 802.11i specification. The Wi-Fi Alliance refers to the IEEE 802.11i enhancements as Wireless-Fidelity Protected Access (WPA).

The initial WPA specification addressed only a subset of IEEE 802.11i, the IEEE security amendment to the MAC layer, because the standard was not yet complete when WPA testing began. WPA employs the Temporal Key Integrity Protocol (TKIP) for data encryption which uses the same RC4 algorithm as WEP, but adds improved key management and message integrity checking. Of WEP, TKIP, and Counter Mode cipher block chaining-message authentication code (CBC-MAC) Protocol (CCMP), only CCMP uses the AES [13], which is FIPS-validated [14]. Both WEP and TKIP are based on Rivest's Cipher (RC4), which is not FIPS-validated. Following ratification of IEEE 802.11i, the Wi-Fi Alliance introduced WPA2, which identifies equipment capable of supporting all 802.11i requirements. In addition, two wired standards were implemented to provide network access control: 802.1x [15] and the Extensible Authentication Protocol (EAP) [16]. A comparison of the IEEE 802.11 security protocols is provided in Table 1.

***1.2.3 IEEE 802.16 Wireless Metropolitan Area Networks.*** As cellular services race toward 3G deployments, Mobile Worldwide Interoperability for Microwave Access (WiMAX) is emerging as a complementary technology to existing telecommunication and fixed-data technologies. The industry trade group WiMAX Forum trademarked the WiMAX name and promotes the interoperability of broadband wireless products based on the IEEE 802.16 standard. WiMAX technology provides yet another wireless service and more drive to develop seamless interoperability standards, such as IMS, among other wireless services, such as cellular and Wi-Fi. WiMAX technology was initially envisioned as a fixed wireless point-to-multipoint service that would provide backhaul services from homes and small businesses. It has evolved beyond this concept into a

**TABLE 1 A Comparison of the 802.11 Security Protocols**

| | WEP (RC4) | WPA (TKIP/RC4) | 802.11i (AES-CCMP) |
|---|---|---|---|
| **Cipher** | RC4 | RC4 | AES |
| **Key size (bits)** | 40/104 | 64/128 | 128[a], 192, 256 |
| **Key life** | 24-bit IV | 48-bit IV | 48-bit IV |
| **Packet key** | Concatenated | Mixing function | Not needed |
| **Data integrity (MSDU)** | CRC-32 | Michael | CCM |
| **Header integrity (MPDU)** | None | Michael | CCM |
| **Replay attack** | None | Use IV | Use IV |
| **Key management** | None | EAP-based | EAP-based |

[a]NIST only specifies this block size.

MSDU, Media Access Control Service Data Unit; MPDU, Media Access Control Protocol Data Unit.

technology that can provide not only last-mile access to homes and businesses but also mobile user access to broadband services.

Not only does the technology support coverage of a large number of users in a geographical area from a single Base Station, but also, with the addition of technologies to address mobility, the system is frequency efficient. A frequency reuse of one to one can be employed, resulting in a single carrier frequency used throughout an entire system. In addition, WiMAX provides high quality of service (QoS) for time-critical services, such as Voice over Internet Protocol (VoIP).

***1.2.4 WiMAX Security.*** The end-to-end WiMAX network architecture is based on a security framework that is service-application agnostic and gives users a strong suite of security tools. In particular, the framework supports the following: strong mutual device authentication between a mobile subscriber (MS) and the WiMAX network; all commonly deployed authentication mechanisms and authentication in homes and visited operator network scenarios based on a consistent and extensible authentication framework; data integrity, replay protection, confidentiality, and nonrepudiation using applicable key lengths; use of MS-initiated and terminated security mechanisms, such as Virtual Private Networks (VPN); and standard secure IP address management mechanisms between the MS/subscriber station (SS) and its home or visited network service provider (NSP). Mobile WiMAX supports current security features by adopting the best technologies available today. Support exists for mutual device and user authentication, flexible key management protocol, strong traffic encryption, control and management plane message protection, and security protocol optimizations for fast handovers. Table 2 details the usage aspects of WiMAX's security features.

**TABLE 2 Usage Aspects of WiMAX Security Features**

| WiMAX Security Feature | Description |
|---|---|
| Key Management Protocol | Privacy and Key Management Protocol Version 2 (PKMv2) is the basis of Mobile WiMAX security as defined in 802.16e-2005. |
| Device/User Authentication | Mobile WiMAX supports device and user authentication using RSA or IETF EAP protocol by providing support for credentials that are SIM based, Universal SIM (USIM) based, or digital certificate or username/password based. |
| Traffic Encryption | AES-Counter with CBC-MAC (CCM) is the cipher used for protecting all user data over the Mobile WiMAX MAC interface. The keys used for driving the cipher are generated from the EAP authentication. A traffic encryption state machine that has a periodic key (TEK) refresh mechanism enables sustained transition of keys to further improve protection. |
| Control Message Protection/ Secure Key Exchange | Control data is protected using AES-based Cipher-based message authentication code (CMAC), or MD5-based hash message authentication code (HMAC) schemes. |
| Fast Handover Support | Mobile WiMAX supports a three-way handshake scheme to optimize the reauthentication mechanisms for supporting fast handovers. This mechanism is also useful to prevent any man-in-the-middle attacks. |

RSA, Rivest-Shamir-Adleman; SIM, Subscriber Identity Module.

## 2 MOBILE AND WIRELESS SECURITY LANDSCAPE

Today, the wireless landscape continues to evolve. Security continues to remain a concern in the commercial or public space and for the handling of sensitive or classified information in government or private organizations. Federal data handling requirements are much more complex and restrictive than those in the commercial market; therefore, wireless systems in the government tend to remain independent of one another and commonly fail to implement an enterprise or holistic approach to information security.

The commercial market's security stance is easier to understand than the government market's stance; as a result, the standards bodies that define and develop future technologies are working to address commercial issues without addressing the added security needs of the federal government. To help close this gap, the federal government has become a greater participant in wireless standards development and therefore, interacts directly with industry standards bodies.

Standards bodies promote regulatory compliance by providing the reference model for layered security. The International Organization for Standardization (ISO) Open System Interconnection (OSI) standard is a worldwide communications framework for implementing protocols in seven layers. Wireless security technologies operate at Layer 1 (physical) and Layer 2 (data link) of the OSI model and may be tightly integrated with higher layer (Layers 3–7) security mechanisms to provide to a robust security solution.

### 2.1 Federal Legislation and Regulation

Although wireless security is not specifically addressed in the federal laws, the requirement to protect information affects the implementation of wireless technologies. Title III of the E-Government Act (Public Law 107-347)—the Federal Information Security Management Act (FISMA)—requires each federal agency to develop, document, and implement an agency-wide information security program. The government has also passed legislations to better regulate commercial industry and protect the privacy of American citizens. These laws include the Health Insurance Portability and Accountability Act of 1996, Gramm-Leach-Bliley Act of 1999, and Sarbanes-Oxley Act of 2002. The 9/11 Commission Act of 2007 also mandates an Federal Communications Commission (FCC) vulnerability assessment of the nation's critical communications and systems infrastructure and to create a backup emergency communications system which includes next generation and advanced communications technologies [17]. In April 2007, the FCC chartered the Communications Security, Reliability, and Interoperability Council (CSRIC) to recommend best practices to ensure the security, reliability, operability, and interoperability of public safety communications systems [18].

Legislation focused on the lawful intercept of confidential communications also includes the Communications Assistance for Law Enforcement Act (CALEA). CALEA is a US wiretapping law passed in 1994 that amends Title 18 of the United States Code to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement and other purposes. CALEA aids law enforcement in its effort to conduct surveillance of citizens via digital telephone networks within the United States.

**TABLE 3 Table of NIST Wireless Security-Related Special Publications**

| NIST Special Publication | Description |
|---|---|
| 800-48 Rev. 1 | Guide to Securing Legacy IEEE 802.11 Wireless Networks, July 2008 |
| 800-52 | Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations, June 2005 |
| 800-57 | Recommendation on Key Management, March 2007 |
| 800-58 | Security Considerations for Voice Over IP Systems, January 2005 |
| 800-77 | Guide to IPsec VPNs, December 2005 |
| 800-88 | Guidelines for Media Sanitization, September 2006 |
| 800-94 | Guide to Intrusion Detection and Prevention (IDP) Systems, February 2007 |
| 800-97 | Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i, February 2007 |
| 800-98 | Guidelines for Securing Radio Frequency Identification (RFID) Systems, April 2007 |
| 800-101 | Guidelines on Cell Phone Forensics, May 2007 |
| 800-111 | Guide to Storage Encryption Technologies for End User Devices, November 2007 |
| 800-121 | Draft Guide to Bluetooth Security, July 2008 |
| 800-124 | Draft Guidelines on Cell Phone and PDA Security, July 2008 |

### 2.2 Federal Standards and Guidance Publications

This category of information security guidance is primarily provided by NIST [19] publications in accordance with the NIST's statutory responsibilities under FISMA. Federal agencies are required to use FIPS-validated cryptographic algorithms verified by the Cryptographic Module Validation Program (CVMP). Products validated as conforming to FIPS 140-2 [20] are accepted by federal agencies for the protection of sensitive information. Table 3 presents a list of NIST publications whose topics touch on wireless technologies.

### 2.3 Industry Standards and Guidance Organizations

Standards and guidance organizations play an important role in information security and interoperability. Industry plays an important role by promoting technical progress within a standard, but it can also pose a barrier to interoperable communications. Fortunately, there are non-profit groups that help drive the adoption of wireless communications standards. The major worldwide communications standards organizations periodically meet at an event called *Global Standards Collaboration* [21]. These organizations address many of industry's technical and operational issues to promote interoperable end-to-end communication solutions. The global standards organizations include the International Telecommunications Union (ITU), Telecommunications Industry Association (TIA), Internet Engineering Task Force (ITEF), Institute of Electrical and Electronic Engineers (IEEE), Alliance for Public Technology (APT), International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC).

Whereas the Department of Defense (DOD) may have departments focused on development of standards and their associated testing to ensure interoperability (e.g. the Joint Interoperability Test Command), civilian agencies lack such standards and verification groups for tactical or mission-critical communications. Fortunately, there are several standards organizations focused on developing this work. The Telecommunications Industry Association, Project 25 Technology Interest Group, Association of Public-Safety Communications Officials International and its subsidiaries promote the development of public safety communications, that is, the Project 25 communications standard. The IEEE 802 LAN/Metropolitan Area Networks (MAN) Standards Committee has also been instrumental in the development of data-centric wireless standards, including IEEE 802.11 (Wi-Fi), 802.15.1-2005[1] (Bluetooth), and 802.16-2004/802.16e-2005 (WiMAX). IEEE is focused on standards development, not interoperability; however, several industry organizations have formed groups (e.g. the WiMAX Forum and Wi-Fi Alliance) to promote the interoperability of several prevalent wireless technologies based on the IEEE 802 family of standards. In addition, perhaps the most widely used wireless technology, cellular communications, is governed through two international partnership projects. The Third Generation Partnership Project (3GPP) focuses on the evolution of the GSM family of technologies to Wideband Code Division Multiple Access (W-CDMA) technologies; whereas, a parallel partnership project, 3GPP2 was established as a collaborative 3G telecommunications specification-setting project for 3G technologies derived from North American Code Division Multiple Access (CDMA) systems (IS-95).

To facilitate the convergence of wireless technologies, the IEEE 802.21 standards body and the 3GPP Unlicensed Mobile Access (UMA) [25] partnerships formed a working group to standardize subscriber access to mobile circuit, packet, and IMS-based services over IP-based access networks, including the Internet.

## 2.4 Governmental Wireless Communications Initiatives

The American National Standards Institute (ANSI) Homeland Security Standards Panel (HSSP) helps identify existing consensus standards. If no standard exists, HSSP assists the U.S. Department of Homeland Security (DHS) and those entities requesting assistance to accelerate development and adoption of consensus standards critical to homeland security [21]. To date, two workshop meetings have been held. Their focus was to identify existing standards, standards under development, and gap areas in standardization for emergency communications. However, government-to-government communications were not addressed by HSSP, as public safety interoperability still remains the responsibility of several Federal agencies and working groups, which include the Federal Communications Commission (FCC), National Public Safety Telecommunications Council (NPSTC), DHS, National Telecommunications and Information Administration (NTIA), Institute for Telecommunication Sciences (ITS), and the National Security Telecommunications Advisory Committee (NSTAC). These organizations promote the advancement of governmental P25 technology and serve as a resource for addressing the telecommunications challenges of Federal agencies, state and local governments.

[1]Following the publication of 802.15.1-2005, the HYPERLINK ”http://en.wikipedia.org/wiki/IEEE” \o ”IEEE” IEEE Study Group 1b voted 90-0 to discontinue their relationship with the HYPERLINK ”http://en.wikipedia.org/wiki/Bluetooth_SIG” \o ”Bluetooth SIG” Bluetooth SIG, effectively meaning that the later versions of Bluetooth will not become future IEEE standards. Bluetooth standards are developed through the Bluetooth Special Interest Group (SIG) http://www.bluetooth.com/Bluetooth/SIG/

DHS relies heavily on wireless communications for mission success. The DHS Science and Technology Directorate is the primary research and development component of DHS, which pilots and evaluates emerging wireless technologies in support of homeland security. The Office of Emergency Communications (OEC) works across Federal, state and local entities to ensure, accelerate, and attain interoperable and operable emergency communications nationwide. OEC has engaged the Federal Partnership for Interoperable Communications Committee to actively address technical and operational interoperable activities with the federal wireless communications community [22]. In addition, DHS has other committees, working groups, subcomponents, and agencies focused on wireless communications and emergency response communications including the Federal Emergency Management Agency (FEMA), National Protection and Programs Directorate (NPPD), Office of Cybersecurity and Communications, Emergency Communications Preparedness Center (ECPC), and the National Communications System (NCS).

Federal government partnerships have also been launched to help facilitate the development of secure and interoperable communications Originally developed by a DoD/National Security Agency (NSA) program, the Secure Mobile Environment Portable Electronic Device (SME PED) is a Type-1 capable mobile and wireless device designed to enhance cross communication and support the mission of the US military, intelligence, and homeland security organizations. The SME PED offers converged secure Type 1 and Non-Type 1 wireless voice and data capabilities and is the first portable device to offer multiple independent levels of secure communication in both unclassified and classified modes.

## 3 CRITICAL NEEDS ANALYSIS

The protection, response, and recovery capabilities among federal, state, and local authorities rely on guaranteed secure wireless communications to extend their disparate wired infrastructures to the first responder. DHS dynamic business requirements and distributed wired infrastructure require complex solutions that are more difficult to secure. All connections to the wireless network must be authenticated, authorized, and protected. Guaranteed communications also require that wireless communications infrastructure provide a high level of availability.

Wireless security must address the areas where the wireless network is vulnerable: the device level and the network level (wireless and wireline). Wireless devices represent the edge of the extended infrastructure and should to be thoroughly secured in case of loss or theft. Unfortunately, a negative trade-off in performance exists when implementing device security. Mobile or portable devices have limited processing and power; therefore, implementing additional device security controls will adversely affect responsiveness and battery life.

Wireless access points are the gateways to an organization's trusted wired network. Although the air interface may be properly secured, a common shortfall of wireless architectures is their infrastructure. Generally, attacks fall into one of two categories: active or passive attacks. Active attacks require actions on the part of the attacker to penetrate or disrupt the network; passive attacks are used primarily for information gathering and surveillance. intrusion prevention systems (IPSs) provide a layer of defense and help protect a wireless system against threat consequences, including unauthorized disclosure, disruption, deception, and corruption [21].

### 3.1 Intrusion Prevention Systems

Wireless IPSs operate at Layer 2 of the OSI model, compared to Layer 3 and higher for wireline systems. IPSs are used to detect the presence of rogue and misconfigured devices, scan the air medium for denial of service (DoS) and other forms of attacks, and take defensive actions to protect the network. A key characteristic of wireless IPS systems is their responsibility to ensure that only authorized devices participate in an enterprise's wireless network. In addition, wireless IPSs address a variety of wireless-only attacks and respond with predefined steps that usually involve the wireless infrastructure. For example, an IPS must be able to identify and respond to known vendor implementation weaknesses, such as the EAP-Lightweight Extensible Authentication Protocol (LEAP) vulnerability to dictionary attacks.

### 3.2 Internet-Based Security Protocols

Wireless technologies must leverage the security capabilities of Internet-based standards. Wireless technologies that implement their own unique security protocols hinder secure and interoperable communications. Security should not be a barrier to communications but rather a catalyst for interoperability.

Federal government-level wireless communications require encryption, authentication, and authorization-related activities. These symmetric and asymmetric keys are required for the generation, distribution, storage, and destruction of cryptographic key material. Public safety technologies should employ key management solutions that are standards-based and promote interoperability.

Wireless technologies can leverage the mature security protocols implemented at higher layers in the protocol stack. For example, Secure Socket Layer (SSL) or Transport Layer Security (TLS) are Layer 4, certificate-based security protocols used extensively over the Internet; Internet Protocol Security (IPSec) is a Layer 3 security protocol that secures Layer 4 and higher. It is important to note that encryption only protects the layer above its implementation. For example, masking an Internet address requires Layer 1 or 2 security, which is where wireless security resides. Secure Multipurpose Internet Mail Extensions (S/MIME) is a security protocol that adds asymmetric encryption for secure text messaging, which is most commonly used for Internet e-mail. Table 4 details some common OSI layer security protocols.

There would be benefit to federal agencies leveraging DoD best practices and technology research. For example, the NIST and NSA established National Information Assurance Partnership (NIAP) to evaluate Information Technology (IT) product conformance to international standards. The program, officially known as the *NIAP Common Criteria Evaluation and Validation Scheme* (CCEVS) for IT Security, is a partnership between the public and private sectors to help organizations select commercial off-the-shelf IT products that meet international security requirements and to help manufacturers of those products gain acceptance in the global marketplace. Twenty countries now recognize the Common Criteria as the official third-party evaluation criteria for IT security products. Civilian agencies may wish to explore NIAP in its product selection to promote security and interoperability throughout the federal government.

First responders and other federal, state, and local personnel will increasingly need to carry radios with multiple air interfaces to interoperate with other agents and civilians in need. The ideal DHS handset would support public safety communication using P25;

**TABLE 4 OSI Layers and Corresponding Security Protocols**

| Layer | Security Considerations |
|---|---|
| Application | Detect and prevent malicious code, viruses, and other malware applications. Mitigation tools include firewalls, antivirus application, and intrusion detection applications. |
| Presentation | Protect data files by cryptography (e.g. file password encryption). |
| Session | Protect system from port exploits and validate digital certificates. SSL operates between the session and transport layers. |
| Transport | Provide authentication and secure end-to-end communications. Encryption protocols include Secure Shell (SSH-2) and Simple Key Management for Internet Protocols (SKIP). |
| Network | Protect the routing and the forwarding protocols. The IPSec standard provides multiple and simultaneous tunnels versus the single connection limit of the lower layer encryption standards. |
| Data Link (Wireless Security) | Protect the MAC layer from masquerade, DoS, impersonation, and Address Resolution Protocol (ARP) threats. Common encryption protocols include the Point-to-Point Tunneling Protocol (PPTP) and the Layer 2 Tunneling Protocol (L2TP). |
| Physical (Wireless Security) | Prevent jamming and DoS attacks in the air medium through frequency hopping and similar techniques. |

cellular telecommunications using CDMA, GSM, and evolving 3G protocols; and personal area communication using Bluetooth, ZigBee, or ultra-wideband techniques. The future will inevitably bring even more capabilities and IP-based services.

First responders need enhanced mobile devices that leverage industry standards to provide secure, scalable, and interoperable communication architectures. In addition, devices need to have a small form factor and be upgradeable, preferably over the air. Approaches that rely on hardware alone do not meet these requirements because adding hardware-based interfaces increases size and weight. Moreover, hardware cannot be modified over the air. Consequently, radio systems will rely increasingly on software. An ideal software radio will be able to switch between all of the air interface protocols discussed on a single platform. The devices might also employ adaptive or cognitive radio technology that senses the spectrum environment and automatically makes choices for the user to optimize the user's communications objectives (e.g. associating with a local Wi-Fi access point when a WiMAX connection is no longer available).

The flexibility of Software Defined Radios (SDRs) also introduces a significant security risk. In particular, when radio systems are software defined, they are vulnerable to software virus attacks. To modify a hardware radio, the attacker must physically touch each device and must have some level of radio expertise. In SDR systems, the potential exists for an attacker to disable thousands of radios over the air using automated tools acquired on publicly accessible web sites.

To counter this threat, SDRs can be designed to authenticate mobile code using digital signature technology. DHS personnel, for example, might only download and execute radio software that has been digitally signed by a DHS authority that vouches for its reliability. SDR platforms can also benefit from isolation kernels and operating systems that can partition computing resources to limit the impact of malicious code. Finally, trusted computing technologies, such as platform attestation and sealed storage, allow network

managers to ensure that only terminals with approved software loads are operating on the network.

## 4 RESEARCH DIRECTIONS

The Internet is the largest system ever built by, and leveraging the Internet's security protocols not only improves interoperability but also improves the public's ability to react and protect against new threats. If a transport medium employs its own unique security protocols, adversaries will quickly adapt and attack a network where it is most vulnerable. Strong physical security or wired encryption is ineffective if the extended wireless network employs untested or weak security controls. Research and development is ongoing and advancing in the wireless security industry. Grants and loans by federal agencies encourage technological advances, help promote economic growth, and encourage international trade.

### 4.1 Intrusion Prevention Systems

As vendors continue to offer all-in-one security solutions, the gap between wired and wireless IPS solutions should narrow. Monitoring the wireless medium alone will not properly safeguard an infrastructure from threats. One current trend is that wireless hardware vendors are partnering with wireless IPS software providers to help meet NIAP Common Criteria Certification as required by the DoD.

### 4.2 Internet-Based Security Protocols

Wireless standards that do not support IP hinder progress and may not provide holistic security or interoperability. Even the well-entrenched LMR (P25) market has started to embrace IP communications. Key and identity management will not be ubiquitous until wireless technologies agree on a common approach or leverage an existing solution, such as Internet public key infrastructure (PKI) or DoD PKI infrastructure. Key generation/distribution dissemination between multiple organizations remains a challenge for a number of reasons, that is, constrained by both technology and bureaucracy.

In addition, an addressing scheme (i.e. a subscriber number) may better enable first responders and law enforcement personnel (federal, state, local, and tribal) to intercommunicate. For example, an IP (or VoIP) Private Branch Exchange (PBX) can incorporate cellular and other IP-enabled devices into a department's in-house telephone switching system, that is, increasing information sharing.

### 4.3 Overlaying Security Services over IP-based Access Networks

When Transmission Control Protocol (TCP)/IP is used as the ubiquitous transport medium, wired and wireless devices can securely communicate if all devices employ the same effective security protocol. For example, personal digital assistants (PDAs) loaded with a secure application on one device can automatically detect and communicate securely with instances of the same application on other devices in network.

IMS is a standardized networking architecture that provides IP-based services through mobile and fixed networks. Mentioned earlier, IMS is agnostic to access technology and

can therefore operate with any endpoint that supports IP capabilities. The service-oriented architecture of IMS facilitates the development of new services while supporting legacy systems. IMS uses open standard IP protocols, defined by the Internet Engineering Task Force (IETF). Therefore, sessions between two IMS users, between an IMS user and a user on the Internet, and between two users on the Internet are established using exactly the same protocol. IMS bridges the interoperability gap of disparate wireless networks by operating with any endpoint that supports IP capabilities.

### 4.4 Mobile Device Security

Improvements in PED processing power coupled with decreased power requirements should be exploited to provide more advanced device security. Mobile devices have four general categories of risk: device access, data storage, data transmission, and data access. Technological advances should be leveraged to comply with Homeland Security Presidential Directive (HSPD-12), and personal identity verification (PIV) solutions that already exist should be explored and implemented where appropriate, such as, the DoD's PKI for the common access cards program. Greater cooperation and information sharing between civilian and defense agencies can help facilitate many legislative requirements focused on information security and empower our country to react better to natural and man-made disasters.

## REFERENCES


1. 3GPP, *3GPP Specification Series*, 3GPP, http://www.3gpp.org/ftp/Specs/html-info/33-series.htm.
2. Rose, G. (2004). *Access Security in CDMA2000, Including a Comparison with UMTS Assess Security, IEEE Wireless Communications*. February.
3. Hart, J. W., Imel, K. J., Powell, J., Tom, T., and Funk, D. (2003). *Understanding Wireless Communications in Public Safety*.
4. TIA (2002). *Standard: Digital Land Mobile Radio, Security Services Overview*, TIA-102.AAAB, Telecommunications Industry Association, Virginia, August 2002.
5. TIA/EIA (2002). *Standard: Project 25, Block Encryption Protocol*, TIA-102.AAAD, Telecommunications Industry Association, Virginia, July 2002.
6. TIA/EIA (2001). *Standard: Project 25, Digital Radio Over-the-Air Reykeying (OTAR) Protocol*, TIA-102.AACA, Telecommunications Industry Association, Virginia, April 2001.
7. TIA/EIA (2000). *Standard: Data Overview—New Technology Standards Project—Digital Radio Technical Standards*, TIA-102.BAEA-2000, Telecommunications Industry Association, Virginia, March 2001.
8. Barber, G., Bunn, L., Eydt, B., Karygiannis, T., and Phillips, T. (2007). NIST 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*.
9. ANSI/IEEE (1999). *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, ANSI/IEEE Std 802.11, 1999 Edition.
10. Arbaugh, W. A., Shankar, N., Wan, Y. C. J., and Zhang, K. (2002). Your 802.11 wireless network has not clothes. *Wireless Commun., IEEE* **9**(6), 44–51.
11. Aime, M. D., Calandriello, G., and Lioy, A. (2007). Ependability in wireless networks: can we rely on WiFi? *IEEE Security Privacy* **5**(1), 23–29.
12. Arbaugh, E. (2003). *Real 802.11 Security*, Addison-Wesley Longman Publishing Co., Inc., Boston, MA.

13. Frankel, S., Eydt, B., Owens, L., Kent, K. (2006). *Guide to IEEE 802.11i: Establishing Robust Security Networks*, National Institute of Standards and Technology Draft Special Publication, 800-97. June. Gaithersburg, MD.

14. National Institute of Standards and Technology (2001). *Announcing the Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication, 197. Gaithersburg, MD.

15. IEEE (2004). *IEEE Standards for Local and Metropolitan area Networks—Port-Based Network Access Control*, IEEE Std. 802.1X, 2004 Edition.

16. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and Levkowetz, H. (2004). *Extensible Authentication Protocol*, Network Working Group, p. 3748. Request for Comments.

17. Koien, G. M. (2007). *Public Information Collection Requirement Submitted to OMB for Emergency Review and Approval*, August 30, 2007. http://a257.g.akamaitech.net/7/257/2422/01jan20071800/edocket.access.gpo.gov/2007/E7-17507.htm.

18. American National Standards Institute (2008). *Emergency Communications Standardization, ANSI Homeland Security Standards Panel*, April 2008. http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/Homeland%20Security%20Standards%20Panel/Workshop%20Reports/Emergency%20Communications.pdf.

19. National Institute of Standards and Technology (2008). *NIST Special Publications, Computer Security Division: Computer Security Resource Center*, http://csrc.nist.gov/publications/nistpubs/.

20. National Institute of Standards and Technology (2008). *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules, Cryptographic Module Validation Program*, http://csrc.nist.gov/cryptval/140-1/140val-all.htm.

21. (2006). IP multimedia subsystems (IMS): a standardized approach to All-IP converged networks. *Bechtel Commun. Tech. J.* **4**(1), 13–36.

22. Shirey, R. (1997). *Internet Security Glossary*, Network Working Group, p. 2828. Request for Comments. Gaithersburg, MD.

## FURTHER READING

Ahson, S. A., and Ilyas, M. (2007). *WiMAX Handbook*, CRC Press, New York.

American National Standards Institute (2008). *Emergency Communications Standardization, ANSI Homeland Security Standards Panel*, April 2008. http://publicaa.ansi.org/sites/apdl/Documents/Standards%20Activities/Homeland%20Security%20Standards%20Panel/Workshop%20Reports/FPIC website. http://www.dhs.gov/xprepresp/committees/gc 1170097478666.shtm. Harte, L. *GSM Overview: Introduction to GSM: Physical Channels, Logical Channels, Network, and Operation.* USA. Heine, G. *GSM Networks: Protocols, Terminology, and Implementation.* USA. Final%20Report%20from%20ANSI-HSSP%20EC%20Workshop.pdf.

IEEE 802 LAN/MAN Standards Committee http://ieee802.org/.

IEEE 802.11 Working Group for WLAN Standards, http://grouper.ieee.org/groups/802/11/.

IEEE 802.16 Working Group on Broadband Wireless Access Standards, http http://grouper.ieee.org/groups/802/16/.

IEEE 802.20 Mobile Broadband Wireless Access (MBWA), http://grouper.ieee.org/groups/802/20/.

IEEE 802.21 Media Independent Handover Services, http://grouper.ieee.org/groups/802/21/.

National Institute of Standards and Technology. *Federal Information Security Management Act Implementation Project*, Computer Security Division: Computer Security Resource Center. http://csrc.nist.gov/sec-cert/.

Potter, B. (2003). Wireless security's future. *Security & Privacy Magazine, IEEE* **1**(4), 68–72.

Project 25, Project 25 Technology Interest Group, http://www.project25.org/modules.php?name=Content&file=viewarticle&id=2.

The Global Standards Collaboration, http://www.gsc.etsi.org/.

Wi-Fi Alliance, http://www.wi-fi.org.

# ENERGY SYSTEMS

# COMPARATIVE RISK ASSESSMENT FOR ENERGY SYSTEMS: A TOOL FOR COMPREHENSIVE ASSESSMENT OF ENERGY SECURITY

PETER BURGHERR AND STEFAN HIRSCHBERG
*Paul Scherrer Institut (PSI), Laboratory for Energy Systems Analysis, Villigen PSI, Switzerland*

## 1 INTRODUCTION

Disasters and accidents occur as a consequence of the exposure of people and their socioeconomic activities to natural and man-made hazards [1–4]. The increase in the numbers and associated consequences of natural disasters and man-made accidents in the last three decades as well as the recurring occurrence of single devastating catastrophes in recent years [5–7] have made the issues of disaster and risk management a top priority at national and international levels. Large loss events cannot be addressed as isolated events anymore because they provide a potential threat to people's health and property, the supply of economic goods and services, and the degradation of ecosystem functions, fauna, and flora. Also, societal vulnerability has further increased because of the steady growth of industrialization, continuing rapid urbanization, the disproportionately high development of coastal and other risk-prone areas, and strong dependency on complex, interrelated infrastructures, constituting a serious challenge to society and its sustainable development [8–12].

Disasters are generally assigned to two principal categories, that is, natural or man-made (anthropogenic or human induced). Natural disasters can be further classified into several distinct groups, including geological (e.g. earthquake and volcano), hydrometeorological (e.g. flood and wind storm), and other (e.g. heat wave, drought, forest fire, and avalanche) disasters. For a more detailed overview, see, for example, the classification schemes used by the Center for Research on the Epidemiology of Disasters (CRED) [13] or international reinsurance companies [6, 7]. Man-made disasters are the result of accidental or intentional human action. Accidental events include transportation accidents, major fires and explosions, releases of chemical and toxic substances, and the

collapse of technical structures (e.g. buildings, bridges, and dams). Purposed malicious action ranges from vandalism and sabotage to terrorism and war.

In the literature, a large variety of more or less precise definitions of the term *risk* can be found, depending on the field of application, and the specific scope, objective, and boundary conditions of the object under study. In engineering and natural sciences, risk is frequently defined in a quantitative way: *risk (R) = probability (p) × consequence (C)*. This definition does not include subjective factors of risk perception and aversion, which can also influence the decision-making process, that is, stakeholders may make trade-offs between quantitative and qualitative risk factors [14]. Quantitative risk assessment is of critical importance in several risk-sensitive industries. Concerning the energy sector, a comprehensive and objective risk evaluation is essential [5] because its complex and interdependent technical systems and facilities comprise critical infrastructure elements to today's information society [11, 15]. Potential accidental events could result in highly undesirable outcomes, calling for an accurate risk assessment and management [16].

In the context of security, risk is often defined as a function of the three variables threat ($T$), vulnerability ($V$), and consequence ($C$): $R = T \times V \times C$. Threat is the measure that a specific accidental or intentional event will take place. Vulnerability is the measure of likelihood that various types of safeguards fail. Consequence is the magnitude of negative effects in the case of an accident or successful attack. This approach allows the identification of areas where high threat levels, extreme vulnerabilities, and high consequences overlap. It is this intersection that causes security concerns. Figure 1 provides an overview of the different aspects of each of the three elements.

Although accidents in the energy sector have been shown to form the second largest group (after transportation) of man-made accidents, their level of coverage and completeness is not satisfactory because they are commonly not surveyed and analyzed separately; rather they are implicitly included as one subgroup of technological accidents. In the early 1990s, the Paul Scherrer Institut (PSI) has developed and established the database ENSAD (*en*ergy-related *s*evere *a*ccident *d*atabase) to close this gap [17]. The focus was on severe accidents because they are viewed controversially by the public and in the energy policy debate, although the sum of smaller accidents is substantial. Furthermore, in relative terms, scarce major accidents have a higher probability of being reported and scrutinized than the much more frequent smaller accidents with minor damages [18, 19]. Since its first publication [17], ENSAD has been continuously maintained, updated, and extended in its content, coverage, and scope [5, 20]. Major progress has been achieved within the "China Energy Technology Program (CETP)" [21–23], the European Union (EU) research project on "New Elements for the Assessment of External Costs from Energy Technologies" (NewExt) [5], and a study of natural gas accident risks for the Swiss Gas and Water Industry Association (SVGW) [24]. Most recently, the database was updated and further extended within the Integrated Project "New Energy Externalities Developments for Sustainability" (NEEDS) of the EU 6th Framework Programme.

The comparative assessment of energy-related accident risks has received increased attention in the past few years for several reasons. The general increase in the annual number of accidents and accompanying damages has triggered public awareness. In addition, a number of extremely devastating disasters have amplified this trend, and at the same time the world-leading reinsurance companies have published damage claims that are one of a kind. Furthermore, there are indications that global climate change may lead to future changes in the intensity and frequency of some hazards. In summary, mankind is facing a tremendous challenge to prevent large-scale disasters and/or to mitigate their

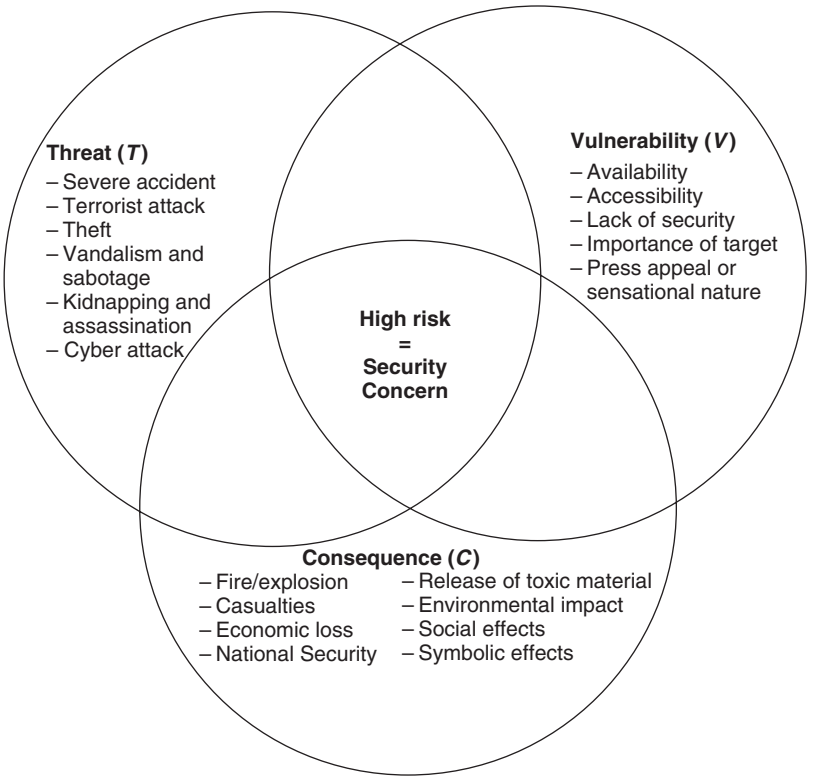



**FIGURE 1** The Venn diagram for security risk shows the various aspects of the three elements threat, vulnerability, and consequence.

impacts because they form a potential threat to the cohesion of society and its sustainable development goals.

However, recent experience has shown that it is not sufficient to direct our efforts only to the energy sector itself. On the one hand, energy provides critical inputs in the production of most goods and services, making them a key driver for all kinds of activities in modern society. On the other hand, the functioning of the energy infrastructure is likewise strongly dependent on supporting infrastructures, including availability and replacement of components, transportation, information and telecommunication systems, fuel and water supply, financial services, and so on. In this context, critical infrastructures denote vital systems that are characterized by mutual interdependencies essential for the provision of minimal services of the economy and government [11, 25, 26]. Parallel to the development of concepts for critical infrastructure protection (CIP), the concept of resilience has been applied to accident prevention, disaster management, and sustainable development [27–29]. Finally, the growing threat of international terrorism since the second half of the 1990s has led to the incorporation of CIP and civil emergency planning (CEP) issues into the broader context of homeland security, addressing a number of key aspects of the above-described methodological approaches and concepts [30–33].

This article provides a comprehensive, state-of-the-art analysis of severe accident risks in the energy sector. The methodological framework for the comparative assessment is presented, followed by an overview of the historical experience as represented in

ENSAD. Finally, comparisons of energy chains are based on aggregated indicators and frequency–consequence ($F-N$) curves, two well-established analytical methods.

## 2 ANALYTICAL APPROACH AND METHODOLOGY

### 2.1 Severe Accident Database

In the initial development phase of ENSAD, the requirements and time exposure were examined to build up a severe accident database for the energy sector. These preliminary investigations clearly showed that such a database should not be set up from the scratch, but rather by using existing information sources, because none of the available individual databases offers a fully satisfactory coverage to form alone a basis for the evaluation of severe energy-related accidents. Databases also differ in their scope, information coverage, level of detail, and quality. Therefore, the combination of information from a large variety of sources allows for the most complete compilation of accident records in terms of available information, level of detail, data quality, time period, and geographical coverage. Additionally, commercial databases should also be included to gain access to proprietary data that are not fully contained in publicly available information sources.

Figure 2 shows the information sources used to document energy-related accidents included in ENSAD for the years 1969–2000. The four most common sources summed up to 48.5%, followed by seven other sources that cumulatively contributed 22.6%. The remaining more than 170 sources amounted to about 29%. However, many of the sources with small shares were of critical importance because they covered specific energy

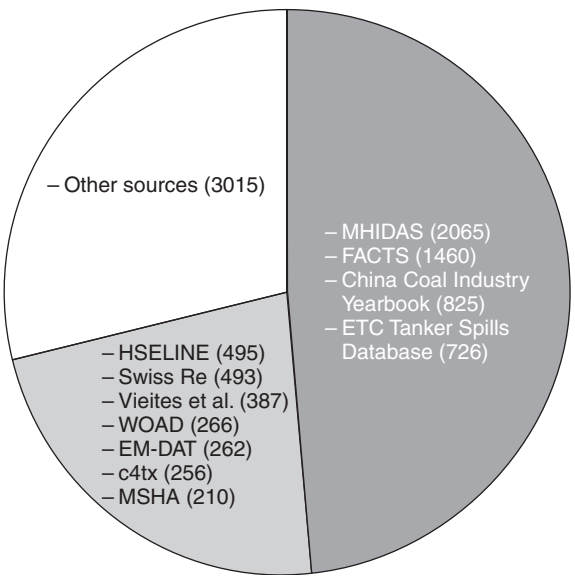



**FIGURE 2** Contributions of major sources to the total number of energy-related accidents stored in ENSAD for the years 1969–2000. Note that the total number of accidents sums up to more than the 6227 accidents documented in ENSAD because a specific accident may be reported by several sources.

chains and/or countries, were useful to resolve contradicting statements, and provided supplementary information that would otherwise not be available.

A database of the purpose such as ENSAD has to be based on relational database software to keep the amount of redundant information at a minimum level, which is not possible with a traditional spreadsheet approach. In our case, Microsoft Access was chosen because it meets our objectives and needs, and allows flexible programming based on SQL or Visual Basic applications. Its abounding export options facilitate data exchange with statistical software packages, the coupling with geographic information systems (GIS), and integration with other office software, internet, or intranet applications. The complete process of database building and implementation has been described in detail elsewhere [5, 17]; therefore, only an overview of the essential steps is provided here:

1. Selection and survey of relevant information sources. Criteria for acquisition include that retrieved data are of sufficient quality in terms of detail and accuracy.
2. Raw information is merged, harmonized, checked for inconsistencies, and verified before records are included in ENSAD.
3. Energy-related accidents are assigned to a specific energy chain and to a specific step within the selected chain. Information on date of occurrence, geographic location and site specification, country-specific attributes, accident type classification, technological characteristics, damage assessment, accident analysis, and verbal description is then collected and entered in ENSAD.
4. The database content of ENSAD is once more cross-checked to keep data errors at the lowest feasible level.
5. Comparative evaluations are then carried out on the basis of customized ENSAD queries.

### 2.2 Severe Accident Definition

In the literature, no unambiguous definition of the term *severe accident* can be found. Differences concern the actual damage types considered (e.g. fatalities, injured persons, evacuees, or economic costs), use of loose categories such as "people affected", and differences in damage thresholds to distinguish severe from smaller accidents.

This can be illustrated by the following examples. The "Worldwide Offshore Accident Database (WOAD)" of the Det Norske Veritas [34] considers an accident as severe or major, if more than one fatality occurred or if the damaged unit (e.g. oil platform, drill ship, or drill barge) experienced total loss. Glickman and Terry [35] define a significant accident for technological hazard, if it resulted in at least five fatalities or if it involved the release of a chemical, petroleum product, hazardous waste, or other hazardous material. The SIGMA publication series of Swiss Re Company [7] does not use the term *severe accidents*, but rather refers to catastrophic events.

The database of ENSAD uses seven criteria to distinguish between severe and smaller accidents. Whenever an accident is characterized by one or more of the following consequences, it is considered to be severe:

1. at least five fatalities;
2. at least 10 injured;
3. at least 200 evacuees;

4. extensive ban on consumption of food;
5. releases of hydrocarbons exceeding 10,000 (metric) tones (t);
6. enforced clean-up of land and water over an area of at least 25 $km^2$; or
7. economic loss of at least 5 million USD (2000).[1]

Generally, fatality data is most reliable, accurate, and complete, whereas in the case of injured or evacuated persons, details on the severity of an injury or the duration of an evacuation are frequently not clearly indicated. The estimation of precise values for economic loss is often difficult because different sources of information report various types of economic damages (e.g. insured vs. total loss), depending on their specific scope (e.g. insurance company vs. disaster recovery organizations). The other consequence indicators are either only relevant for specific energy chains or ENSAD contains very few entries with sufficiently detailed information. Therefore, ENSAD-based results presented here are focused on the number of fatalities.

### 2.3 Consideration of Full Energy Chains

The ENSAD database allows carrying out comprehensive analyses of accident risks that are not limited to power plants but cover full energy chains. Such a broader perspective is essential because for the fossil chains, accidents at power plants play a minor role compared to the other chain stages, that is analyses based on only power plants would radically underestimate the real situation [17].

In general, an energy chain may comprise the following stages: exploration, extraction, transports, storage, power and/or heat generation, waste treatment, and disposal. However, one should be aware that not all these stages are applicable to every energy chain. Table 1 gives an overview of distinct stages for the major fossil (coal, oil, natural gas, and liquefied petroleum gas (LPG)), hydro, and nuclear chains.

### 2.4 Normalization and Allocation of Damages

Comparisons of the various energy chains were based on data normalized to the unit of electricity production. For fossil energy chains, the thermal energy was converted to an equivalent electrical output using a generic efficiency factor of 0.35. For nuclear- and hydropower, the normalization is straightforward since in both cases the generated product is electrical energy. The gigawatt-electric-year ($GW_e$yr) was chosen because large individual plants have capacities in the neighborhood of 1 GW of electrical output ($GW_e$). This makes the $GW_e$yr a natural unit to use in discussions of total electricity production.

Results are provided separately for OECD (Organization for Economic Co-operation and Development) and non-OECD countries because of large differences in levels of technological development and safety performance. This distinction is also meaningful because of the substantial differences in management, regulatory frameworks, and general safety culture between these two groups of countries [5, 17, 36, 37]. Analyses were complemented by separate calculations for the Chinese coal chain. In the case of China, coal chain data were analyzed only for the years 1994–1999 when data from the China

[1]Different currencies were all converted to USD values. To take account of inflation, specific amounts were extrapolated using the US Consumer Price Index (CPI) to obtain year 2000 values.

**TABLE 1 Chain Stages of Major Energy Chains. Based on Hirschberg et al. [17]**

| | Coal | Oil | Natural Gas | LPG | Nuclear | Hydro |
|---|---|---|---|---|---|---|
| Exploration | Exploration | Exploration | Exploration | - | Exploration | |
| Extraction | Mining and Coal Preparation | Extraction | Extraction and Processing | - | Mining/Milling | |
| Transport | Transport to Conversion Plant | Transport to Refinery (Long Distance Transport) | Long Distance Transport (Pipeline) | - | Transport | |
| Processing | Conversion plant | Refinery | | • Refinery<br>• Natural gas processing Plant | Upstream Processing | |
| Transport | Transport | Regional Distribution | Distribution:<br>- Long Dist.<br>- Regional<br>- Local | Distribution:<br>- Long Dist.<br>- Regional<br>- Local | Transport | |
| Power/Heat Generation | Power Plant/Heating Plant | Power Plant/Heating Plant | Power Plant/Heating Plant | Heating Plant | Power Plant | Power Plant |
| Transport | | | | | Transport to Reprocessing Plant | |
| Processing | | | | | Reprocessing | |
| Waste Treatment | Waste Treatment | | | | Waste Treatment | |
| Waste Disposal | Waste Disposal | | | | Waste Disposal | |

Coal Industry Yearbook were available, indicating that previous years were subject to substantial underreporting [21–23].

A difficulty that arises in comparative studies with aggregated normalized severe accident records is that a large number of severe accidents occur in non-OECD countries at stages in the energy chain relevant for the export to OECD countries. This can be incorporated in the calculations by adding the appropriate share of the consequences of accidents that occurred at such energy chain stages in non-OECD countries to the damages that physically occurred in OECD countries, that is, OECD countries "import" fatalities. The net amounts of energy carriers imported to OECD countries from non-OECD countries form the basis for this allocation procedure, which has been described in detail in Hirschberg et al. [17]. It has been shown that OECD countries import from non-OECD countries a large fraction of their total consumption of crude oil and LPG, a small fraction of natural gas, and a negligible fraction of coal [5]. Aggregated indicators with allocation are particularly useful within a sustainable development perspective because they assume that the industrial OECD countries should bear a certain share of these damages.

## 2.5 Simplified Probabilistic Safety Assessment for Nuclear Power Plants

The simplified approach used by us in comparative risk studies is described in detail in [22, 23]. It builds on adapting plant-specific source terms from publicly available Level II probabilistic safety assessment (PSA) and combining them with a simplified assessment of off-site consequences resulting from hypothetical nuclear accidents. The basis for the methodology is calculations carried out using MACCS2 consequence code for the same light water reactor (LWR) plant and for two hypothetical accidents, one with early containment rupture and the other with a late vented release. Data for two different sites are used for the dispersion and dose calculations, the first a European continental site with relatively large population density in the vicinity of the plant, and the other a US site with relatively low population density within the first 10 km.

Early fatalities can be extrapolated from one site to another from the ratio of population within 8–10 km. This is because the radioactive content in a passing cloud is effectively dispersed over a very large volume very quickly (the MACCS2 code uses a Gaussian dispersion model), and the MACCS2 calculations show that mortality distance does not exceed 20 km under the worst possible weather conditions (i.e. with very small probability).

Delayed cancer deaths are found to be strongly correlated with the total population within 80–120 km. The MACCS2 calculations show that only a small background of delayed fatalities may occur beyond this distance. This is due to cloud dispersion and dilution of activities, since the dose must be incurred via inhalation or submersion in the passing cloud. Cancer deaths occurring from ingestion (late deaths) are found to be correlated with the total population around the site considered. For both the sites, a maximum distance of 800 km was considered; therefore, late deaths are considered proportional to the ratio of populations within 800 km.

Finally, land contamination is assumed to be correlated with the ratio of land fractions to 120 km, even though the correlation was found to be weaker than the ones found for health effects. A distance of 120 km is assumed for this type of calculations, because the MACCS2 results show that the maximum distance where land can be severely contaminated does not exceed 120 km for any of the radionuclide groups.

In conclusion, off-site consequences may be calculated approximately using activity of releases, as provided by Level II PSAs for the relevant source terms and the ratios discussed above.

## 3 OVERVIEW AND CONTENTS OF ENSAD

Currently, 18,706 accident records are stored in the ENSAD database, of which 88.4% fall in the period between 1969 and 2000. Within this period, 6995 accidents were considered severe because they resulted in at least five fatalities. Of these accidents, 39.5% were natural disasters and the other 4233 were man-made accidents. The latter can be further divided into energy-related accidents (1870 or 44.2%) and other man-made accidents (2363 or 55.8%). Figure 3 shows fatalities in all categories of severe (≥5 fatalities) man-made accidents and natural disasters from 1969 to 2000, totaling to about 3.4 million fatalities. Of these victims, more than 90% were due to natural catastrophes and about 10% were due to severe man-made accidents; 37% of the latter were killed in energy-related accidents.

The largest natural disasters were a storm and flood catastrophe in Bangladesh in 1970 (300,000 fatalities), the Tangshan earthquake in China in 1976 (290,000), and a drought and civil strife in Sudan in 1983 (250,000). In contrast, the largest man-made accidents resulted in fatalities one to two orders of magnitude lower. The top-ranked energy-related accidents include the Banqiao/Shimantan dam failure in China in 1975 (26,000 fatalities), the collision of the tanker "Victor" with the Ferry "Dona Paz" off the Philippines in 1987 (4386), and a tank truck collision with another vehicle in the Salang

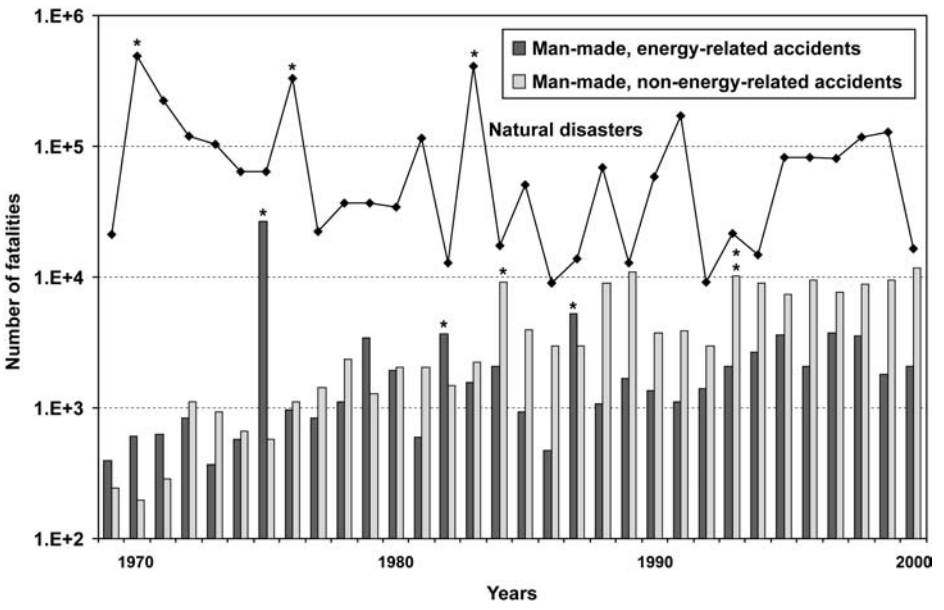



**FIGURE 3** Number of fatalities for severe (≥5 fatalities) accidents that occurred due to natural disasters and man-made accidents in the period 1969–2000. Years marked by an asterisk indicate the three most deadly accidents per category, which are also described in the text.

tunnel in Afghanistan's Parvan province in 1982 (2700). Furthermore, 9 out of the 10 most deadly accidents in the energy sector occurred in non-OECD countries, and were attributable to oil and hydro chains. Large nonenergy-related severe accidents include the accident at a pesticide plant in Bhopal in India in 1984 (5000 fatalities), the sinking of the ferry "Neptune" near the coast of Haiti in 1993 (1800), and the failure of the Gouhou dam (primary purpose: irrigation and water supply) in China in 1993 (1250).

For the period 1969–2000, the ENSAD database comprises 1870 severe accidents attributable to the energy sector, with a corresponding total of 81,258 fatalities (Table 2). The coal chain accounted for 65.3% of all accidents, with oil a distant second at 21.2%. Contributions by the natural gas (7.2%) and LPG (5.6%) chains were much less, while both hydro and nuclear account for less than 1% each. This dominance of coal chain accidents is fully attributable to the release of detailed accident statistics by China's coal industry, data that were not previously publicly available [21–23]. Altogether, 819 of the 1044 accidents collected for the Chinese coal chain occurred in the years 1994–1999, implying substantial underreporting prior to the release of the annual editions of the China Coal Industry Yearbook. Fatalities were clearly dominated by the Banqiao/Shimantan dam failures, which together resulted in 26,000 deaths. As a consequence, the hydro chain accounts for 36.8% of all fatalities. Among the fossil chains, coal accounted for the most fatalities, followed by oil, LPG, and natural gas.

Cumulated numbers of accidents for the different fossil energy chains were plotted on a world map for each country to visualize spatial distribution patterns and to identify accident hotspots (Figure 4). Additionally, total fatalities and chain contributions are shown for the top 10 countries in terms of fatalities, and for each energy chain the most deadly accident is indicated. Among the countries with highest death tolls, seven of them were non-OECD countries and only three belonged to the OECD countries. However, Mexico and South Korea gained OECD membership only in the mid 1990s (1994 and 1996, respectively), whereas United States has been a member since OECD's foundation in 1961. China was the most accident-prone country with 19,141 fatalities, of which

**TABLE 2 Summary of Numbers (acc) and Fatalities (fat) of Severe (≥5 fatalities) Accidents for the Different Energy Chains and Country Groups for the Years 1969–2000**

| | OECD | | Non-OECD | | Worldwide | |
|---|---|---|---|---|---|---|
| Energy chain | Acc | Fat | Acc | Fat | Acc | Fat |
| Coal | 75 | 2259 | 102 | 4831 | 1221 | 25,107 |
| | | | 1044 | 18,017 | | |
| | | | 819[a] | 11,334[a] | | |
| Oil | 165 | 3713 | 232 | 16,505 | 397 | 20,218 |
| Natural gas | 90 | 1043 | 45 | 1000 | 135 | 2043 |
| LPG | 59 | 1905 | 46 | 2016 | 105 | 3921 |
| Hydro | 1 | 14 | 10 | 29,924[b] | 11 | 29,938 |
| Nuclear | 0 | 0 | 1 | 31[c] | 1 | 31 |
| Total | 390 | 8934 | 1480 | 72,324 | 1870 | 81,258 |

[a]Three values (first to third line) are given for the coal chain in non-OECD countries: non-OECD without China, China 1969–2000, and China 1994–1999 (see text).
[b]Banqiao/Shimantan dam failures together caused 26,000 fatalities.
[c]Only immediate fatalities, see text for latent fatalities.

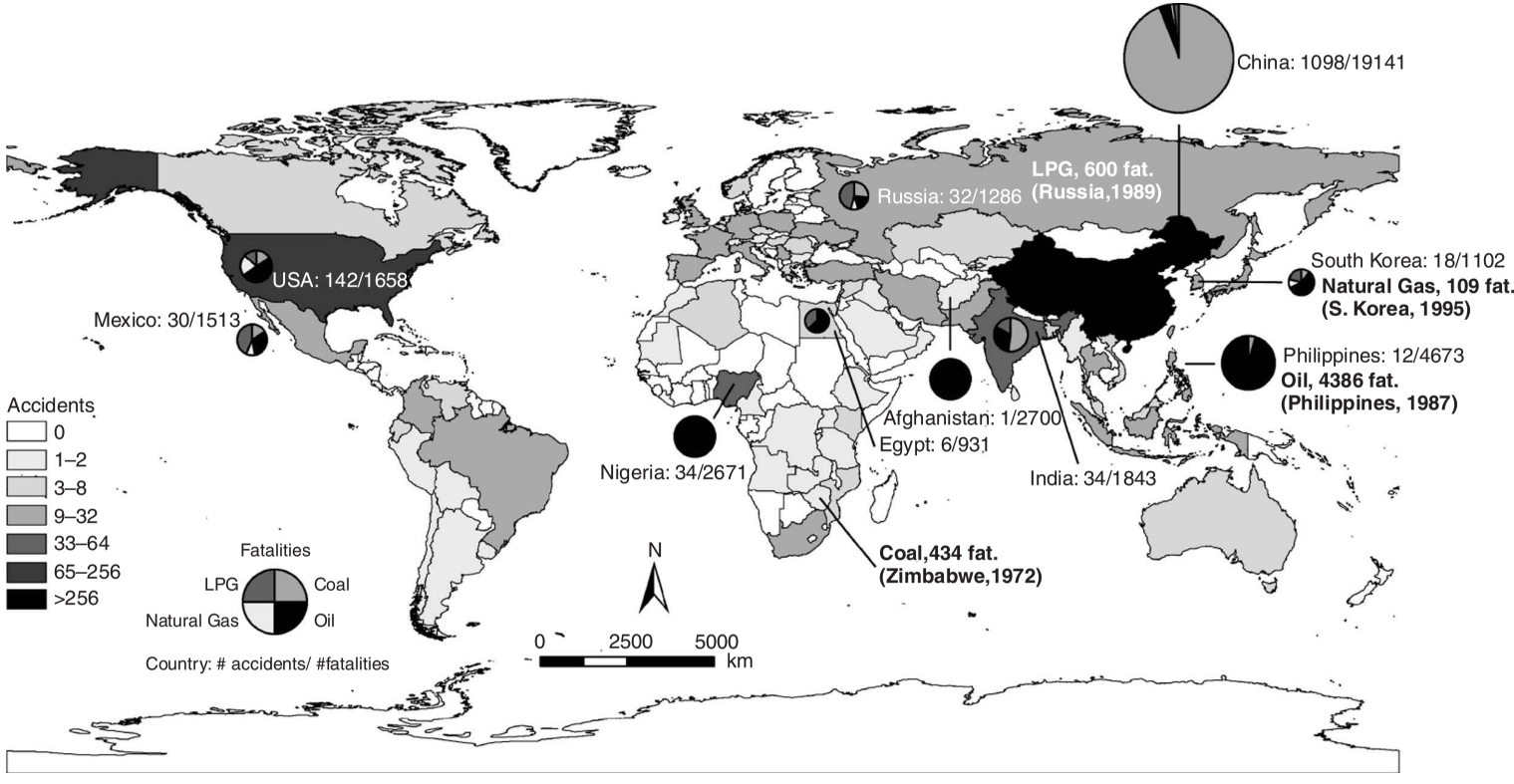



**FIGURE 4** Individual countries are shaded according to their total number of severe accidents in fossil energy chains (coal, oil, natural gas, and LPG) for the period 1969–2000. Pie charts show the contributions per chain for the top 10 countries in terms of fatalities. The most deadly accident for each chain is also indicated.

18,017 fatalities occurred in 1044 accidents attributable to the coal chain, but only nine of these resulted in 100 or more fatalities (Table 2). In contrast, the cumulated fatalities of the Philippines, Afghanistan, Nigeria, India, Mexico, Russia, South Korea, and Egypt were strongly influenced by a few very large accidents that contributed a substantial share of the total [36, 37]. United States exhibited a distinctly different pattern compared to the other countries with no extremely large accidents (only 3 out of 142 with more than 50 fatalities), and over 70% of accidents and associated fatalities taking place in the oil and gas chains.

## 4 COMPARATIVE ANALYSIS OF ENERGY CHAINS

The majority of accidents in fossil energy chains do not occur in power plants, but rather in other stages in the energy chains (Table 3). Over 95% of the victims in the coal chain lose their lives in mines, primarily due to gas explosions. With oil, the transportation to the refinery and regional distribution is the most accident-prone stage; most frequent are tanker accidents at sea and road accidents involving tank trucks. Transportation

**TABLE 3 Relative Share of Accidental Fatalities in the Stages of Different Energy Chains**

| | Coal | Oil | NaturalGas | LPG | Hydro | Nuclear |
|---|---|---|---|---|---|---|
| **Exploration / Extraction** | Explosions and fires in mines | Well blowouts, accidents on drilling platforms at sea | Well blowouts, accidents on drilling platforms at sea | | | |
| **Long Distance Transport** | | Tanker accidents at sea | Pipeline accidents | Pipeline accidents, LPG tankers at sea | | |
| **Processing / Storage** | | Process accidents in refineries and tank farms | | Accidents at refinery / natural gas processing plants | | |
| **Regional / Local Distribution** | | Overturning and collisions of tank trucks | Pipeline accidents | Overturning and collisions of tank trucks | | |
| **Power / Heat Generation** | | | Process accidents | Process accidents | Overflow or failure of storage dam | Core meltdown with large release of radioactivity |
| **Waste Treatment / Disposal** | | | | | | |

| 0 – 5% | 6 – 15% | 16 –30% | 31 – 60% | 61 – 100% |
|---|---|---|---|---|

is also a weak stage in the natural gas chain, which is dominated by pipeline accidents in transmission (long distance) and distribution (regional/local) networks. In the LPG chain, transportation accidents are most prominent too, particularly in regional and local distribution. In contrast, hydropower and nuclear power accidents occur only near the area of the storage dam or reservoir and the plant site, respectively. While coal chain victims are almost exclusively work related, gas and oil accidents involve a significant number of innocent bystanders as victims. If a storage dam breaks, then the general populace is almost exclusively affected, with the exception of the dam operators. Nuclear plant accidents may also lead to immediate fatalities, but here the deaths are dominated by latent fatalities (compare Sections 3.1 and 3.2) due to eventual cases of cancer.

### 4.1 Aggregated Indicators

Aggregated fatality rates of severe ($\geq$5 fatalities) accidents are reported only for immediate fatalities, whereas the significance of latent fatalities in the case of the nuclear chain is discussed in Section 3.2. Damage rates differed substantially among energy chains and country groups, with OECD countries generally showing significantly lower fatality rates than non-OECD countries (Table 4). Among the fossil chains, natural gas has the best performance, followed by oil and coal, whereas the value for LPG is one order of magnitude worse. The lowest fatality values occur for western style nuclear and hydropower plants, whereas dam failures in non-OECD countries may lead to thousands of victims in the downstream population. Additionally, Table 4 also displays a full allocation of damages for fossil energy chains on the basis of imports and exports (Section 1.4) because a large number of severe accidents in non-OECD countries are related to energy exports to the OECD countries. Severe fatality rates for the oil and LPG chains exhibited the most distinct increase for OECD countries and decrease for non-OECD countries compared to the rates without allocation, whereas differences for coal and natural gas chains were

**TABLE 4 Aggregated Fatality Rates for Full Energy Chains Based on Historical Experience of Severe Accidents ($\geq$5 immediate fatalities) in OECD and Non-OECD Countries for the Period 1969–2000, Except for China 1994–1999 (compare text). Allocated Values Incorporate Imports and Exports between OECD and Non-OECD**

| | No Allocation/With Allocation [fatalities/$GW_e$yr] | |
|---|---|---|
| | OECD | Non-OECD |
| Coal | 0.157/0.163 | 0.597/0.589 |
| | | 6.169[a] |
| Oil | 0.132/0.390 | 0.897/0.502 |
| Natural gas | 0.085/0.097 | 0.111/0.096 |
| LPG | 1.957/3.317 | 14.896/5.112 |
| Hydro | 0.003 | 10.285 |
| | | 1.349[b] |
| Nuclear | — | 0.048[c] |

[a]First line: OECD without China; second line: China for the period 1994–1999.
[b]Chinese dam failures of Banqiao/Shimantan with a total of 26,000 fatalities are excluded.
[c]Only immediate fatalities of Chernobyl accident; see text for latent fatalities.

distinctly less. Within the framework of sustainable development, it could be argued that the highly industrialized OECD countries should assume a certain share of these damages.

### 4.2 Frequency–Consequence Curves

Figure 5 provides $F-N$ curves for severe ($\geq$5 fatalities) accidents in OECD and non-OECD countries, including allocated curves. For fossil chains in OECD countries, natural gas has the lowest frequency, coal and oil are intermediate, and LPG has the highest frequency, whereas hydro and nuclear chains perform significantly better. Maximum consequences are negligible for hydro, followed distantly by natural gas (109 fatalities), and the other fossil chains have maxima between 2.5 and 4.5 times greater than natural gas. Concerning allocated $F-N$ curves, those for natural gas are practically identical (not shown in figure), the allocated curve for LPG exhibits higher frequencies at corresponding numbers of fatalities, whereas for the oil chain maximum consequences increase by a factor of about 3.8. This is fully attributable to the extremely deadly accident in the Philippines with 4386 fatalities already discussed before.

Non-OECD countries showed a comparable ranking as for OECD countries, except for the Chinese coal chain that performed significantly worse. However, the frequencies at corresponding numbers of fatalities were generally higher for non-OECD countries compared to OECD countries. Additionally, values for maximum consequences were one order of magnitude higher for the oil chain (4386 fatalities) compared to OECD countries, and the Chinese dam failure of Banqiao/Shimantan with 26,000 fatalities is by far the most deadly accident in terms of immediate fatalities. Concerning allocated $F-N$ curves, the oil and LPG chains have clearly lower maxima, whereas curves for natural gas are again almost identical.

For nuclear energy, immediate fatalities play a minor role, whereas latent fatalities clearly dominate. Therefore, total fatalities are split into the following categories: early (immediate) fatalities that occur shortly after exposure and latent fatalities that include all potential deaths occurring within 70 years from the radioactive release. For details see Burgherr et al. [5] and Hirschberg et al. [17]. Accident frequencies causing actual damage external to the plant associated with the nuclear chain (Chernobyl) are relatively low, but the maximum credible consequences may be very large due to the dominance of latent fatalities. According to Hirschberg et al. [17], estimated latent fatalities due to delayed cancers range from about 9000 (based on dose cutoff) to 33,000 (entire northern hemisphere with no dose cutoff) over the next 70 years. In 2005, a study by the "Chernobyl Forum"—a consortium of several United Nations organizations, the World Bank and the Russian, Belarus and Ukrainian governments—estimated that in the areas with high contamination, up to 4000 people could eventually die due to radiation doses from the Chernobyl accident, most of them among the so called liquidators [38]. Because of the more limited area considered, this value is substantially lower than the PSI values previously mentioned. The upper range in PSI's estimate is conservative (as intended) because it was not limited to the most contaminated areas. Finally, one should be aware that no dependable statistics can be determined from this single, severe accident. The Chernobyl accident data also cannot be transferred to Western plants, because they use a very different technology. For realistic calculations, it is necessary to use PSA (Figure 5).

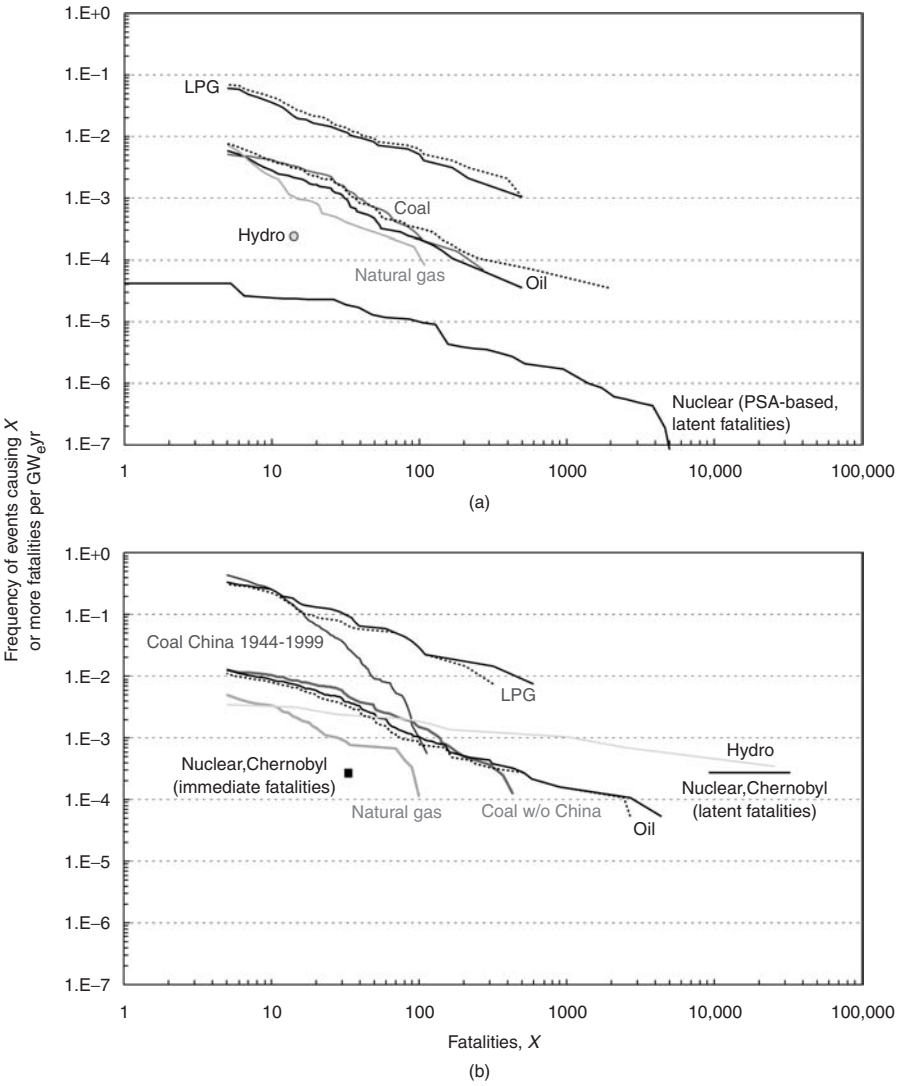



**FIGURE 5** Comparison of frequency–consequence curves for full energy chains based on historical experience of severe accidents in (a) OECD and (b) non-OECD countries for the period 1969–2000, except for China 1994–1999 (compare text). Dashed lines denote $F-N$ curves based on allocated values, that is, taking into account imports and exports between OECD and non-OECD countries. For natural gas, allocated curves are not shown as they are almost identical to nonallocated ones.

## 5 CONCLUSIONS AND RECOMMENDATIONS

### 5.1 Comparative Aspects

– The ENSAD database provides comprehensive accident data for the objective and quantitative analysis of specific technical aspects and the comparative assessment

of severe accident risks in the energy sector. However, it is in the nature of the topic that new accidents continuously occur; therefore, the ENSAD database needs to be maintained, updated, and extended to keep up with the growing historical experience and to provide state-of-the-art estimates of risk indicators.

– Energy-related accident risks in non-OECD countries are distinctly higher than in OECD countries; reflected by aggregated indicators as well as $F-N$ curves.
– The most accident-prone energy chain stages are upstream stages (i.e. extraction, refining, and transportation) in fossil energy chains, and hydropower in the less developed (non-OECD) countries.
– Expected fatality rates are lowest for Western hydropower and nuclear power plants. However, the maximum consequences can be very high. The associated risk valuation is subject to stakeholder value judgments and can be pursued in multicriteria decision analysis [39, 40].
– PSA perspective on severe accident risks is particularly important for energy chains whose risks are dominated by power plants, the historical experience of accidents is scarce, or its applicability is highly restricted. These conditions are valid for most Western hydro- and nuclear power plants.

## 5.2 Selected Future Developments

– Estimation of risk indicators for *future technologies* based on extrapolations of currently operating systems. This type of analysis has been introduced in the NEEDS Project of the EU 6th Framework Programme, and is further developed, systematized, and extended in several upcoming projects.
– Further advancement of the *simplified PSA approach* to establish a broader reference database for site-specific risk indicators for advanced nuclear designs has been initiated.
– Broader and *systematic evaluation of smaller accidents* in the fossil chains, as it has already been undertaken for natural gas [24]. Such an effort, however, requires access to the relevant raw data that are often subject to proprietary use.
– Qualitative analysis of *indirect impacts of accidents* on the energy sector. Besides the purely physical effects of severe accidents, a variety of indirect effects can occur, including environmental concerns (e.g. oil spills), acceptance problems of specific technologies due to extremely large maximum credible consequences or high accident frequencies, potential social conflicts among stakeholders (e.g. oil companies and local tribe communities in developing countries), and so on.
– Enhanced coupling of the ENSAD database with *Geographic Information System* (ArcGIS) together with multivariate statistical analyses to analyze spatial patterns across hierarchical scales.

## REFERENCES

1. Dao, H., and Peduzzi, P. (2004). Global evaluation of human risk and vulnerability to natural hazards. In *Proceedings from: EnviroInfo 2004 Conference*, Editions du Tricorne, Geneva, Vol. 1.

2. Dilley, M. (2006). Setting priorities: global patterns of disaster risk. *Philos. Trans. R. Soc. A* **364**, 2217–2229.
3. Lerner-Lam, A. (2007). Assessing global exposure to natural hazards: progress and future trends. *Environ. Hazards* **7**, 10–19.
4. UNDP (2004). *Reducing Disaster Risk: A Challenge for Development*, UNDP Bureau for Crisis Prevention and Recovery, New York.
5. Burgherr, P., Hirschberg, S., Hunt, A., and Ortiz, R. A. (2004). *Severe accidents in the energy sector. Final Report to the European Commission of the EU 5th Framework Programme "New Elements for the Assessment of External Costs from Energy Technologies" (NewExt)*, DG Research, Technological Development and Demonstration (RTD),Brussels, Online-Version under: http://www.ier.uni-stuttgart.de/public/de/organisation/abt/tfu/projekte/newext/newext_final.pdf.
6. Munich, R. (2007). *Topics Geo: Natural Catastrophes 2006—Analyses, Assessments, Positions*, Munich Re Group, Munich.
7. Swiss, R. (2008). *Natural Catastrophes and Man-made Disasters in 2007: High Losses in Europe. Sigma No. 1/2008*, Swiss Reinsurance Company, Zurich.
8. Barnett, J. (2003). Security and climate change. *Glob. Environ. Change* **13**, 7–17.
9. Beniston, M. (2007). Linking extreme climate events and economic impacts: examples from the Swiss Alps. *Energy Policy* **35**, 5384–5392.
10. Dilley, M., Chen, R. S., Deichmann, U., Lerner-Lam, A. L., Arnold, M., Agwe, J., Buys, P., Kjekstad, O., Lyon, B., and Yetman, G. (2005). *Natural Disaster Hotspots. A Global Risk Analysis*, Disaster Risk Management Series, No. 5. The World Bank, Hazard Management Unit, Washington, DC.
11. Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Syst. Mag*. **21**(6), 11–25.
12. WEF (2008). *Global Risks 2008—A Global Risk Network Report*, World Economic Forum, Cologny/Geneva.
13. EM-DAT (2008). *The OFDA/CRED International Disaster Database*, Retrieved from http://www.em-dat.net (January 2008).
14. Gregory, R., and Lichtenstein, S. (1994). A hint of risk: tradeoffs between quantitative and qualitative risk factors. *Risk Anal*. **14**(2), 199–206.
15. Gheorghe, A. V., Masera, M., Weijnen, M., and De Vries, L. J. (2006). *Critical infrastructures at risk. Securing the European Electric Power System*, *Series: Topics in Safety, Risk, Reliability and Quality*, Springer, Dordrecht, Vol. 9.
16. Flyvbjerg, B. (2006). From Nobel Prize to project management: getting risks right. *Proj. Manage. J*. **37**(3), 5–15.
17. Hirschberg, S., Spiekerman, G., and Dones, R. (1998). *Severe Accidents in the Energy Sector*, 1st ed., Paul Scherrer Institut, Villigen PSI, PSI Report No. 98-16.
18. Marshall, V. C. (1987). *Major Chemical Hazards*, Ellis Horwood Limited, Chichester.
19. van Beek, P. C. (1994). *Presentation of FACTS, A Database for Industrial Safety*, AC-Laboratorium, Spiez.
20. Hirschberg, S., Burgherr, P., Spiekerman, G., and Dones, R. (2004). Severe accidents in the energy sector: comparative perspective. *J. Hazard. Mater*. **111**(1–3), 57–65.
21. Burgherr, P., and Hirschberg, S. (2007). Assessment of severe accident risks in the Chinese coal chain. *Int. J. Risk Assess. Manage*. **7**(8), 1157–1175.
22. Hirschberg, S., Burgherr, P., Spiekerman, G., Cazzoli, E., Vitazek, J., and Cheng, L. (2003). Assessment of severe accident risks. In *Integrated Assessment of Sustainable Energy Systems in China. The China Energy Technology Program—A Framework for Decision Support in the*

*Electric Sector of Shandong Province*, *Alliance for Global Sustainability Series*, B. Eliasson, and Y. Y. Lee, Eds. Kluwer Academic Publishers, Amsterdam, Vol. 4, pp. 587–660.

23. Hirschberg, S., Burgherr, P., Spiekerman, G., Cazzoli, E., Vitazek, J., and Cheng, L. (2003). *Comparative Assessment of Severe Accidents in the Chinese Energy Sector*, Paul Scherrer Institut, Villigen PSI, *PSI Report No. 03-04*.
24. Burgherr, P., and Hirschberg, S. (2005). *Comparative Assessment of Natural Gas Accident Risks*, Paul Scherrer Institut, Villigen PSI, PSI Report No. 05-01.
25. IRGC Policy Brief (2007). *Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*, International Risk Governance Council, Geneva.
26. Jones, A. (2007). Critical infrastructure protection. *Comput. Fraud Secur*. **2007**(4), 11–15.
27. Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., Shinozuka, M., Tierney, K., Wallace, W. A., and von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra* **19**(4), 733–752.
28. Hollnagel, E. (2006). Resilience—the challenge of the unstable. In *Resilience Engineering: Concepts and Precepts*, E. Hollnagel, D. D. Woods, and N. Leveson, Eds. Ashgate, Aldershot.
29. Perrings, C. (2006). Resilience and sustainable development. *Environ. Dev. Econ*. **11**, 417–427.
30. Moteff, J., and Parfomak, P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification*, Congressional Research Service (CRS), The Library of Congress, Washington, DC.
31. The White House (2003). *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, The White House, Washington, DC.
32. The White House (2007). *National Strategy for Homeland Security*, Homeland Security Council, Washington, DC.
33. Willis, H. H., LaTourrette, T., Kelly, T. K., Hickey, S., and Neill, S. (2007). *Terrorism Risk Modeling for Intelligence Analysis and Infrastructure Protection. RAND Center for Terrorism Risk Management Policy for the Department of Homeland Security*, RAND Corporation, Santa Monica, CA.
34. DNV (1999). *Worldwide Offshore Accident Databank (WOAD)*, WOAD statistical report 1998. Det Norske Veritas AS, Hovik.
35. Glickman, T., and Terry, K. (1994). *Using the News to Develop a World-wide Database of Hazardous Events*, Center for Risk Management, Resources for the Future, Washington, DC.
36. Burgherr, P., and Hirschberg, S. (2008). Severe accident risks in fossil energy chains: a comparative analysis. *Energy* **33**(4), 538–553.
37. Burgherr, P., and Hirschberg, S. (in press) A comparative analysis of accident risks in fossil, hydro and nuclear energy chains. *Hum. Ecol. Risk Assess*. **14**(5), 947–973.
38. Chernobyl Forum (IAEA, W, UNDP, FAO, UNEP, UN-OCHA, UNSCEAR, World Bank, Governments of Belarus, the Russian Federation and Ukraine) (2005). *Chernobyl's Legacy: Health, Environmental and Socio-economic Impacts and Recommendations to the Governments of Belarus, the Russian Federation and Ukraine. The Chernobyl Forum: 2003–2005,* Second revised version, IAEA, Vienna.
39. Hirschberg, S., Dones, R., and Gantner, U. (2000).Use of external cost assessment and multi-criteria decision analysis for comparative evaluation of options for electricity supply. In *Proceedings of the "5th International Conference on Probabilistic Safety Assessment and Management PSAM 5", 27 Nov–1 Dec 2000, Osaka, Japan*, Universal Academy Press, Tokyo.
40. Hirschberg, S., Dones, R., Heck, T., Burgherr, P., Schenler, W., and Bauer, C. (2004). *Sustainability of Electricity Supply Technologies Under German Conditions: A Comparative Evaluation*, Paul Scherrer Institut, Villigen PSI, *PSI-Report No. 04-15*.

## FURTHER READING

Ale, B. J. M., and Uitdehaag, P. A. M. (1999). *Guidelines for Quantitative Risk Analysis*, (CPR18E) RIVM. SDU-Publishers, The Hague.

Bajpai, S., and Gupta, J. P. (2007). Securing oil and gas infrastructure. *J. Petrol. Sci. Eng*. **55**, 174–186.

Duffey, R. B., and Saull, J. W. (2003). *Know the Risk. Learning from Errors and Accidents: Safety and Risk in Today's Technology*, Butterworth-Heinemann, Burlington, MA.

Eliasson, B., and Lee, Y. Y. (eds.) (2003). Integrated assessment of sustainable energy systems in China. The China Energy Technology Program—A framework for decision support in the electric sector of Shandong province. In *Alliance for Global Sustainability Bookseries Science and Technology: Tools for Sustainable Development*, J. M. Kauffmann, Ed. Kluwer Academic Publishers, Dordrecht / Boston / London, Vol. 4.

Jonkman, S. N., van Gelder, P. H. A. J. M., and Vrijling, J. K. (2003). An overview of quantitative risk measures for loss of life and economic damage. *J. Hazard. Mater*. **99**, 1–30.

Konstandinidou, M., Nivolianitou, Z., Markatos, N., and Kiranoudis, C. (2006). Statistical analysis of incidents reported in the Greek petrochemical industry for the period 1997–2003. *J. Hazard. Mater*., **135**(1–3), 1–9.

Swiss, R. (2002). *Terrorism—Dealing with the New Spectre (Focus Report)*, Swiss Reinsurance Company, Zurich.

Wilson, R., and Crouch, E. A. C. (2001). *Risk-benefit Analysis*, Harvard University Press, Cambridge, MA.

# LESSONS LEARNED FOR REGIONAL AND GLOBAL ENERGY SECURITY

YAROSLAV MINULLIN

*IIASA-DYN, Laxenburg, Austria*

LEO SCHRATTENHOLZER

*Visiting Professor of the Royal Institute of Technology, Sweden, (deceased)*

## 1 INTRODUCTION

One major thrust for the production of this volume on Science and Technology for Homeland Security was the "need for a coordinated scientific and technological response to terrorism" [1]. As a political response to terrorism, the Homeland Security Presidential Directive/HSPD-7 established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks [2]. Voeller [1], (*op. cit*.) argues that the Presidential Directive

does not emphasize the "need to mobilize the nation's skills in science and technology" as strongly as the operational concerns. This apparent lack of emphasis was the stimulus for the study by the National Research Council (NRC) *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* [3]. In response to the research priorities identified by the NRC report, the present volume was proposed to create a major new reference resource. Picking up one of the aims proposed for this handbook, this overview article addresses "the international dimensions of homeland security."

## 1.1 Background

The background of the authors of this article is in the field of systems analysis. Together, they gathered some 40 years of work experience at the International Institute for Applied Systems Analysis (IIASA), a nongovernmental global institute for scientific research [4]. Adhering to the scientific method requires working with terms and concepts that are rigorously defined. In this regard, it appears unfortunate that the term "terrorism" has not been unambiguously defined (that is, in absolute rather than relative terms) even politically, let alone scientifically. We therefore refrain from using this term in the description of our analysis following below. In our opinion, the term "deliberate attacks" is a more precise—and therefore better—descriptor of what is commonly referred to as "terrorist attacks."

***1.1.1 Systems analysis.*** There appears to be no universally accepted single definition of systems analysis. One of the reasons is that the term has a specific meaning in some fields. Even IIASA itself does not promote a unique interpretation of its name on its website, but it is obvious that interdisciplinary research of interactions of systems is a key characteristic of systems analysis. A particularly important aspect of studying interaction is to avoid the pitfall of neglecting crucial interdependencies between systems. For the general question of national security, any systems analytical approach must therefore consider relevant international aspects in the form of outside reactions to national policies.

The second major pillar on which we want to base our concept is a general and fundamental tenet of systems analysis, according to which systems vulnerability is proportional to systems efficiency.[1] To the extent that increasing efficiency of a system goes along with decreasing redundancy, the assertion appears immediately plausible because in a system with many redundancies, the possibilities for substitution (of a malfunctioning subsystem) are greater than in a system with fewer redundancies. Furthermore, if we understand resilience as the opposite of vulnerability, we see that an important systems analytical issue to study is the interplay (trade-off) between resilience and efficiency, that is, to find a joint optimum (maximum) of the conflicting objectives, resilience and efficiency.[2]

As to energy systems, vulnerability and resilience are related to security in an obvious way. Energy security can be enhanced by increasing the resilience of the energy (infrastructure) system. For the purpose of analysis, we believe that it is useful to also distinguish between resilience in the short term and resilience in the long term. While short-term

[1]This general insight has been formulated and substantiated in many specific cases. See, for instance, [14], who analyzed different efficiency, vulnerability and cost functions and found "that these magnitudes display strong correlations."

[2]Accordingly, one of the first major themes of research undertaken at IIASA was a collaborative effort on resilience by IIASA's Ecology and Energy Projects [5, 6].

resilience is related to natural disasters and deliberate attacks, long-term resilience is more a fundamental structural feature of any system.

As a sequel, we cover two topics. The first section deals with basic design features of secure energy systems, and the next addresses the modeling of energy security and competition by presenting the design and some illustrative results of a model of gas-market competition. We also discuss policy implications of the analysis presented here.

## 2 COOPERATIVE ENERGY SECURITY

### 2.1 Resilient Energy Systems

In systems analytical terms, one important manifestation of resilience is the stable equilibrium of a system [6]. To illustrate this mathematically for the case of a one-dimensional dynamic system,

$$Y = \dot{x}(t),$$

a stationary state $x_0$ defined by

$$\dot{x}(t_0) = 0$$

is a stable equilibrium of the system if and only if

$$\ddot{x} < 0$$

In an interval around $x_0$, the dynamics of the system move it toward the equilibrium point.

Applying the concept to an energy system means that the system can be called resilient if it is designed in a way that the dynamic forces determining the evolvement of the system lead it back to the original equilibrium state after a minor (accidental) shock has displaced it away from the equilibrium point.[3] "An example of such a shock would be a deliberate hostile attack on a particular part of energy infrastructure. Addressing such a shock would be addressing the short-term resilience of an energy supply system.

Let us now turn to long-term energy system resilience and, consequently, on resilience as a fundamental structural feature of the energy system.

Doing so requires looking at the long-term vulnerabilities of a national energy system. One important—maybe the most important—long-term security threat to any national energy system is the failure of international suppliers of energy to deliver according to signed agreements or established market principles. Looking at examples of the past, we find that supply disruptions often were justified with disagreements among the partners (consuming, producing, and transit countries) and thus political rather than technical. From this we conclude that long-term resilience of energy supply requires energy importers, exporters, and transit countries to share a strong common interest,

[3]Perhaps one of the most well-known applications of the equilibrium concept is the model of equilibrium price, which results from the intersection of the demand curve and the supply curve. According to this model, for instance, a downward movement ("shock") of the demand curve is followed by an adjustment (reduction) of supply of the item in question. The shock and the adjustment together lead to a new price equilibrium. Alas, recent experiences (in particular in the years 2007 and 2008) have shown that in practice, and contrary to what the model suggests, prices can "run away" from levels that were considered stable.

which stabilizes any equilibrium and which treats "shocks" as a stability problem that must be solved jointly.

A prerequisite of such a system design is therefore symmetry, in the sense that the system must serve the interests of all parties involved. Thus if security of supply is the main criterion for the long-term resilience of an energy system from the importer's perspective, security of demand must be seen as the symmetric criterion from the perspective of an exporter. Both criteria taken together gave rise to cooperative energy security. We cover the two criteria, one by one, in the following two subsections.

Recent work in this area [7] generalizes the concept of resiliency in relation to critical infrastructures (e.g. energy infrastructures) by introducing cooperative systems models for quantitative vulnerability assessment for interdependent complex structures. They describe the resiliency of systems by highlighting the coexistence of two meta-indicator sets defined as tangibles (investments, available resources, and so on), and intangibles (geopolitics, cultural aspects, and so on).

## 2.2 Security of Supply

For a long time, energy security was more or less tacitly assumed to refer to the security of supply only. Accordingly, national energy security was defined as "adequate and reliable energy supply by reasonable prices to avoid damages of fundamental national goals and principles". Even the World Energy Council had only supply in mind when it defined energy security as the "Security of citizens, economics, society and nations against damages and for sustainable fuels and energy supply". Similarly, the International Energy Agency (IEA) sees energy security as the "availability of energy, sufficient (by volume) and available (by price)." In the case of the IEA, the lack of consideration of energy demand security is of course understandable on the grounds that its mission is defined as "energy policy advisor to 27 member countries in their effort to ensure reliable, affordable and clean energy for their citizens" [9].

Recently, energy supply security was analyzed also from the perspective of strategic goals that enhance the long-term resilience of the global energy system in terms amenable to energy modeling. Schrattenholzer [10] identified two indicators that are argued to measure long-term energy security. These are the resource-to-production (R/P) ratio of mineral primary-energy resources and equity, which are defined as follows:

The R/P ratio is defined, for any given year and any given resource, as the amount of the resource left for consumption ("in the ground"), divided by the annual consumption in that given year. Equity was defined as the ratio of average GDP per capita in today's developing regions and today's industrialized world regions.[4] Most global long-term scenarios include the data that allow these indicators to be calculated. Important examples are the scenarios published by IPCC's Special Report on Emission Scenarios [11].

## 2.3 Security of Demand

As we have argued above, symmetry is a necessary requirement for stable equilibria. Since the notion of energy demand security is a comparatively recent concept, we begin this discussion by deriving specific aspects of demand security from their "mirror images" on the supply side.

[4]In 1990, this ratio was approximately six per cent.

*Vulnerability of supply to natural disasters and deliberate attacks.* Natural disasters and deliberate attacks on energy supply infrastructure are hazards to suppliers as well as to consumers and thus symmetric in principle. Recognizing this suggests that producers and consumers have a natural interest in jointly addressing the risks posed by these hazards.

*Use of energy as a weapon by suppliers.* This demand-side hazard figures strongly in the public coverage of the issue of energy security. Often the symmetric hazard of consumers using the same situation as a weapon against suppliers is not included in the discussion. Considering the fact, however, that energy deliveries, for instance, those of natural gas, require sizable up-front investments, the possibility that consumers use sunk cost as leverage is an obvious hazard for suppliers.

*Energy prices.* Energy prices so high as to be felt as threatening the security of energy supply has, for suppliers, the mirror hazard of energy prices so low as to fail covering costs.

### 2.4 Conclusions

So far, we have mainly argued that a systems analytical approach suggests that the security of energy supply and the security of energy demand should be considered together. Now we turn to the question: *To which degree are security of supply and security of demand different concepts?*

To the extent that security is the absence of risk and risk is "*the probability of an unwanted event*" (Oxford University), the concepts are the same—only the unwanted events are different! If consumers and producers follow identical concepts, it is easier for them to practice active energy security in an institutionalized dialogue. Moreover, as our analysis suggests, disruptions (of supply or demand) can be avoided by timely planning. This is another argument for embarking on a comprehensive dialogue, supported by analysis and research, between consumer, producer, and transit countries. Following this argument, one would, for example, aim at minimizing the joint probabilities of all sides' unwanted events.

Also, the actors in such a global energy security management are likely to orient their assessment of the (subjective) probabilities involved in this exercise, according to scenarios of future developments. Thus, energy projections have always played a major role in long-term national security considerations but also in short- and medium-term policy decisions of governments and international organizations such as the IEA and the European Union.

## 3 MODELING ENERGY SECURITY

### 3.1 An Illustrative Example: Natural Gas

In order to illustrate how the concept described above can be applied to the formal modeling of real-world issues, we turn to one of the most interesting examples in the wider area of energy security, the international natural gas markets.

Before summarizing the model, we want to note that in our opinion, what is usually referred to as the natural-gas market lacks important features of more conventional markets. The main reason for this opinion is the lack of a global referencing point for the

price formation (as in case of oil), and the undeveloped trade on well-established markets. Due to its environmental friendliness—relative to the other fossil energy carriers, coal and oil—the share of natural gas in the primary-energy mix is on the increase, with some countries supplying 40 to 60% of their primary-energy needs with the "blue fuel." Although this "success story" began as early as in the 1970s, not much has been done in terms of establishing an institutional framework for efficient and reliable gas trade.

In pursuit of a suitable arrangement, in the beginning of the "gas era," consumers and producers tried to hedge the risks of both parties by negotiating long-term contracts (LTCs) which—as a rule—serve to protect producers' interests by introducing a minimum price and an indexing scheme (in some cases there is an additional condition called "take-or-pay," which increases the security of demand, but compromises the flexibility of the consumer) and consumers' interests by guaranteeing a certain delivery pattern throughout each year at predictable prices. The equivalent of *market clearance* occurs during re-negotiation phases, which can take years. These re-negotiations lead to contract amendments regulating the pricing mechanism. By adjusting the coefficients in the "formula," round by round, each party approaches an equilibrium price.

Today global gas trade is still following the formula "if there are no good relations between supplier and consumer, there is no gas trade." This condition immediately extends the matter from an economic layer to a political, if not—given the strategic interests of each party—geopolitical layer. The quoted formula wants to express that in most cases, physical gas deliveries under import-export deals require good bilateral relations between two or three countries. LNG (liquefied natural gas) imports into the USA[5] are a minor counterexample at best as only some 50% of these imports were delivered under short-term LNG contracts.[6] Likewise, regional and local distribution especially in Eurasia is also characterized by nonmarket price formation for end users.

These peculiarities of gas trade can be explained—among others—by the facts that (i) consumption and production centers are concentrated, (ii) the infrastructure for natural-gas production, transportation, and distribution and is very inflexible (due to the long economic service life of the equipment involved) and cost-intensive, (iii) there are few alternative means of gas delivery, which are, again, inflexible, and, finally, (iv) there are few major gas producers, and these are geographically scattered.

In any case, these types of international relations have an obvious bearing on national energy security. Our formal analysis of these relations builds on the notion of equilibrium in the form of agreed-upon prices and volumes.

In practice, such equilibrium suffers several drawbacks. First, the negotiation position of a consumer depends on a set of geopolitical factors and the state of bilateral relations. Second, there is very little or no competition between sellers at all (primarily due to inflexibility of the import infrastructure), which provides more leverage to the supplier. Thus, the equilibrium is defined on a very narrow optimization interval, which is sensitive to externalities and influenced by many intangible factors.

On the other hand, such long-term arrangement provides two very important ingredients to cooperative energy security: it guarantees the long-term demand for the supplier, which is a key condition to invest into natural-gas production and transmission infrastructure; and it allows the consumer to do national energy planning at given volumes and prices.

[5]The USA is often believed to be a pioneer in the liberalization of natural-gas trade, and LNG has been attributed the role of a "dissolver" of long-term trading agreements.

[6]Moreover, the share of LNG imports in the US consumption is very small—only 3.7% in 2007.

In public discussions in (Western) consuming countries, this mutual dependence of a producer and a consumer is often mistakenly perceived as a burden of the consumer alone. It is obvious, however, that both parties should be interested to act and plan jointly, thus improving energy security of both.[7] Although we recognize at the same time that such long-term interdependence, which extends to the energy sectors of both parties, can also reduce the flexibility of each of them and therefore can be associated with the disadvantages of long-term form of gas contracts.

Responding to the perceived shortcomings of long-term markets, the established up-to-date practice of short-term gas deals had the primary goal of reducing the burden of mutual dependence—the heritage of LTCs. Whereas past local gas markets were formed from scratch, new spot-markets were formed by analogy to oil markets. The main instruments in this spot-market trade are financial derivatives, covered by physical deliveries under long- or short-term contracts. Among the advantages of such a scheme one could highlight the room for competition, transparency (prices and quantities are reported publicly) and indifference with regard to suppliers.

However, while resolving almost all the supply-related drawbacks of the LTCs, markets (in their pure form) bring one big disadvantage with respect to security of demand, which is near zero. We can characterize such markets as *delivering energy security to consumer and supplier at the cost of efficiency and mutual dependence*, and we have encountered another manifestation of the tenet of systems analysis mentioned in the introduction, according to which efficiency (market efficiency from the perspective of suppliers) is proportional to vulnerability (of suppliers). Following the logic of cooperative energy security, it is thus natural to expect that the deterioration of suppliers' security will eventually reflect on consumers.

The arguments for the latter consideration go back to the issue of high investment intensity of gas infrastructure. Payback times, usually equivalent to between 10 and 15 years of a pipeline operating at maximum capacity, pose rather strict necessary conditions even for consideration of an export project.

We summarize main characteristics of the two market types (Table 1).

This comparison makes it obvious that both market models have advantages and disadvantages. Therefore a harmonious solution of cooperative energy security should include features of both of them.

### 3.2 Economic Aspects and Rationality

In previous sections, we identified that competition can help mitigating a number of unwanted features of gas trade; not to mention that fostering competitive energy markets is one of the key elements in modern energy policies of almost all countries. Competition and energy security are thus the key ingredients of the model that we shall summarize here.

The model is named GASCOM (*Gas* Market *Com*petition) and belongs to the family of gaming models. The key idea behind the model was to combine competition with existing methods of evaluating the economic efficiency of energy export projects. GASCOM covers gas trade from an evaluation of a transport corridor on a national level, to precise supply schedules and corresponding cash flows.

[7]The interests of transit countries will be discussed in the section on "Expanding the Scope: Geopolitics and the Inclusion of Transit Countries into the Analysis."

**TABLE 1 Main Characteristics of International Gas Trade Models**

| Long-term, Bilateral | Free-market |
|---|---|
| • Few producers, few consumers | • More producers, more consumers |
| • Price is indexed by alternative fuels | • Competitive short-term price formation (seasonality pattern) |
| • "Shock-absorbing" price formation | • High price volatility |
| • Two-way reliability (prices and quantities) | • Infrastructure development: mostly operational (storage), risky for transmission lines |
| • Infrastructure development: small risk | • Less dependable because more erratic |
| • Foreseeable thus dependable for consumers, producers, investors | • Indifferent with regard to suppliers or consumers |
| • Requires maintaining "good" long-term political relations; creates mutual dependence | |

One of the key characteristics of the gaming approach is that it provides an insight to all admissible strategies (in this particular example: of supply volumes and the timing of market penetration) of all agents. The model thus confirms with our understanding of systems analysis as described in the introduction because it includes all relevant feedbacks and interactions. The result is, for *all* agents,[8] an optimized supply schedule and an optimized time for entering the market.

Here are two interpretations of this model solution:

– In the case of LTCs the model replicates rounds of negotiations between the agents[9] who iteratively update their knowledge about their competitors and adjust their own strategy accordingly. Thus, having collected all information about responses of others to their strategy, agents are capable of defining an "optimal" time of entering the market, optimality being defined by the minimum time passed from the point of decision-making to payback (this option of optimality criterion is closer to maximization of internal rate of return, IRR, of the project rather than traditionally applied maximization of the net present value, NPV). Having determined the time of market entry, agents engage in the second, distinct phase of negotiations, because naturally, this represents another game, when agents control their supply to the market. Eventually (in most cases) all agents will reach a point (the Nash Equilibrium), where varying the timing or supply schedule will not improve their own benefit.

[8]This feature is in contrast to models in which the NPV of *one* (and only one) is maximized.
[9]In the example discussed here, the agents are one importer and many exporters.

Thus, for a LTCs case, a gaming model such as GASCOM, permits each agent to reveal the potential demand of the importer as well as the potential supply —a strategic advantage.

– In case of mid- and short-term contracts, the model imitates the market price formation (in our example, with regard to the future with the delivery in one year), where market fundamentals and the project's economical characteristics identify its competitive advantage. Technically, the solution is similar to the case of LTCs, but the essence of results is different. First, the equilibrium solution involves much higher market risks due to additional impact on price caused by agents' supply strategies. Second, the solution also presumes coordination between agents: no long-term plans will be valid in case there is some irrational behavior for one of the agents (i.e. deviation from equilibrium in pursuit of strategic interests).

Before presenting illustrative results, we would like to mention that most arguments in this section apply to cases when there is a need for the construction of new upstream infrastructure. With growing world demand for natural gas and a trend for diversification of supply sources, this issue is most relevant. Another consideration is that once a gas transmission pipeline has paid back, the risk profile of this infrastructure changes. This, in fact, defines the turning point with regard to providing cooperative energy security: it is most crucial for the payback period; after return of investments, the supplier might gradually engage in free trade.

The three figures below illustrate the processes described above. They illustrate results from a recent case study in which GASCOM was used to analyze the perspectives and the potential of the emerging gas market in China as well as of a set of proposed export projects from Russia, Kazakhstan, Turkmenistan, and LNG in the Pacific Basin [12]. In Fig. 1 we present the discounted cash flows before optimization, that is, the cash flows

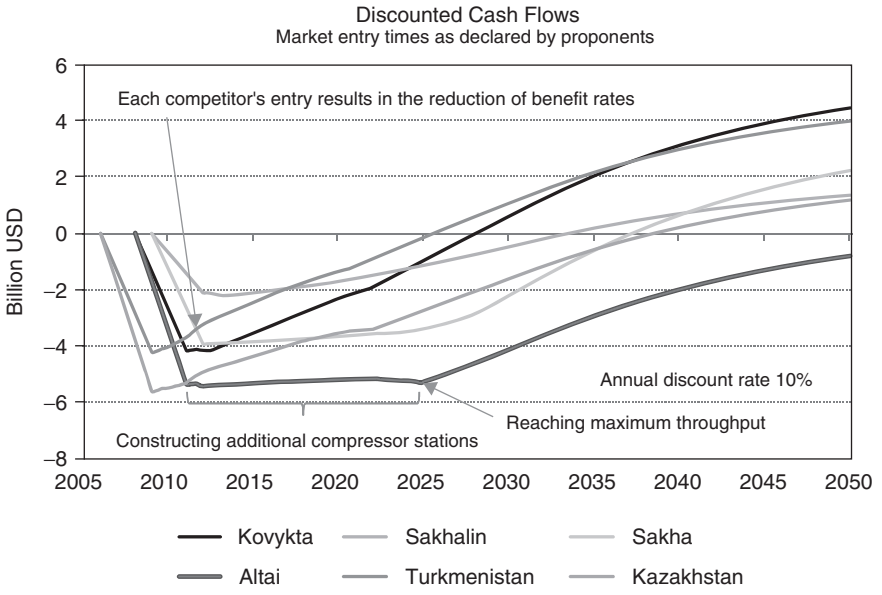



**FIGURE 1** Discounted cash flow with timing as announced by the promoters.

as a consequence of realizing the projects as announced by the representative companies. Explanations inserted into the graphics and the shapes of the curves demonstrate that the model reflects all important peculiarities of a transmission project. Not only that, without optimization one of the projects does not pay off before 2050; most of them also have a relatively low IRR. The underlying reason for this is that all agents endeavor to take a strategic position on a newly emerging market and therefore all of them enter it as quickly as they can. Since demand is limited, achievable prices are insufficient for the candidate projects to be economically attractive.

Figure 2 displays the cash flows for the same set of candidate projects after GASCOM optimization. Now all the projects pay off in a shorter time frame, and they have a higher IRR.

To give a broader picture, Fig. 3 presents the supply schedule by the agents and how it compares to total demand in the market after optimization with the GASCOM model.

From the past studies with the GASCOM model we would like to highlight two—as we believe—important conclusions.

In case of traditional gas trade, based on long-term contractual agreements, the suppliers have an incentive to cooperate with each other with the aim to mitigate market risks and to achieve the best financial results for all parties.

In the case of market trade, we have observed that the suppliers acting in a market with limited representation (i.e. not so many suppliers and even less consumers, which is the case of today's natural-gas markets) tend to keep it in deficit, thus increasing instantaneous profits which, given no possibility to build on long-term planning, is a more profitable strategy for them.

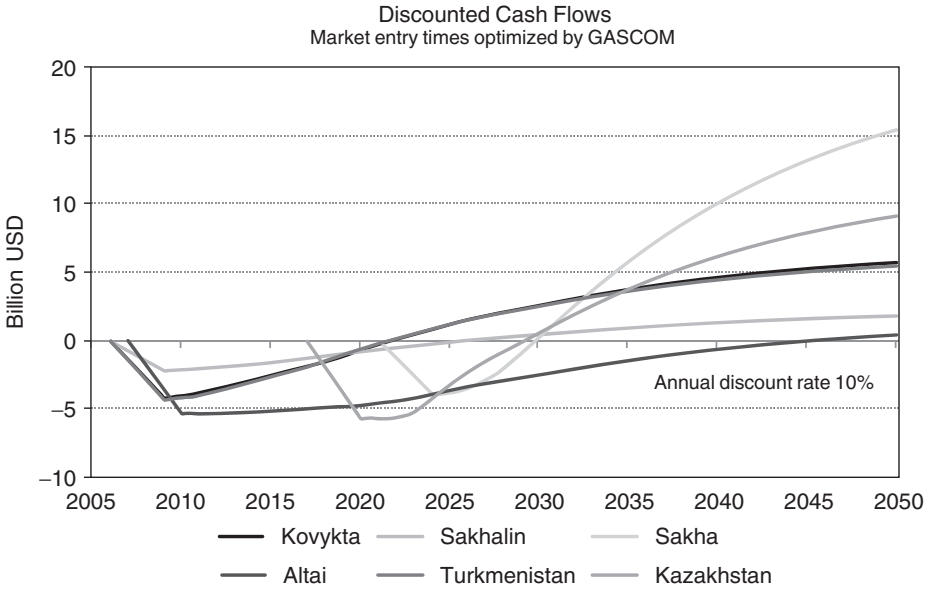



**FIGURE 2** Discounted cash flow with timing optimized by GASCOM.

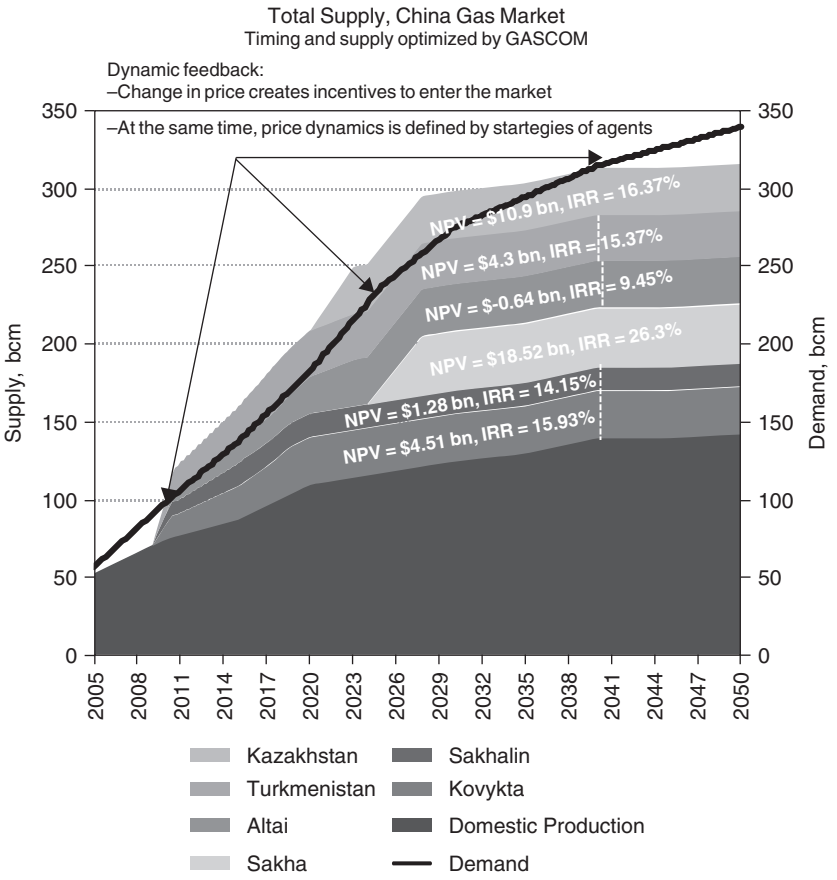



**FIGURE 3** Total supply in the market, timing and supply schedule optimized by GASCOM.

### 3.3 Expanding the Scope: Geopolitics and the Inclusion of Transit Countries into the Analysis

So far we based our discussion of energy security on price and volume factors. However, there are a number of concerns, which make it necessary to enhance the existing analysis tools so as to be closely related to the real world.

1. There has been a growing number of instances in which strategic aspects have dominated over traditionally considered technical and economical feasibility in the process of decision-making in the field of international energy deals.
2. Additional concerns are being raised by the growing complexity of the world energy infrastructure, which strongly exposes interdependability of its layers and sensitivity to short and long-term threats.
3. The interruption of the export flows of Russian gas in January 2009 suggest that role of transit regions in providing the security of supply had been underestimated by research. It is also important that bypassing traditional transit regions will have

a significant socioeconomic impact on them, which, in turn, will affect cooperative energy security.

GASCOM is being enhanced to take these concerns into account.

By monitoring the unwanted events (e.g. a supply disruption for a critical period of time) the new system will be capable of answering questions such as the following:

- Which setup and evolution of the import-export network guarantees the minimum vulnerability in case the given unwanted event occurs?
- How will alternative supply routes impact the cooperative security, that is, to which degree will it serve the suppliers' demand security, the consumers' supply security and the socioeconomic objectives of the transmitters?

In our opinion, these examples of modeling energy security are distinct from previous approaches to energy systems and capable of dealing with the nexus of energy system and its economic-environmental solutions in a dynamic geopolitical global perspective.

## 4 POLICY IMPLICATIONS

Viewing the resilience of a national energy system as a problem of homeland security can go a long way, but as we have argued in this article, going the whole way to international long-term energy security requires a systems analytical approach. One of the most important ingredients of such an approach is to include symmetry, most importantly the symmetry of demand security and supply security. We have illustrated this conviction with examples of popular arguments, which we analyzed from the perspective of symmetry. The resulting recommended strategy we call cooperative energy security.

The second major focus of this article was the presentation of GASCOM, a concrete model of gas trade, which is one of the most important issues in long-term international energy supply and demand. At the core of that model is the notion of Nash Equilibrium, which is completely symmetric by its very formulation.

Applying the model we analyzed two trade modes, a long-term, bilateral mode and a free-market mode. From our analysis of the advantages and disadvantages of the two modes we conclude that the "optimal" mode of the model is fully consistent with the strategy of cooperative security: LTCs until the end of the payback period, free trade afterwards. In addition to its security aspect, we think that cooperation is needed in any gas trade model due to the limited nature of gas "markets."

But how can we implement symmetry of global energy security in the real world? Generally speaking, consumer-producer dialogues that recognize this kind of symmetry and that enter the dialogue in a spirit of joint problem-solving, would appear as a prerequisite. Modest steps in this direction were undertaken jointly by IIASA's Dynamic Systems (DYN) and Environmentally Compatible Energy (ECS) Programs in 2004–2006. In the spirit of systems analysis, a forum was created, on which academia, industry, and policy-making from consumer and producer countries regularly exchanged their views about energy security—in this case of natural gas in particular—in a scientific and neutral environment.

Activities of this forum were the basis of contributions, by the authors of this chapter and their colleagues, to the Energy Modeling Forum's study on "Prices and Trade in a

Globalizing Natural Gas Market" (EMF-23), to the Civil G-8 activities preparing for the St. Petersburg G8 Summit, and to industrial applications.

In order to better understand the phenomena illustrated in this chapter, IIASA's DYN Program has embarked on the Fragility of Critical Infrastructures (FCI) initiative. The purpose of FCI is to view critical infrastructures in the context of systems analysis, that is assessing not only physical properties but also operational, regulatory and behavioral aspects of network nodes and agents involved.

In the meanwhile, the forum has been transformed into the so-called WIEN (***W***orld ***I***ndependent ***E***nergy***N***etwork) Group, moderated by the Institute of Energy and Finance, Moscow [13]. WIEN is an informal network of independent experts and acts as an assembly of individuals with academic, governmental, and industrial backgrounds who are interested in specific issues which are being addressed by the Network.

Also the thoughts presented in this article were inspired by the discussions on that forum and in the WIEN Group. Nonetheless, the authors are solely responsible for the contents presented here.

## REFERENCES


1. Voeller, J. G. (2007). *Handbook of Science and Technology for Homeland Security*, A Guide for Authors. Wiley.
2. Bush, G. W. (2003). *Homeland Security Presidential Directive/HSPD-7*. The White House.
3. NRC, National Research Council Committee on Science and Technology for Countering Terrorism. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. National Academies Press, Washington, DC.
4. IIASA. (2008). http://www.iiasa.ac.at/.
5. Holling, C. S. (1973). Resilience and stability of ecological systems. *Annu. Rev. Ecol. Syst.* **4**, 1–23, reprinted as Research Report 73-3, International Institute of Applied Systems Analysis, Laxenburg, Austria.
6. Häfele, W. (1976). Resilience of energy systems. In *Second Status Report of the IIASA Project on Energy Systems*, Research Report 76-1, W. Häfele, et al., Eds. International Institute of Applied Systems Analysis, Laxenburg.
7. Gheorghe, A., and Vamanu, D. (2009). Mining intelligence data in the benefit of critical infrastructures security: vulnerability modelling, simulation and assessment, system of systems engineering. *Int. J. Syst. Syst. Eng.* **1**(1/2), 189–221.
8. Yergin, D. (1973). *The energy crisis: time for action*. *Time Magazine*.
9. IEA. (2008). http://www.iea.org/about/index.asp.
10. Schrattenholzer, L. (2008). Scenarios of energy demand and supply until 2100: implications for energy security. In *Facing Global Environmental Change: Environmental, Human, Energy, Food, Health and Water Security Concepts, Hexagon Series on Human and Environmental Security and Peace*, Vol. 4, H. G. Brauch, Ú. O. Spring, J. Grin, C. Mesjasz, P. Kameri-Mbote, N. C. Behera, B. Chourou, and H. Krummenacher, Eds. Springer-Verlag, Berlin, Heidelberg, New York, in print.
11. IPCC, Nakicenovic, N., Alcamo, J., Davis, G., de Vries, B., Fenhann, J., Gaffin, S., Gregory, K., Gruebler, A., Jung, T. Y., Kram, T., La Rovere, E. L., Michaelis, L., Mori, S., Morita, T., Pepper, W., Pitcher, H., Price, L., Riahi, K., Roehrl, R. A., Rogner, H.-H., Sankovski, A., Schlesinger, M., Shukla, P., Smith, S., Swart, R., van Rooijen, S., Victor, N., and Dadi, Z. (2000). Special Report on Emissions Scenarios (SRES). *A Special Report of Working Group III of the Intergovernmental Panel on Climate Change*. Cambridge University Press, Cambridge.

12. Minullin, Y. (2008). Queuing to China's gas market. *Oil Russ. J.* **5**, (in Russian).
13. Grigoriev, L., et al. (2008). *World Independent Energy Network*, Draft Mission Statement.
14. Criado, R., Hernández-Bermejo, B., Marco-Blanco, J., and Romance, M. (2007). Asymptotic estimates for efficiency, vulnerability and cost for random networks. *J. Comput. Appl. Math.* **204**(1), 166–171.

## FURTHER READING

EIA DOE. (2009). *U.S. Natural Gas Imports and Exports: 2007*, Special Report.

Energy Charter Secretariat. (2007). *Putting a Price on Energy: International Pricing Mechanisms for Oil and Gas*.

Energy Modeling Forum, EMF-23. (2007). *Prices and Trade in a Globalizing Natural Gas Market, Stanford University*. Available at http://www.stanford.edu/group/EMF/projects/emf23/emf23.pdf.

Klaassen, G., Kryazhimsky, A., Minullin, Y., and Nikonov, O. (2002). On a game of gas pipeline projects competition. *International Congress Of Mathematicians, Game Theory and Applications Satellite Conference (ICM2002GTA), Proceedings Volume*. Qingdao publishing house, China, pp. 327–334.

Kryazhimsky, A., Minullin, Y., and Schrattenholzer, L. (2005). Global long-term energy-economy-environment scenarios with an emphasis on Russia. *Perspect. Energy J.* **9**, 119–137.

Minullin, Y. (2008). Whose pipeline will go east? *Oil Russ. J.* **3**, (in Russian).

Victor, D. G., Jaffe, A. M., and Hayes, M. H. (2006). *Natural Gas and Geopolitics: From 1970 to 2040*. Cambridge University Press.

# LARGE-SCALE ELECTRICITY TRANSMISSION GRIDS: LESSONS LEARNED FROM THE EUROPEAN ELECTRICITY BLACKOUTS

HANS GLAVITSCH

*Swiss Federal Institute of Technology, Zurich, Switzerland*

## 1 INTRODUCTION

Electricity as the most versatile form of energy is the commodity of civilization, which has become something without which modern life is unthinkable. It is not a primary

form of energy, but rather a secondary one, which has to be converted from various primary forms. The locations where these are available may be at distances to those where they are consumed; for example, hydraulic sources or technical constraints may require distant placements of generating stations, although primary sources would allow their site anywhere. Further, electricity requires a transport by conductors or better by transmission lines. Thus, transmission is a basic means for providing electricity to consumers. Since the transportation loss is a function of the current, the transportation over long distances is done at high voltages as high voltages allow low currents, which produce low losses. Single transmission lines are not enough as they do not guarantee enough reserves. Hence, the practice has led to the formation of interconnected transmission networks, which provide reserves, contribute to the economy of the operation and equalize between deficiencies and surplus.

The interconnection, however, implies the propagation of disturbances over wide areas. Hence, deficiencies or surplus of power are felt in the overall system. In extreme condition, a disturbance with all possible internal corrections may evolve to a blackout or near blackout as experienced in recent years in the European interconnected system. There are various causes for blackouts, such as technical, conceptual, due to misunderstanding of phenomena, or simply due to human error.

## 2 BASIC MECHANISM OF ELECTRIC POWER TRANSMISSION IN A LARGE GRID

Electric power transmission is predominantly realized by the system of alternating currents (AC system), in particular by three-phase currents. The alternating mode allows transformation of voltages by the relatively simple transformer. A single-phase system generates a stream of pulsating power. However, if three single-phase systems—as a three-phase system consists of three single phase systems—are combined in such a way that the three single phase systems are shifted one third time period each the shifted pulsating powers result in one constant power stream. Alternating voltages and currents create synchronizing forces between generators such that all machines rotate at the same speed yielding one unique frequency in the system.

The sum of the input powers, thus the generated output, is balanced by the total of the consumed load. The level is adjusted such that the speed that is directly proportional to the frequency of the voltage stays at the nominal level, in terms of frequency 60 or 50 Hz. Any disturbance in the power balance causes a change in frequency. Thus, a drop in frequency is a signal that there is not enough primary power or an excess of load. The Union for the Co-ordination of Transmission of Electricity (UCTE) has established rules [1] for the contribution of generators in subsystems (areas) to the correction or maintenance of frequency. Should there be a major drop in frequency, each subsystem has to be adjusted such that it contributes in terms of the so-called primary control an amount of power proportional to its annual consumption. The amount is derived from an assumed maximum loss of generation of 3000 MW, which does not cause more than 180 mHz of frequency deviation. Besides global changes in frequency, there are local changes on transmission circuits, which may cause overloads.

Another important phenomenon is the change in system voltage. The transport of large amounts of power over long distances leads to a decrease in voltage, which may cause instabilities. Generally, the whole system is an oscillatory system that breaks up if the

amplitudes of the swings exceed a limit, and then there is a loss of generation, which could cause a chain reaction, that is, further losses. In order to counteract undesired oscillations, damping measures are installed in generators, explicitly in voltage regulators. The magnetic field in the generators is mainly responsible for the voltage, and the excitation system controlled by the voltage regulator reacts to any change in the voltage.

## 3 POWER FLOWS IN INTERCONNECTED GRIDS

Power flows in the grid are determined by the injected nodal powers, that is generation and consumption, and by the laws of the network acting on meshes and nodes, which consist of balances of voltages generated by currents times impedances in a loop or by balances of nodal currents. Impedances are characteristics of transmission lines. Because of mechanical properties, transmission lines can carry flows up to a predetermined thermal limit (conductor temperature determining the sag of conductors). Since the flows from one location to a distant one is fixed by the injected powers, the loss of a transmission circuit causes a redistribution of local flows. In extreme condition, the loss of one of the several parallel circuits causes a shift of the flow to the remaining ones, which can lead to overloads. A numerical example of a flow situation is given in Figure 1.

The total of flows is given by the injections at nodes A and B equaling the output at nodes C and D, that is 490 MW. In the normal operation, the flows in the circuits A–C, A–D, and B–D are also 490 MW. When the line A–C is lost, the loading on A–D reaches 279.4 MW and on B–D 210.6 MW without any change in the total of input/output at the nodes.

## 4 THE EUROPEAN INTERCONNECTED SYSTEM—THE UCTE SYSTEM

The European interconnected system consists of three major parts that are connected by high voltage direct current (HVDC), namely, the central UCTE system, the Scandinavian

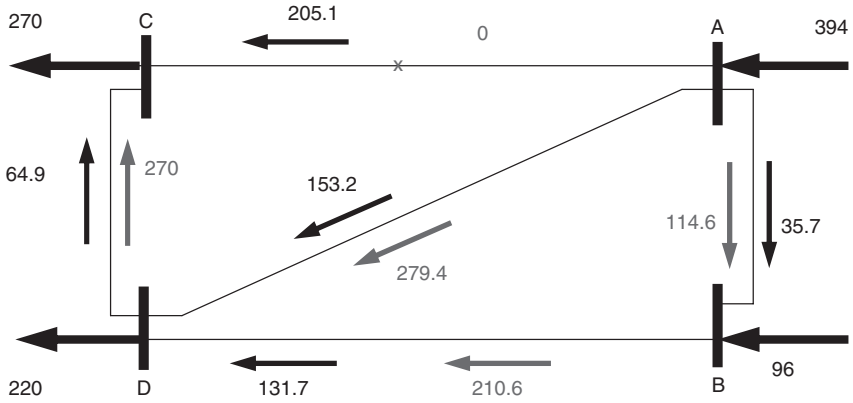



**FIGURE 1** Effect of outage of one circuit (A–C): black figures flow in nondisturbed network and grey figures flow when circuit A–C is tripped.

network, and the network on the British Islands. Here, the interconnected synchronous AC system, the UCTE system, is of interest. It extends from Denmark to Spain and from France to Greece and the East European countries. It consists of 380- and 220-kV-transmission lines operated to a maximum of 420 and 245 kV, respectively. The structure of the grid is characterized by substations where a large number of transmission lines terminate and a larger number of substations where just three or four lines are connected. Typical line lengths for 380 kV are in the range of 100–150 km, sometimes 200 km. For 220 kV, they are considerably shorter (50 km). In France, the line lengths are above 200 km for 380 kV. In Germany, Switzerland, and Northern Italy, the grid is highly interconnected. Tie-lines (circuits crossing borders) are not numerous, except in Germany and Switzerland. The number of tie-lines to East European countries is relatively less.

Originally, the UCTE system had the function to provide the security of supply in continental Europe. For this purpose, the system has been developed over the last 50 years with a view of assuring mutual assistance between national subsystems. However, there has been a fundamental change of paradigms over the past one or two decades. The transmission infrastructure is no longer just a tool for mutual assistance, but has become a platform for shifting ever growing power volumes all across the continent. On the other hand, the development of the system is more and more affected by stricter constraints and limitations in terms of licensing procedures and construction times.

In the UCTE system, the annual production in the year 2006 amounted to 2584.6 TWh, the maximum load 390.6 GW (third Wednesday in December) and the annual load reached 2530.1 TWh. Electricity is produced in nuclear stations (37%), conventional thermal stations (47%), and in hydro stations (16%, figures of 1999).

Within a country, one or more control areas operated by independent transmission system operators (TSOs) and a large number of market participants (traders) are in existence. Today there are 29 TSOs in 24 countries. Energy is exchanged for various reasons, hydro to thermal, day to night and vice versa, as well as for economic benefits. The annual exchange 2006 among UCTE countries reached 296,822 GWh, that is 11.7% of the consumption. This is an increase over the time before the opening of the market as the exchanged energy is typically in the order of 9–10%.

## 5 MANAGEMENT OF THE SYSTEM

### 5.1 Before Opening of the Market

The vertically organized utilities were focused on their system and consumers. Tariffs for the exchange between voltage levels were fixed and state controlled. On the transmission level, an exchange of energy and power took place for the benefit of reducing reserves, peaking power, system regulation, better control of frequency, area control, and coordinated scheduling. The TSOs were the traders and the actors. The operation was coordinated by the rules of UCTE, which comprised the reserve management, primary, secondary, and tertiary frequency control, as well as security management.

### 5.2 In the Open Market

The Directives of the European Community introduced the liberalization of the electricity market [2], which was implemented step by step and is now nearly complete. The aim is

a fully liberalized electricity market for all consumers whereby generation, transmission, and distribution are unbundled. The market participants are the traders and the TSOs are responsible for the technical aspects of operation. Explicitly, traders are utilities, power producers, and consumers, whereas TSOs are organizations for system control. In the open market, the exchange is governed by short-term economic objectives and trading takes place in a bilateral way and on central exchanges. However, there are also long-term contracts among partners being apart for short and long distances. As compared to the modes of operation, before liberalization flow patterns change markedly from hour to hour. There are countries that mainly export and import, that is France, Switzerland, and Germany export and Italy and Netherlands import. Some are net importers/exporters, others show changing patterns, and still other traders sell energy not originating in the own area.

As mentioned, TSOs are responsible for congestion management and system security; however, quite often they are not in command of controlling flows in their own area since the cause and origin of the problem lie outside the area, that is corresponding generation and consumption. The UCTE rules as laid down in the handbook [1] supplemented by the multilateral agreement (MLA [3]) are still in effect, the latter in particular focused on maintaining security. Congestion management is predominantly implemented in terms of auctions on cross-border transmission circuits. The methodology is market conform, but has limited effects as the TSOs lack information from neighboring areas and congestions within the areas are not handled. This is not satisfactory, as the annual exchange is increasing particularly in local zones such as in countries like Switzerland, France, Germany, Netherlands, and Italy.

## 6 THE ITALIAN BLACKOUT 2003

### 6.1 Introduction

The Italian transmission system is in a particular situation as the connection to the European network is geographically concentrated on the North only. The cross-border lines consist of not too many 380 kV circuits concentrated toward France and Switzerland. There is a 380 kV connection to Slovenia, but the network behind, that is, through Austria, consists of 220 kV lines only. The 380 kV loop through Hungary is not very effective because of high impedances, see Figure 2.

Because Italy does not generate nuclear energy and is with high energy costs due to fossil fired units, energy is imported from France, Germany, and Switzerland (for economic reasons) and the energy is stored in pump storage units during nights and weekends. The power flows predominantly over the circuits from France and Switzerland. As the flows are substantial and when it has been realized that the loadings of the tie-lines are critical, the countries involved established reference flows for the summer and the winter period, which were derived from power injections in the zone north of the Alps. According to these reference flows, the maximum import to Italy may reach 6500 MW in winter and 5500 MW in summer. These imports when appropriately distributed over the cross-border zones and circuits have been designed to guarantee an $(n-1)$-secure system. (The concept of $(n-1)$-security is discussed below.)

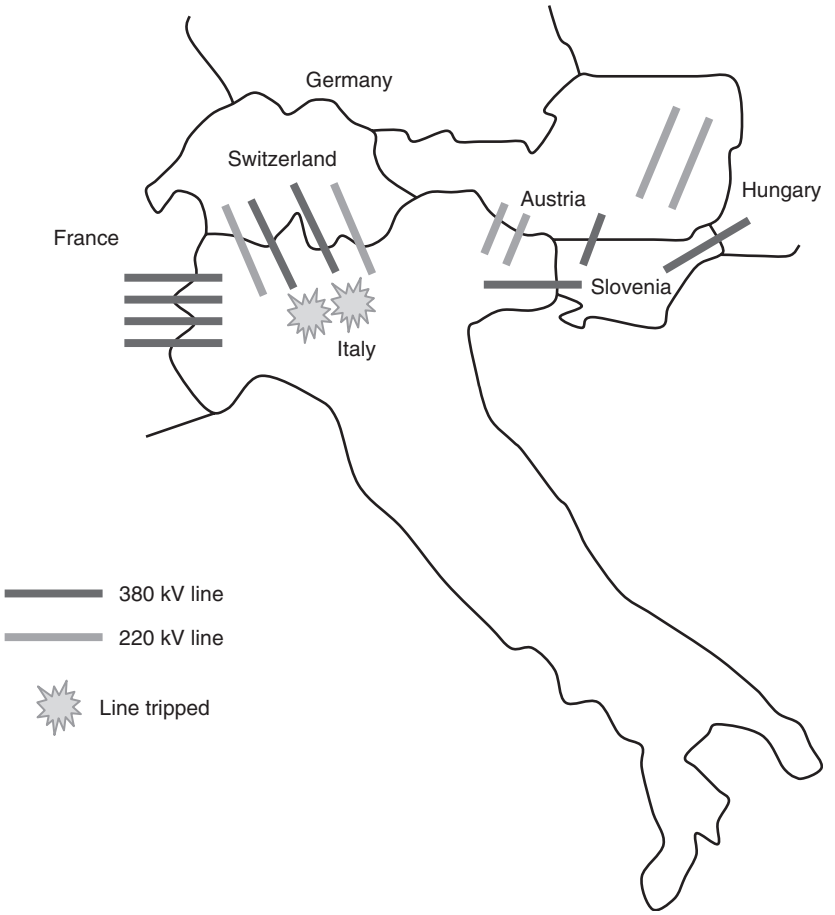



**FIGURE 2** Italy—tie-lines to the north.

### 6.2 Factual Sequence of Events—Blackout September 28, 2003

On September 28, 2003, a Sunday, at 03:00 a.m., a typical situation existed where 6651 MW was imported and apparently used for pumping (pump load 3638 MW). At this time, the total consumption in Italy was 27,702 MW. The tie-line flows and the scheduled flows are as follows [4, 5]:

| | Physical flows (MW) | Scheduled flows (MW) |
|---|---|---|
| Switzerland–Italy | 3610 | 3068 |
| France–Italy | 2212 | 2650 |
| Slovenia–Italy | 638 | 467 |
| Austria–Italy | 191 | 223 |

The physical flows are those actually measured and the scheduled flows are those set on the load—frequency controllers.

The cross-border circuits between Switzerland and Italy consisted, at that time, of two 380 kV circuits (single lines) and several 220 kV circuits. The 380 kV circuits run from Mettlen to Lavorgo (Lukmanier line) and Sils to Soazza (San Bernardino line), both cross the Alpes. The latter substations are still in Switzerland, but are connected via 380 kV lines to stations in Italy.

In the following paragraph, the exact sequence of events is discussed as reported in Refs. [4, 5].

At 03:01:42 a.m., the 380 kV circuit Mettlen–Lavorgo tripped due to a tree flashover. The automatic reclosure was unsuccessful because of a phase angle difference of 42° across the open breaker (the setting on the breaker was 30°). A subsequent manual trial was just as unsuccessful. As a consequence, the 380 kV circuit Sils–Soazza overloaded and reached 110% of its thermal rating. At this point, the state of $(n-1)$-security was lost. The operator at the control center in Laufenburg (at that time ETRANS, now Swissgrid) was unaware of the urgency of the situation. The Swiss operator noticed that the actual flows to Italy were roughly 300 MW above the scheduled value and requested a reduction of the imports from the Italian TSO (GRTN–Gestore della Rete di Trasmissione Nationale) by telephone at 03:11 a.m. The tolerable time for the reduction of the current was 15 min.

The reduction was performed and the imports reached the scheduled value after 10 min. However, the reduction was not sufficient and at 03:25:11 a.m., the circuit Sils–Soazza tripped due to a tree flashover (probably because of a high sag caused by the overload). Immediately afterwards further 220 kV circuits tripped, and at 03:25:28 a.m. the Italian network lost synchronism with the rest of the UCTE system. The Italian system has lost about 6500 MW, the frequency dropped causing the shutdown of generating stations, which led to the blackout (definite at 03:27:58 a.m. when the frequency dropped below 47.5 Hz). The rest of the UCTE system experienced a rise in frequency to 50.25 Hz with swings to 50.3 Hz. In the immediate vicinity of the Italian border in Switzerland (Ticino and Valais), the systems were lost (blackout). Otherwise the UCTE system was not affected, although it experienced the frequency changes.

The report [4] mentions four main reasons for the blackout:

1. Unsuccessful reclosing of the line Mettlen–Lavorgo (Lukmanier) because of a too high phase angle difference.
2. Lacking sense of urgency regarding the Sils–Soazza (San Bernardino) line overload, and call for inadequate countermeasures in Italy.
3. Angle instability and voltage collapse in Italy.
4. Right-of-way maintenance practices.

However, the principle of $(n-1)$-rule in chapter "Security and reliability standards—safety of the system" states that a single incident must not jeopardize the system, which implies that after a loss of the (n–1)-state the system is supposed to return to the $(n-1)$-state as soon as possible. This means identifying countermeasures which would enable the system to be brought back to a secure state. The report states that the appropriate countermeasure after the loss of the Mettlen–Lavorgo circuit would have been the shutting down of the pumps in the storage plants in Italy having a load of about 3500 MW.

### 6.3 Comments on and Interpretations of the Events/Findings

The reasons given in Ref. 4 are certainly true and correct, but do not give the complete picture. In particular, the first two points need further explanations. As far as point 1 is concerned it has to be realized that there was a substantial flow across the Swiss network where the circuit Mettlen–Lavorgo is imbedded. This flow caused the phase angle difference of 42°, which should have been below 30°. The Swiss Federal Office of Energy (SFOE) investigated the situation and came to the conclusion that the flow situation has been far away from the reference flow [6]. The reference flow would have produced a phase angle difference of 20° and there would have been no overload on the circuit in the first place. A simplified network illustrates the effect of flows on the phase angle difference at an open breaker, see Figure 3.

The phase angle difference is proportional to the sum of the flows C + D + E or to the flow A or B. A phasor diagram is shown on the right-hand side where phasors are the terminal voltages. The tree flashover is probably due to excessive sag of the conductors, which was caused by the overload. Hence, the flow situation is the primary cause of the tripping and the unsuccessful reclosing. The report states that the system was still $(n-1)$-secure at 03:00 a.m., which would have been correct if the countermeasures had been identified and implemented. This is one of the basic flaws in the whole process that must be further criticized by the following.

A quite similar disturbance happened in the critical zone of the Swiss network in the year 2000, which is documented in the annual report 2000 of UCTE [7]. On September 8, 2000, the San Bernardino (Sils–Soazza) 380 kV circuit tripped at 9:46 p.m. and at 10:11 p.m. the Mettlen–Lavorgo (Lukmanier) 380 kV circuit tripped, followed by trippings of 220 kV circuits between Switzerland and Italy as well as between Austria and Italy. These line trips led to load displacements on France to Italy line resulting in a flow of 3900 MW on 380 kV and 220 kV lines. As a result of this overloading, these transfrontier lines together with five other 380 kV lines in France reached their 20 min overload protection threshold, others even their 10 min overload protection threshold.

Italy was required to produce an additional 1800 MW, in order to ensure operational security without network separation. It was not possible to implement a sufficiently rapid reduction of nearly 1500 MW in exchange programs between Italy and Switzerland. For these reasons, the UCTE network frequency rose to 50.15 Hz.

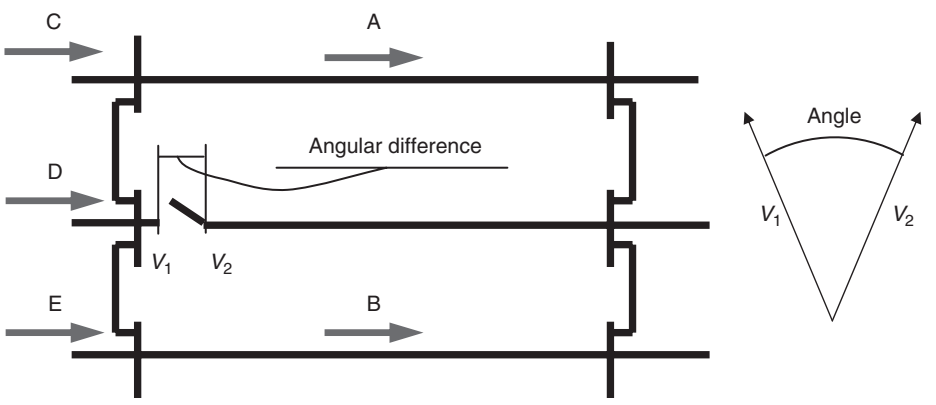



**FIGURE 3** Flows generating phase angle difference at open breaker.

The report mentions numerous problems that took place in the following hours and on September 9, 2000. However, no disturbances in the distribution were recorded. What is important is the concluding statement in the report:

> As a result of the events described above, TSOs in Italy, France, Switzerland have agreed to a joint procedure for the improvement of communications and the implementation of arrangements for the modifications of exchange programs in case of emergency.

The events after 03:00 a.m. on September 28, 2003, do not indicate that such a joint procedure has been established. Further, it is an open question what the countermeasures would have been if the outages had taken place during the week around 11:00 a.m. when no pumps were in operation.

Unless one would resort to substantial load shedding in Italy (the remedial measure to point 3 above), the solution to the problem is careful congestion management whereby flow patterns close to the reference flow are maintained and the security is monitored whenever the load changes. Swissgrid, the Swiss TSO, has implemented a security monitoring scheme [8], which generates security information within half a minute whereby the Swiss network plus the surrounding network comprising 6000 nodes is modeled. Today this is the only realistic and practical procedure to master the problem.

## 7 THE SYSTEM DISTURBANCE NOVEMBER 4, 2006

### 7.1 Situation and Actions before the Disturbance

On November 4, 2006, at 10:10 p.m., the European network was split into three parts caused by a planned outage of a double circuit 380 kV line in northern Germany where the consequences were meant to have been orderly estimated and considered secure, but finally evolved to a cascading process. The process separated the UCTE and caused low-frequency load sheddings, but did not lead to a complete blackout. A precondition to the disturbance was the heavy cross-border flow situation between East and West Germany on the one hand and Eastern Europe and South Eastern Europe on the other hand. Since this is essential to the understanding of the disturbance of the network areas, the generation and cross-border flows are shown in Figure 4 [9].

The East–West flow of 9260 MW was caused by a heavy load in the Netherlands, which was supplied by wind generation in the northeast. The double circuit line that was switched was the Conneforde–Diele line shown in Figure 5 located in the far northwest corner of Germany.

The line belongs to the network of E.ON, the important German utility and the taking-out-of-service was planned for November 5 and prepared the days before. The operation was requested by a shipyard for passing of ship on a canal that is crossed by the line. It was also coordinated with Tenne T, the TSO of the Netherlands. E.ON Netz, the TSO of E.ON, carried out an analysis of the impact of the operation using standard planning data. As no violation of the $(n-1)$-criterion was detected, E.ON Netz provisionally approved the switching off. On November 3, around 12:00, the shipyard requested E.ON Netz to advance the disconnection of the line by 3 h, to November 4 at 10:00 p.m. A provisional agreement was given by E.ON Netz after a new analysis did not reveal a violation of the $(n-1)$-criterion. At this point, the TSO of Rheinisch-Westfaelisches-Elektrizitaetswerk (RWE) of the adjacent German network

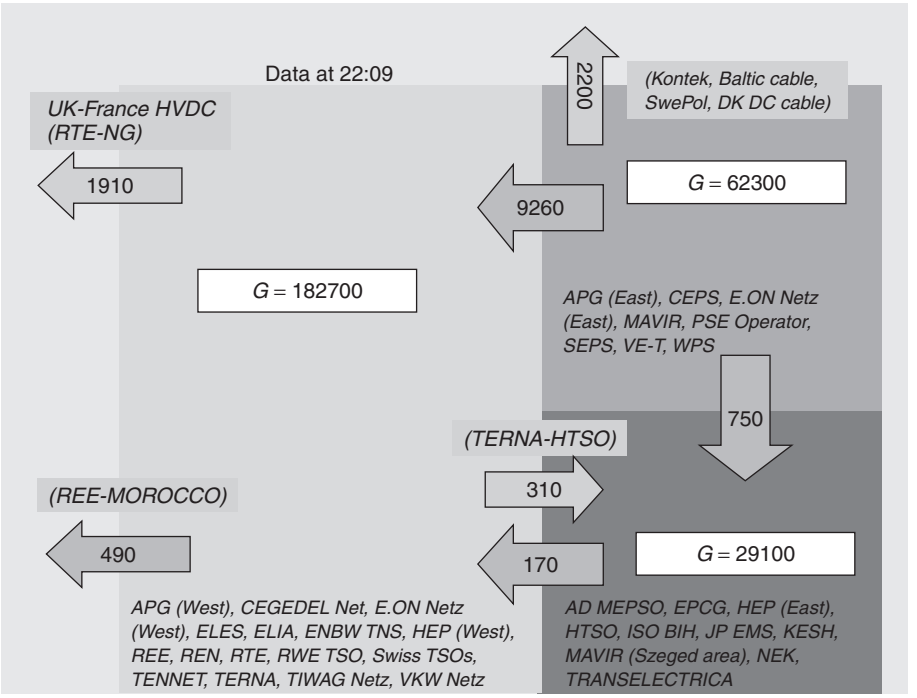



**FIGURE 4** Schematic of UCTE system: three areas before separation at 9:09 p.m. and generation and cross-border flows.

and the TSO of Tenne T were not informed about this procedure, so no special security analyses were made.

For the new situation, it was not possible to reduce the exchange program between Germany and the Netherlands including the outage of the Conneforde–Diele line (agreed timing, setting of capacities, and auctions). Further, there was no indication of the switching operation in the planning tools and data, such as day ahead congestion forecast (DACF), by E.ON Netz to all UCTE TSOs on November 3 with the forecast for November 4 at 10:00 p.m. and beyond.

As late as 6:00 p.m., E.ON Netz informed Tenne T and RWE TSO about the new time for the disconnection of the line.

At 9:29 p.m., a load flow calculation by E.ON Netz did not indicate any violation of limit values. On the basis of an empirical evaluation of the grid situation, E.ON staff assumed, without numerical computations, that, after the disconnection of the line, the security of the system would be met.

RWE TSO also made a load flow calculation and an $(n-1)$-analysis at 09:30 p.m. just before the opening of the line, which confirmed that the RWE grid would be highly loaded but secure.

### 7.2 Evolvement of the Disturbance

The two circuits of the Conneforde–Diele line were switched off at 9:38 p.m. and 9:39 p.m. Shortly afterwards, E.ON Netz received warning messages about the high loading

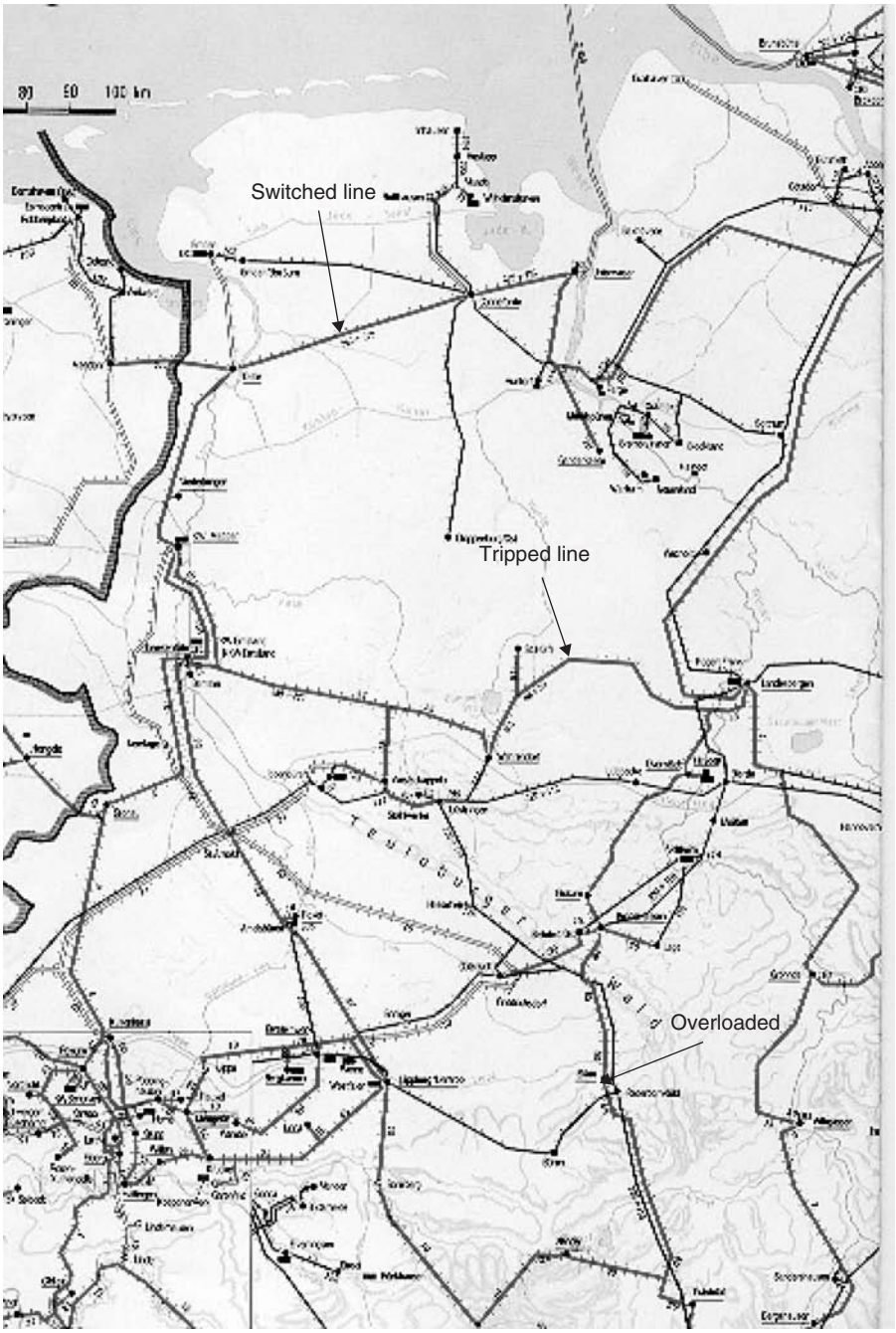



**FIGURE 5** Line diagram, section of northern Germany.

on a line south of the area shown in Figure 5 and at 9:41 p.m. RWE TSO informed E.ON Netz about the safety limit of 1795 A on the line Landesbergen–Wehrendorf, an interconnection between the E.ON network and the RWE network. This line is shown in Figure 5. However, at this point in time the critical current on this line has not been reached. The report [9] documents that the protection settings on either sides of this line were different and the TSO of E.ON was not aware of this fact, that is tripping current 3000 A on the E.ON side and 2100 A on the RWE side. In phone calls between the TSOs of E.ON, RWE, and Vattenfall, up to 10.00 p.m. the situation was considered to be critical and apparently RWE TSO informed E.ON Netz about the settings.

Between 10.05 p.m. and 10.07 p.m., the load on the 380 kV line Landesbergen–Wehrendorf increased and exceeded the warning value of 1795 A, which caused the RWE TSO to request from E.ON Netz an urgent intervention to restore the security of the system. E.ON Netz made an empirical assessment of corrective switching measures in terms of coupling of the busbars in Landesbergen expecting a reduction of the line current by about 80 A. The operation was done at 10:10 p.m., but resulted in the opposite effect. The line current increased and caused the tripping of the Landesbergen–Wehrendorf line, leading to a subsequent cascading opening of circuits along the vertical line shown in Figure 4 and separation of the southeastern network.

### 7.3 Consequences of the Opening

The European network was separated into three parts, as shown in Figure 6, whereby different frequency patterns developed. Since a substantial flow between the East and West part was interrupted, the area 1 experienced a drop and the area 2 a rise in frequency. In area 3, there was a frequency drop but it was only 200 mHz. The low frequency in areas 1 and 3 caused a series of load sheddings spread over the areas and the loss of loads was substantial, that is between 3% and 19% of the load. In some areas, pumps were disconnected between 240 and 450 MW. In all areas, generation was tripped, namely, 10,909 MW in total. The switching operations caused heavy intersystem

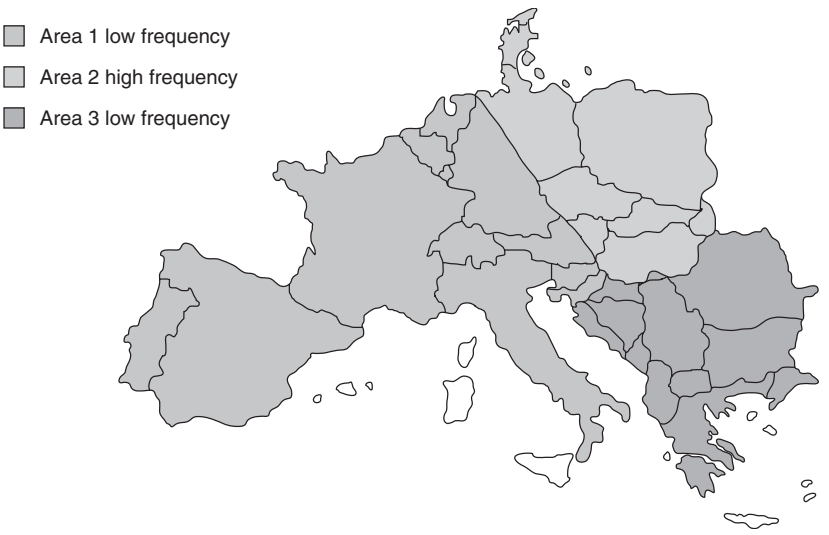



**FIGURE 6** Separation of the UCTE network into three parts.

flows after 10:10 p.m. A complete blackout did not result in neither of the areas. This allowed the restoration and the resynchronization of the areas fairly soon after the initial disturbance.

The actions of the resynchronization process showed three different phases, namely:

- resynchronization trials that did not result in real interconnection;
- resynchronization attempts that resulted in real interconnection, but failed after a few seconds;
- successful resynchronization steps.

The milestones of resynchronization were first successful reconnection of tie-lines between areas 1 and 2 at 10:47 p.m. when areas 1 and 2 were connected, and area 3 was connected at 10:49 p.m.

The problems in the resynchronization process were the missing information on the state of generating units and of the network, as well as noncoordinated trials of operators to synchronize generators. In particular, actions in the distribution network were completely non-coordinated.

### 7.4 Failures and Mistakes that Led to this Disturbance

On the basis of report [9], several items that caused the disturbance can be identified. The main cause is the omission of contingency analyses at various stages of the preparation of the switching operation, both by E.ON Netz and RWE TSO. This applies to the points in time before the opening of the line, right after the opening of the line, and before the coupling of the busbars in Landesbergen. It is not just an analysis of the respective own area, which should have been performed, but a comprehensive analysis of the own area including the surrounding network, that is E.ON network plus RWE network plus Tenne T network as it is possible today and described in [8]. Another item is the missing information of RWE TSO and Tenne T by E.ON Netz about the advance of the switching of the line. This did not allow the TSOs to check the consequences of the switching early enough.

A crucial item was the different protection settings on the Landesbergen–Wehrendorf line about which E.ON Netz was not aware. It was not only this line which was heavily loaded, but also several lines in the E.ON and RWE network, which when tripped, could have caused the disturbance. The load increase between 10:00 and 10:10 p.m., which led to the tripping, was also affected by the change in exchange programs that usually takes place around this time, for example, 340 MW from Germany to the Netherlands.

Generally, there was insufficient coordination between the TSOs. According to [9], this was considered the second main cause of the disturbance.

## 8 UNBUNDLING AND DECENTRALIZATION—FEATURES IN CONTRADICTION TO SECURITY

Further to the detailed discussions and conclusions from the reports on disturbances, there are general features of the liberalized system in Europe, which are detrimental for the security of the network. One of the features is the requirement of the Directive of the European Community to unbundle generation, transmission, and distribution.

Unbundling is justified in the normal state of the system. However, in a critical situation, the cooperation of generation and transmission is absolutely necessary and therefore unbundling has to be suspended. A TSO must have direct access to generation for the correction of a flow. Above all, the European system is decentralized. According to [9], there are 29 TSOs in 24 countries which manage an area or subsystem. But for the purpose of security, a comprehensive control over a wide region, that is overlapping the own, would be necessary. Each TSO is obliged to carry out such an analysis and TSOs have to cooperate and communicate in critical situations.

Thus, decentralization, congestion management, and security control in the European system are unresolved items.

## 9 CONCLUSIONS

The large-scale electricity transmission grid with a decentralized control structure, that is independent transmission operators as in the UCTE system, and under the concept of unbundling is only partly suited to manage disturbances and to avoid blackouts, at least with the presently implemented tools. Unbundling and decentralization are detrimental for security as the electricity grid acts as a whole, in terms of frequency, voltage, and flows, from one end to the other. Contracts over long distances and the ensuing flows are difficult to control by TSOs. Hence, cooperation and closer communication is needed.

## REFERENCES

1. UCTE. *Operation Handbook*, www.ucte.org.
2. Directive European Union 2003/54/EG (previous 96/92/EG).
3. Multi-Lateral Agreement (MLA) in UCTE. *Operation Handbook*, http://www.ucte.org/e default asp.
4. UCTE (2003). *Report–Interim Report of the Investigation Committee on the 28 September 2003 Blackout in Italy*, 27 October, www.ucte.org.
5. Gheorghe, A. V., Masera, M., Weijnen, M., and De Vries, L. (2006). *Critical Infrastructures at Risk—Securing the European Electric Power System*, Appendix A.1 Learning from the Past—Electric Power Blackouts and Near Misses Europe. Springer, New York.
6. SFOE Swiss Federal Office of Energy (2003). *Bericht über den Stromausfall in Italien am 28. September 2003*, November (Report on the blackout in Italy). SFOE Swiss Federal Office of Energy, Switzerland.
7. UCTE 2000 Annual Report, www.ucte.org.
8. Nordanlycke, I., Bossert, G., and Glavitsch, H. (2007). Security and congestion management tool for the use in extended transmission systems. *IEEE Powertech 2007*. Lausanne, July 1–5, www.ucte.org.
9. UCTE (2006). *Final Report - System Disturbance on 4 November 2006, www.ucte.org*.

## FURTHER READING

Taylor, C. W. (1994). Power System Voltage Stability McGraw-Hill International Editions—Electrical Engineering Series.

Philipson, L., and Lee Willis, H. (1999). *Understanding Electric Utilities and De-Regulation*, Marcel Dekker, Inc., New York.

Shahidehpour, M., and Alomoush, M. (2001). *Restructured Electrical Power Systems—Operation, Trading, and Volatility*, Marcel Dekker, Inc., New York.

Kundur, P. (1993). *Power System Stability and Control*, McGraw-Hill Inc., New York.

# INTERDEPENDENT ENERGY INFRASTRUCTURE SIMULATION SYSTEM

G. Loren Toole and Andrew W. McCown

*Los Alamos National Laboratory, Threat Reduction Directorate/Decision Applications, Los Alamos, New Mexico*

## 1 INTRODUCTION

IEISS was derived from the energy interdependence simulation (EISim) and simulation object framework for infrastructure analysis (SOFIA) software architectures that have been applied routinely at Los Alamos since the mid-1990s. The National Infrastructure Simulation and Analysis Center (NISAC), supported by the Department of Homeland Security, Office of Infrastructure Protection, funds for the use of this software. The NISAC program was established to meet the need for a comprehensive capability to assess the national system of interdependent infrastructures. In the USA PATRIOT Act of October 2001, NISAC was chartered to "serve as a source of national competence to address critical infrastructure protection and continuity through support for activities related to counter terrorism, threat assessment, and risk mitigation".

This article discusses the underlying simulation concepts, application of interdependent energy infrastructure simulation system (IEISS) to an interdependency case study of urban infrastructure, and IEISS applications to other problems of national interest.

Interconnected and interdependent energy infrastructures are extremely complex systems, consisting of physical facilities (such as power plants and refineries), transmission lines, phone lines, roads, railways, waterways, and so on, as well as human decision makers (e.g. consumers, legislators, investors, and chief executive officers). Examples of critical infrastructures that are interconnected and interdependent are shown in Figure 1.

A comprehensive simulation tool is needed to model the nation's key infrastructures (e.g. energy, communication, and transportation) and their intra/interdependencies.

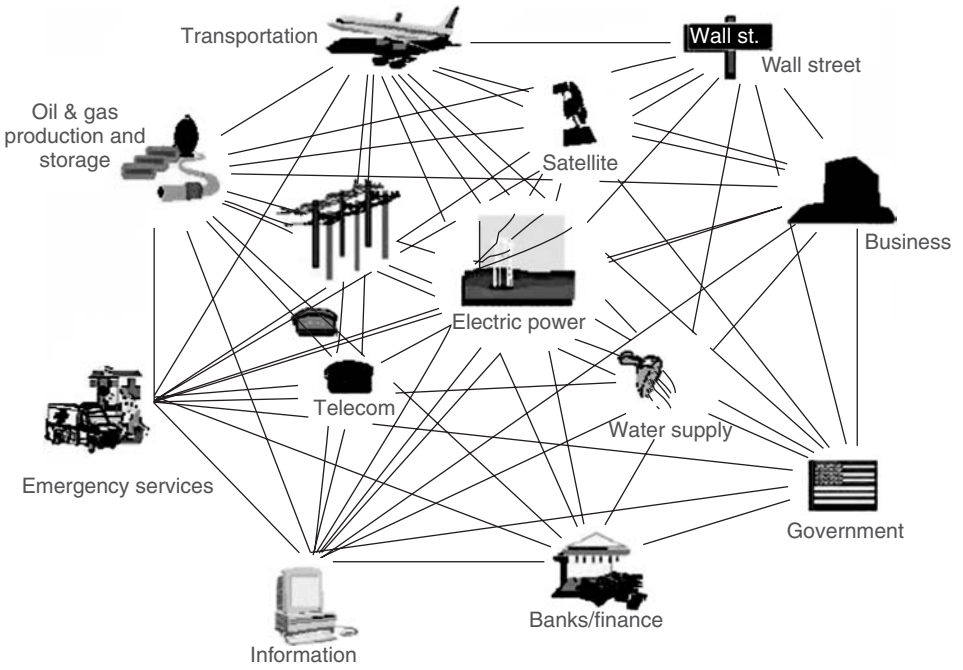



**FIGURE 1** National interconnected and interdependent infrastructures.

However, these dependencies must be identified and understood before infrastructure protection, mitigation, response, and recovery options can be provided. Although existing technology well analyzes single-domain infrastructures, severe limitations arise when this technology is applied to interdependent infrastructures. For these cases in which multiple infrastructures are considered, analysts typically treat these interdependencies in an *ad hoc* manner. To represent the complex, nonlinear, and interdependent nature of these infrastructures, advanced computer simulations are needed. Without these simulations, it is simply too expensive, too risky, and too time consuming to determine the impact of policy and security decisions.

## 2 IEISS SIMULATION CONCEPTS

An infrastructure interdependency is defined as a physical, logical, or functional connection from one infrastructure to another, where the loss or severing would affect the operation of the dependent infrastructure. Although short-term service interruptions of energy infrastructures routinely occur, catastrophic system failures, or large-scale blackouts, are rare events. As infrastructures become more complex and interdependent, the probability of having large-scale outages increases. Because a component failure in one infrastructure does not necessarily result in a propagating failure in another interdependent infrastructure (or for that matter, within the same infrastructure), this cascading phenomenon is difficult to analyze. An example of interdependencies among network-like infrastructures is given in Figure 2. "Network-like" refers to an inherent topological feature of the infrastructure itself, namely, a connected structure of linked nodes.

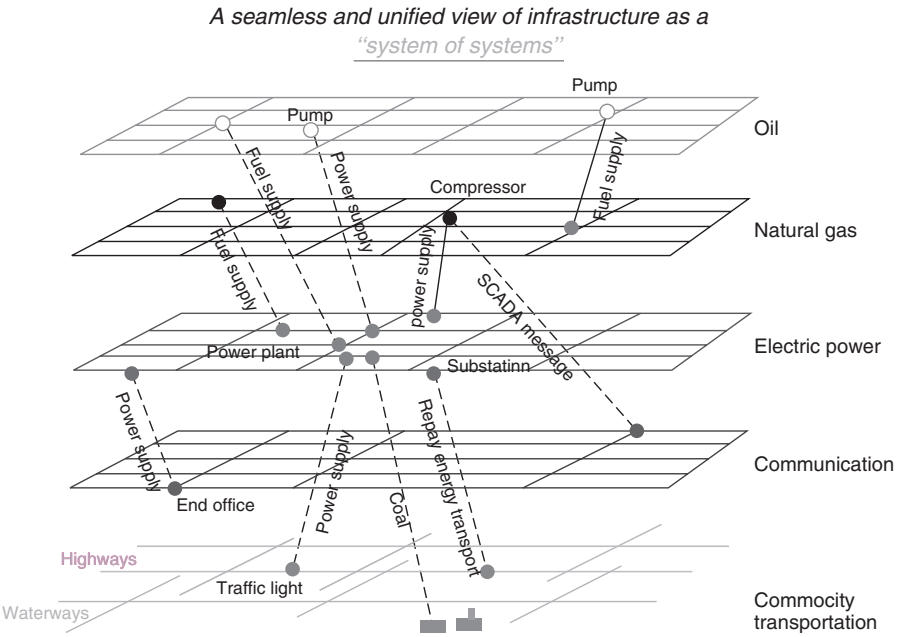



**FIGURE 2** Illustration of interdependencies among network-like infrastructures.

The horizontal layers in the figure represent dependencies within an infrastructure, and the vertical lines indicate interdependencies between infrastructures. Although Figure 2 shows only physical infrastructures, future capability will include nonphysical infrastructures as well, such as financial and/or other economic networks. IEISS does not replace single-infrastructure tools since existing technology analyzes these domains in sufficient detail. However, when this technology is applied to interdependent infrastructures, severe limitations usually exist.

IEISS relies on an actor-based (or object-oriented) modeling approach of infrastructures [1]. Each physical, logical, or functional entity in an infrastructure corresponds to a software a*ctor* (sometimes called a *software agent*) that has a variety of attributes and behaviors that mimic its real-world counterpart. The connections within or between infrastructures are represented by connections between the relevant actors, and the actors interact in the software through a message-passing protocol. Mathematically, infrastructures can be represented by graphs. Thus, any infrastructure(s) that can be represented in terms of a dependency graph can be modeled using this actor-based, message-passing representation. This approach is suitable for a wide variety of network-like infrastructures.

## 3 THE COMPLEXITY OF MULTIPLE INFRASTRUCTURES

A simulation of coupled infrastructures necessarily requires the use of multiple, heterogeneous algorithms [2]. Each infrastructure under consideration has its own dynamic laws and, thus, its own types of algorithms. It may be useful to mix different solution methods in the same simulation because of their varying accuracy and speed or to compare the

results of simulations using different algorithms. Ideally, "pluggable" algorithms could be attached individually to each actor in the system or to groups of actors. Mixtures of algorithms may be required by geography, infrastructure, or time.

Because of the potential complexity of coupled infrastructures, it is important that the solution algorithms be able to handle problems involving the "forward" simulation of systems and the "inverse" search problems. That is, given an initial state of the system, its evolution could be followed forward in time or, given the final state (typically involving loss of service), initial states could be determined that might evolve to this final state if a given number of contingencies were to occur.

When one or more interconnected components are forced out of service because of an operational or intentional failure, affected dependent or secondary components are also treated by IEISS as interdependency. This approach is based on the service area/outage area concept [3, 4]. For example, if an electric power substation is forced out of service, a polygonal representation of the service area normally served by the component is calculated. If components from other infrastructures lie within the calculated service area boundary and these components are dependent on the services of the failed substation, a propagation of the failure to dependent infrastructures is assumed. If the service areas of any affected infrastructures cannot be mitigated or reduced in extent through recovery measures, they are assumed to represent the outage area. This concept is further discussed in the next section.

Finally, if a service area can be estimated for all affected infrastructures, the simulation approach for interdependent cascading failures can be illustrated by the logic flow diagram shown in Figure 3. The simulation is initiated by creating a "contingency" event that

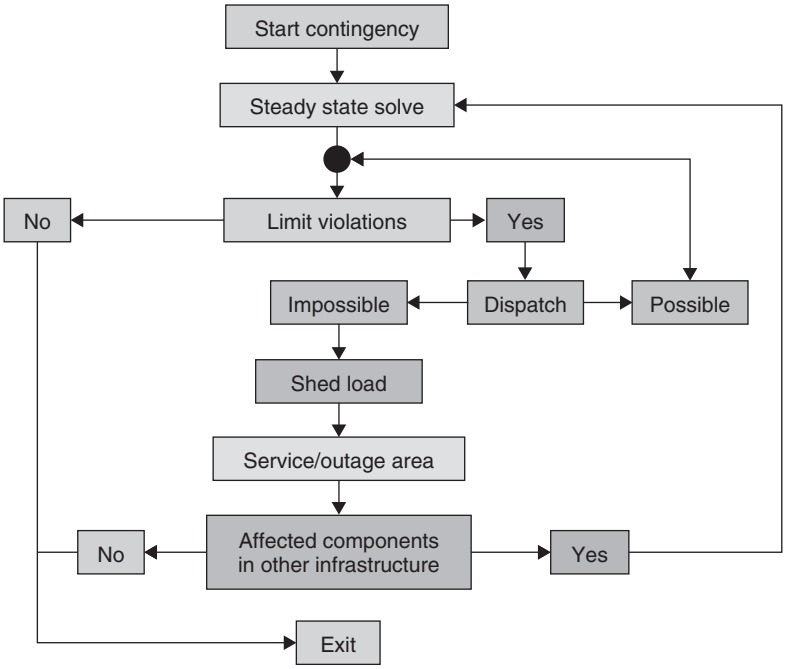



**FIGURE 3** IEISS logic diagram describing network limit violations.

involves single (or multiple) outages in one or more infrastructures. Steady-state solutions are then obtained for all infrastructures with key attributes reported (e.g. pressure or flow). If an attribute is not within its normal operating range, for example, a pipeline is operating above its maximum allowable operating pressure, the associated components are subject to limit violations [5]. Limit violations must be mitigated or else severe consequences can result. Mitigation can be accomplished by a variety of measures such as dispatching or reducing demand. Dispatching requires adjustments to operating parameters of variable equipment such as generators or compressors. The dispatch box shown in Figure 3 contains algorithms to eliminate limit violations.

If the contingency can be mitigated by dispatching, limit violations are rechecked and the simulation is ended ("possible"). However, if further violations exist ("impossible"), IEISS sheds customer load near the contingency and then calculates outage areas. Affected components in other infrastructures are also identified. Another simulation will be required to determine if loss of the affected components cause violations within their respective infrastructure(s) or propagation of effects is stopped. The IEISS simulation process ends when all limit violations have been eliminated. The final result is a list of outage areas, failed components, history of cascading events, and so on.

## 4 IEISS CASE STUDY: URBAN INTERDEPENDENCIES

A key element in modeling interdependent infrastructures is the ability to predict the propagation of a perturbation. This condition results from a component failure created within an infrastructure, which cascades to other interdependent infrastructures. This cascading effect is a key issue, but usually the least understood phenomenon. Although short-term service interruptions of energy infrastructures are routine in many areas, catastrophic system failures, or large-scale blackouts, are rare events. As urban infrastructures become more complex and interdependent, the probability of having large-scale outages increases.

The underlying concepts of interdependency and application of IEISS are illustrated by a fictitious example. Interconnected electric power and natural gas component attributes were input into the IEISS model, which are notionally representative of urban networks in most US cities. The model incorporated multiple layers of components operating at different voltages and pressures. Because of the network-like features, disruptions to key components in one layer can affect the operation of colocated components in other layers, creating an interdependency event. During the analysis, IEISS reported greater effects than would have resulted if single components were individually outaged.

The first phase of this event requires simultaneous loss of two components: an electric substation and a natural gas pipeline junction. An outage of the natural gas pipeline junction disrupts natural gas delivery to gas-fired power plants located approximately 10 miles to the south. The simultaneous outage of a 230-kV electric substation completes the initiating event. Components "A" and "B" are located approximately 30 miles apart as shown in Figure 4.

Following the initial loss of components, high-voltage electric transmission lines will be overloaded. This condition forces the utility to shed customer load to avoid equipment

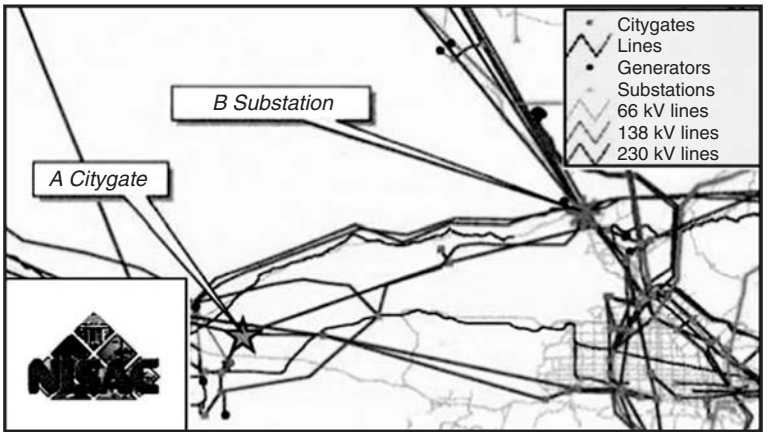



**FIGURE 4** Natural gas (NG) and electric power (EP) components in the IEISS model, highlighting locations of outaged nodes.

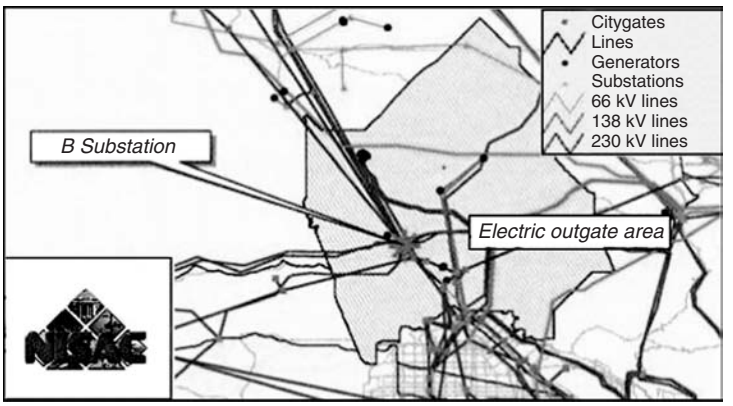



**FIGURE 5** Outage area (gray shade) resulting from the loss of substation "B".

damage and to stabilize the local network. In turn, this action will create an outage area, as shown in Figure 5.

The outaged electric substation provides connections to areas west of this location. Under normal operating conditions, electric generators are capable of providing more power than needed locally, so excess is exported to the east. Following a loss of electric generation due to pipeline junction "A" outage, customer demand must be met by supplying from the east. Three 230-kV transmission lines normally support this power flow. However, two of three lines originate at the outaged electric substation "B". Since this component is outaged, power can only be supplied by a single 230-kV line, which is severely overloaded. The result is an additional area of customer load shed, as shown in Figure 6.

Because large area is affected by this event, many businesses and facilities critical to continued operation of urban infrastructure would lose electricity and natural gas

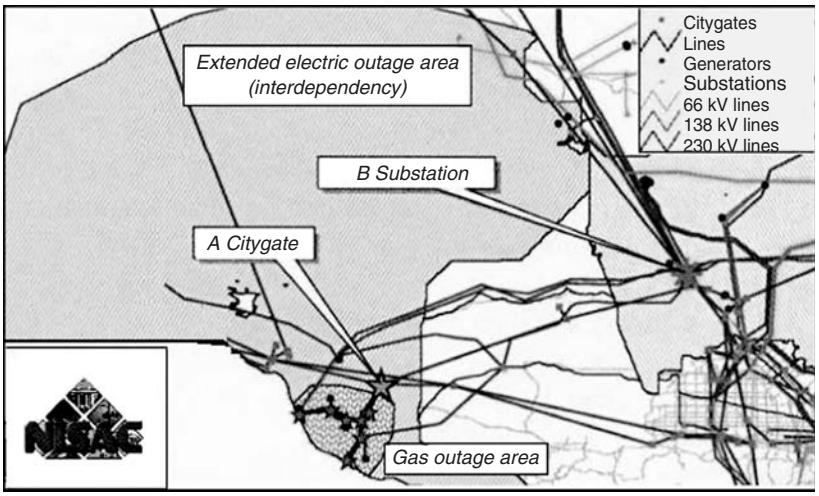



**FIGURE 6** Additional load shed due to transmission line overload from electric substation "B" results in the final interdependency event.

service. The total outage area encloses nearly 2700 sq. miles. On the basis of average business sales density, the direct cost of a 3-day interdependency outage would total approximately $150 million. Indirect costs due to supply chain disruptions, noninsured loss of perishable goods, and related items may also be significant. In addition, key emergency facilities such as hospitals, telecommunication end offices, police, and fire stations would be outaged forcing extended reliance on emergency backup power.

## REFERENCES

1. Bush, B. W., Bush, A. B., Fisher, R., Folga, S., Giguere, P., Holland, J., Hurford, J., Kavicky, J., Linger, S., McCown, A., McLamore, M., Pontante, E., Rothrock, L., Salazar, M., Shamsuddin, S., Unal, C., Visarraga, D., and Werley, K. (2005). *Interdependent Energy Infrastructure Simulation System–IEISS Version 2.1 Technical Reference Manual*, Report LANL-D4-05-0027, Los Alamos National Laboratory.
2. Unal, C., Werley, K. A., and Gigue, P. (2001). *Energy Interdependence Modeling and Simulation*, Report LA-UR-01-1879, Los Alamos National Laboratory.
3. Linger, S. P., Toole, G. L., and McPherson, T. (2001). *A Primer on Estimating Electrical Service and Outage Areas Using GIS and Cellular Automata Based Methods*, Report LA-UR-01-0490, Los Alamos National Laboratory.
4. Werley, K. A. (2002). *Constrained Cellular Colonization (C3) for Estimating Service and Outage Areas in Electric Power Transmission Networks (Rev. 4)*, Report LA-UR-01-4845, Los Alamos National Laboratory.
5. Werley, K. A. (2001). *An AC Dispatcher for Relieving Problems within Electric Power Transmission Networks*, Report LA-UR-03-8266, Los Alamos National Laboratory, pp. 1–16.

## FURTHER READING

National Infrastructure Protection Plan (2006). http://www.dhs.gov/xprevprot/programs/editorial_0827.shtm.

# SELF-HEALING AND RESILIENT ENERGY SYSTEMS

S. MASSOUD AMIN
*University of Minnesota, Minneapolis, Minnesota*

## 1 INTRODUCTION

The rise of our nation into a global economic power, which began with the opening of a vast continent in the mid-1800s by the railroads, was followed in the nineteenth century by expansion of the networks of commerce, navigable waterways, transportation, water supply and wastewater, dams, electric power networks, and rural electrification (in the early to mid-twentieth century), aviation, transit, and highways. This has dramatically transformed our nation and the resultant economic output has been unprecedented in history.

The tremendous value of infrastructure systems such as roads and bridges and the nation that help make possible indispensable activities of our modern societies cannot be overstated. I would submit that along with our bricks and mortar infrastructure—railroads, highways, bridges, seaports, and airports—another important part is the "hidden infrastructure" that supports the workings of all aspects of our $14 trillion economy.[2]

## 2 THE BIGGER PICTURE

Energy, telecommunications, transportation, and financial infrastructures are becoming increasingly interconnected, thus posing new challenges for their secure, reliable, and efficient operation. All of these infrastructures are themselves complex networks, geographically dispersed, nonlinear, and interacting both among themselves and with their

[1]Honeywell/H.W. Sweatt Chair in Technological Leadership, Director of the Center for the Development of Technological Leadership (CDTL), Professor of Electrical and Computer Engineering, and University Distinguished Professor. Contact information: amin@umn.edu, or http://umn.edu/amin.

[2]A 24-page special feature in *The Wilson Quarterly* for Spring 2008 (Vol. 32, No. 2) includes three articles under the heading, "BACKBONE: Infrastructure for America's Future." The three are "The Secret Is the System," "Get Smart," and "Built to Last." An introduction notes that "building tomorrow's infrastructure will pose larger political and technological challenges than ever before-with potential payoffs to match." Examples cited are the huge new water tunnel being dug beneath New York City, started in 1970 and to be completed by 2020; the collapse of the I-35W bridge in Minneapolis, the 2003 blackout affecting 50 million people, and the proposed North American Super Corridor, from Mexico to Canada that would create a road, rail, and shipping system around the existing I-35. Some excerpts: Shopping for Infrastructure The American Society of Civil Engineers *Report Card for America's Infrastructure* (2005) offers a daunting menu of future needs and calls for more than $300 billion in additional annual spending (for more information please see http://www.wilsoncenter.org/index.cfm).

human owners, operators, and users. No single entity has complete control of these multiscale distributed, highly interactive networks, nor does any such entity have the ability to evaluate, monitor, and manage them in real time. In fact, the conventional mathematical methodologies that underpin today's modeling, simulation, and control paradigms are unable to handle the complexity and interconnectedness of these critical infrastructures.

Power, telecommunications, banking and finance, transportation and distribution, and other infrastructures are becoming more and more congested partially due to dramatic population growth, particularly in urban centers. These infrastructures are increasingly vulnerable to failures cascading through and between them. A key concern is the avoidance of widespread network failure due to cascading and interactive effects. Moreover, interdependence is only one of several characteristics that challenge the control and reliable operation of these networks. Other factors that place increased stress on the power grid include dependencies on adjacent power grids (increasing because of deregulation), telecommunications, markets, and computer networks. Furthermore, reliable electric service is critically dependent on the whole grid's ability to respond to changed conditions instantaneously.

Secure and reliable operation of complex networks poses significant theoretical and practical challenges in analysis, modeling, simulation, prediction, control, and optimization. The pioneering initiative in the area of complex interactive networks and infrastructure interdependency modeling, simulation, control, and management was launched and successfully carried out during 1998–2002, through the Complex Interactive Networks/Systems Initiative (CIN/SI). It studied closely the challenges to the interdependent electric power grid, energy, sensing and controls, communications, transportation, and financial infrastructures.

It comprised six university research groups consisting of 108 university faculty members and over 220 researchers who were involved in the joint Electric Power Research Institute (EPRI) and US Department of Defense program. During 1998–2002, CIN/SI developed modeling, simulation, analysis, and synthesis tools for damage-resilient control of the electric power grid and interdependent infrastructures connected to it. This work showed that the grid can be operated close to the limit of stability given adequate situational awareness combined with better security of communications and controls. A grid operator is similar to a pilot flying an aircraft as in monitoring how the system is being affected, how the "environment" is affecting it, and having a solid sense of how to steer it in a stable fashion.

In recent decades, in light of increased demand, we have reduced the generation and transmission capacity margins of the electric power grid, and we are indeed flying closer to the edge of the stability envelope. Ongoing programs at EPRI, Department of Energy (DOE) are continuing pursuit of these objectives.

Earlier work by the author during the 1990s on damaged F-15 aircraft in part, provided background for the creation, successful launch, and management of research programs for the electric power industry, including the EPRI/DOD CIN/SI mentioned above, which involved six university research consortia along with two energy companies, to address challenges posed by our critical infrastructures. This work was done during the period from 1998 to early 2002. CIN/SI laid the foundation for several ongoing initiatives on the self-healing infrastructure and subsets focusing on smart reconfigurable electrical networks. These have now been under development for some time at several organizations, including programs sponsored by the National Science Foundation (NSF), DOD,

DOE, and EPRI (including the "Intelligrid" program), and the US DOE's "Gridwise" and "Modern Grid" initiative.

To provide a context for this, the EPRI/DOD CIN/SI aimed to develop modeling, simulation, analysis, and synthesis tools for robust, adaptive, and reconfigurable control of the electric power grid and infrastructures connected to it. In part, this work showed that the grid can be operated close to the limit of stability given adequate situational awareness combined with better sensing of system conditions and communication controls. A grid operator steers it in a stable fashion by keeping the lines within their operating limits while helping a instantaneous balance between loads (demand) and available generation. Grid operators often make these quick decisions under considerable stress. Given that in recent decades we have reduced the generation and transmission capacity, we are indeed flying closer to the edge of the stability envelope.

As an example, one aspect of the Intelligrid program is aimed at enabling grid operators have greater look-ahead capability and foresight, overcoming limitations of the current schemes which at best have over a 30-seconds' delay in assessing system behavior. This is analogous to driving to the car by looking into the rear-view mirror instead of the road ahead. This tool using advanced sensing, communication, and software module was proposed during 2000 to 2001 and the program was initiated in 2002 by the author while at EPRI, under the Fast Simulation and Modeling (FSM) program. This advanced simulation and modeling program promotes greater grid self-awareness and resilience in times of crisis, in three ways: by providing faster-than-real-time, look-ahead simulations (analogous to master chess players rapidly expanding and evaluating their various options under time constraints) and thus avoiding previously unforeseen disturbances; by performing what-if analysis for large-region power systems from both operations and planning points of view; and by integrating market, policy, and risk analysis into system models, and quantifying their integrated effects on system security and reliability.

## 3 INFRASTRUCTURES UNDER THREAT

The terrorist attacks of September 11th exposed critical vulnerabilities in America's essential infrastructures: never again can the security of these fundamental systems be taken for granted. Electric power systems constitute *the* fundamental infrastructure of modern society. A successful terrorist attempt to disrupt electricity supplies could have devastating effects on national security, the economy, and the life of every citizen. Yet, power systems have widely dispersed assets that can never be absolutely defended against a determined attack.

The growing potential for infrastructural problems stems from multiple sources, including system complexity, deregulation, economic effects, power market impacts, and human error. The existing power system is also vulnerable to natural disasters and intentional attacks (terrorism). Regarding the latter, a November 2001 EPRI assessment developed in response to the September 11th attacks highlights three kinds of potential threats to the US electricity infrastructure.

We discuss them briefly and in very broad terms, without providing a "blue book" for potential attackers: The first is attacks *upon* the power system. In this case, electricity infrastructure is the primary target—with ripple effects, in terms of outages extending into the customer base. The point of attack could be a single component, such as a critical

substation or a transmission tower. There could also be a simultaneous, multipronged attack intended to bring down the entire grid in a specific region of the United States An attack could also target electricity markets which are highly vulnerable because of their transitional status.

The second type of attack is *by* the power system. In this case the ultimate target is the population, using parts of the electricity infrastructure as a weapon—similar to the way our transportation and mail delivery systems were used against our nation. Power plant cooling towers, for example, could be used to disperse chemical or biological agents.

The third means is attack *through* the power system. In this case, the target is the civil infrastructure. Utility networks include multiple conduits for attack, such as lines, pipes, underground cables, tunnels, and sewers. An electromagnetic pulse, for example, could be coupled through the grid with the intention of damaging computer and/or telecommunications infrastructure.

As seen from these scenarios, the specter of terrorism raises a profound dilemma for the electric power industry: How to make the electricity infrastructure more secure without compromising productivity in today's complex, highly interconnected electric networks? Resolving this dilemma requires short-term and long-term technology development and deployment, affecting fundamental characteristics of today's power systems.

The North American electric power system needs a comprehensive strategy to prepare for the diverse threats posed by terrorism. Such a strategy should both increase protection of vital industry assets and assure the public that they are well protected. A number of actions will need to be considered in formulating an overall security strategy:

- The grid must be made secure from cascading damage.
- Pathways for environmental attack must be sealed off.
- Conduits for attack must be monitored, sealed off, and "sectionalized" under attack conditions.
- Critical controls and communications must be made secure from penetration by hackers and terrorists.
- Greater intelligence must be built into the grid to provide flexibility and adaptability under attack conditions, including automatic reconfiguration.
- Ongoing security assessments, including use of game theory to develop potential attack scenarios, will be needed to ensure that the power industry can stay ahead of changing vulnerabilities.

A survey of electric utilities revealed real concerns about grid and communications security on the perceived threats to utility control centers. The most likely threats were bypassing controls, integrity violations, and authorization violations, with four-in-ten rating each as either a 5 or 4, out of 5. Concern about potential threats generally increased as the size of the utility (peak load) increased.

The system's equipment and facilities are dispersed throughout the North American continent, which complicates absolute protection of the system from a determined terrorist attack. In addition, another complexity needs to be considered—the power delivery systems' physical vulnerabilities, and susceptibility to disruptions in computer networks and communication systems. For example, terrorists might exploit the increasingly centralized

control of the power delivery system to magnify effects of a localized attack. Because many consumers have become more dependent on electronic systems that are sensitive to power disturbances, an attack that leads to even a momentary interruption of power can be costly. A 20-min outage at an integrated circuit fabrication plant, for example, could cost US$30 million.

**The Grid Then and Now**

*The first grids*. The worldwide electrical grid deployment, now costing trillions of dollars and reaching billions of people, began very humbly. The first grids came into being in the 1880s, for bringing electrical energy to a variety of customers for a variety of uses; at first mostly for illumination but later for turning power machines and moving trolley cars. The most important of these early grids, the first established big city grid in North America, was the network built by Thomas Edison in lower Manhattan. From its power station on Pearl Street, practically in the shadow of the Brooklyn Bridge, Edison's company supplied hundreds and then thousands of customers. Shortly thereafter, Edison's patented devices, and those of his competitors—devices such as bulbs, switching devices, generators, and motors—were in use, in new grids in towns all over the industrialized world.

**Grid Overview**

- Power, communications, and computing are all converging, making entire systems as sensitive as the most sensitive component.
- Secure and reliable combined electric power, communications, fuel supply, and financial networks are essential to today's microprocessor-based economy, public health and safety, and overall quality of life.
- The demands of our secure digital economy are outpacing the electricity and communication infrastructures that support it.
- It costs the United States $75–180 billion in annual losses from power outages and disturbances. On any day, typically half a million people are without power for 2 or more hours.
- The US power grid operates under ever more stress from increasing electrical traffic and from a changing economic climate. Here are four notable grid issues: (i) the regulatory problem: federal and state grid guidelines often conflict; (ii) the investment problem: demand for power is increasing faster than new grid construction; (iii) the reliability problem: operating rules should keep the grid up and running more of the time; (iv) the marketplace problem: in many instances, the production, transmission, and distribution of power is subject to unfair competition.
- Operating the grid will increasingly come to resemble the flight of combat aircraft, including the use of complex adaptive software.

**Smart Self-Healing Grid**

- What is "self-healing?"
  - A system that uses information, sensing, control and communication technologies to allow it to deal with unforeseen events and minimize their adverse impact.
- Why is self-healing concept important to the energy infrastructure?
  - It is a secure "architected" sensing, communications, automation (control), and energy-overlaid infrastructure as an integrated, reconfigurable, and electronically controlled system that will offer unprecedented flexibility and functionality. It will also improve system availability, security, quality, resilience and robustness.

## 4 A STRESSED INFRASTRUCTURE

The major outage on 14 August 2003, in the eastern United States and the earlier California power crisis in 2000–2001 are only the most visible parts of a larger and growing US energy crisis from inadequate investments in the infrastructure, leading to a fundamental imbalance between growing demand and an almost stagnant supply. The imbalance had been brewing for many years and is prevalent throughout the nation.

From a broader view, the North American electricity infrastructure is vulnerable to increasing stresses from several sources. One stress is caused by an imbalance between growth in demand for power and enhancement of the power delivery system to support this growth. From 1988 to 1998, the United States' electricity demand rose by nearly 30%, but the capacity of its transmission network grew by only 15%. This disparity is likely to increase from 1999 to 2009: analysts expect demand to grow by 20%, while planned transmission systems grow by only 3.5%. Along with that imbalance, today's power system has several sources of stress:

- *Demand is Outpacing Infrastructure Expansion and Maintenance Investments.* Generation and transmission capacity margins are shrinking and unable to meet peak conditions particularly when multiple failures occur, while electricity demand continues to grow.
- *The Transition to Deregulation is Creating New Demands That Are Not Being Met.* The electricity infrastructure is not being expanded or enhanced to meet the demands of wholesale competition in the industry; so connectivity between consumers and markets is at a gridlock.
- *The Present Power Delivery Infrastructure Cannot Adequately Handle Those New Demands of High End Digital Customers and Twenty-First-Century Economy.* It cannot support the levels of security, quality, reliability, and availability needed for economic prosperity.
- *The Infrastructure Has Not Kept Up with New Technology.* Many distribution systems have not been updated with current technology including IT.

- *Proliferation of Distributed Energy Resources (DERs).* DER includes a variety of energy sources—microturbines, fuel cells, photovoltaics, and energy storage devices—with capacities from approximately 1 kW to 10 MW. DER can play an important role in strengthening energy infrastructure. Currently, DER accounts for about 7% of total capacity in the United States, mostly in the form of backup generation, yet very little is connected to the power delivery system. By 2020, DER could account for as much as 25% of total US capacity, with most DER devices connected to the power delivery system.
- *Return on Investment(ROI) Uncertainties Are Discouraging Investments in the Infrastructure Upgrades.* Investing new technology in the infrastructure can meet these aforementioned demands. More specifically, according to a June 2003 report by the NSF, R&D spending in the United States as a percent of net sales was about 10% in the computer and electronic products industry and 12% for the communication equipment industry in 1999. Conversely, R&D investment by electric utilities was less than 0.5% during the same period. R&D investment in most other industries is also significantly greater than that in the electric power industry.
- *Concern about the National Infrastructure's Security (1).* A successful terrorist attempt to disrupt electricity supplies could have devastating effects on national security, the economy, and human life. Yet power systems have widely dispersed assets that can never be absolutely defended against a determined attack.

Competition and deregulation have created multiple energy producers that share the same energy distribution network, one that now lacks the carrying capacity or safety margin to support anticipated demand. Investments in maintenance, and research and development continue to decline in the North American electrical grid. Yet, investment in core systems and related IT components are required to ensure the level of reliability and security that users of the system have come to expect.

From a national security viewpoint, in the aftermath of the tragic events of September 11th and recent natural disasters and major power outages, there are increased national and international concerns about the security, resilience and robustness of critical infrastructures in response to evolving spectra of threats. Secure and reliable operation of these networks is fundamental to national and international economy, security and quality of life[3].

[3]Executive Order 13010, signed by President Clinton in 1996, defined critical infrastructures as "so vital that their incapacity or destruction would have debilitating impact on the defense or economic security of the United Stares" and included "telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water-supply systems, emergency services and continuity of government." The US Department of Homeland Security (DHS) in the National Infrastructure Protection Plan has expanded the concept to include "key resources" and added food and agriculture, health and health care, defense industrial base, information technology, chemical manufacturing, postal and shipping, dams (including locks and levees), government facilities, commercial facilities, and national monuments and icons. The National Infrastructure Improvement Act (S. 1926) defines "infrastructure" as any of a number of components of the transportation system, water supply and control facilities, resource recovery facilities, and solid waste disposal facilities." While in our research we focus on a subset of (i) energy and power, (ii) cyber and telecommunications, (iii) transportation, (iv) banking and finance, and their couplings and interdependencies; elsewhere in our nation, all the 17 sectors identified by DHS are under study by the ASME, DHS, National Labs, and other organizations.

## 5 WHERE ARE WE AND HOW DID WE GET HERE?

The existing electricity infrastructure evolved to its technology composition today from the convolution of several major forces, only one of which is technologically based. Today opportunities and challenges persist in worldwide electric power networks, these include: reducing transmission congestion, increasing system/cyber security, increasing overall system and end-use efficiency while maintaining reliability, and so on. Many other challenges engage those who plan for the future of the power grid: producing power in a sustainable manner (embracing renewable fuels while accounting for their scalability limitations, for example, increased use of land and natural resources to produce more renewable electricity will not be sustainable, thus not being able to lower emissions from existing generators), delivering electricity to those who do not have it (not just on the basis of fairness but also because electricity is the most efficient form of energy, especially for things like lighting), and using electricity more wisely as a tool of economic development, and pondering the possible revival of advanced nuclear reactor construction. To prepare for a more efficient, resilient, secure and sustainable electrical system it is helpful to remember the historical context, associated bottlenecks and forcing functions:

As the readers of this article know, the trends of worldwide electrical grid deployment, costing trillions of dollars and reaching billions of people, began very humbly. Some obvious electrical and magnetic properties were known in antiquity. In the seventeenth and eighteenth centuries, partially through scientific experiments and partially through parlor games, more was learned about how electric charge is conducted and stored. But only in the nineteenth century, with the creation of powerful batteries, and through insights about the relations between electric and magnetic force could electricity in wires service large-scale industries—first the telegraph and then telephones.

And only in the 1880s did the first grids come into being for bringing electrical energy to a variety of customers for a variety of uses, at first mostly for illumination but later for turning power machines and moving trolley cars. The most important of these early grids, the first established big city grid in North America, was the network built by Thomas Edison in lower Manhattan. From its power station on Pearl Street, practically in the shadow of the Brooklyn Bridge, Edison's company supplied hundreds and then thousands of customers. Shortly thereafter, Edison's patented devices, and those of his competitors—devices such as bulbs, generators, switching devices, generators, and motors—were in use in new grids in towns all over the industrialized world.

From a historical perspective the electric power system in the United States evolved in the first half of the twentieth century without a clear awareness and analysis of the system-wide implications of its evolution. In 1940, 10% of the energy consumption in America was used to produce electricity. By 1970, this had risen to 25%, and by 2002 it had risen to 40%. (Worldwide, current electricity production is near 15,000 billion kWh/year, with the United States, Canada, and Mexico responsible for about 30% of this consumption.) This grid now underlies every aspect of our economy and society, and it has been hailed by the National Academy of Engineering as the twentieth century's engineering innovation that has been most beneficial to our civilization. The role of electric power has grown steadily in both scope and importance during this time and electricity is increasingly recognized as a key to societal progress throughout the world, driving economic prosperity, security and improving the quality of life. Still it is noteworthy that at the time of this writing, there are about 1.4 billion people in the world

with no access to electricity, and another 1.2 billion people have inadequate access to electricity (meaning that they experience outages of 4 h or longer per day).

Once "loosely" interconnected networks of largely local systems, electric power grids increasingly host large-scale, long-distance wheeling (movement of wholesale power) from one region or company to another. Likewise, the connection of distributed resources, primarily small generators at the moment, is growing rapidly. The extent of interconnectedness, like the number of sources, controls, and loads, has grown with time. In terms of the sheer number of nodes, as well as the variety of sources, controls, and loads, electric power grids are among the most complex networks made.

In the coming decades, electricity's share of total energy is expected to continue to grow, as more efficient and intelligent processes are introduced into this network. Electric power is expected to be the fastest-growing source of end-use energy supply throughout the world. To meet global power projections, it is estimated by the US DOE/EIA that over $1 trillion will have to be spent during the next 10 years. The electric power industry has undergone a substantial degree of privatization in a number of countries over the past few years. Growth in power generation capacity is expected to be particularly strong in the rapidly growing economies of Asia, with China leading the way.

The electric power grid's emerging issues include: creating distributed management through using distributed intelligence and sensing; integration of renewable resources; use of active-control high voltage devices; developing new business strategies for a deregulated energy market; and ensuring system stability, reliability, robustness, and efficiency in a competitive marketplace and carbon-constrained world.

In addition, the electricity grid faces (at least) three looming challenges: its organization, its technical ability to meet 25-year and 50-year electricity needs, and its ability to increase its efficiency without diminishing its reliability and security.

As an example of historical bifurcation points, the 1965 Northeast blackout not only brought the lights down, it also marked a turn in grid history. The previous economy of scale, according to which larger generators were always more efficient than small machines, no longer seemed to be the only risk-managed option. In addition, in the 1970s two political crises—the Middle East war of 1973 and the Iranian Revolution in 1979—led to a crisis in fuel prices and a related jump in electric rates. For the first time in decades, demand for electricity stopped growing. Moreover, the prospects of power from nuclear reactors, once so promising, now faced public resistance and the resultant policy threats. Accidents at Brown's Ferry, Alabama in 1974 and Three Mile Island, Pennsylvania in 1979, and rapidly escalating construction costs caused a drastic turnaround in orders for new facilities. Some nuclear plants already under construction were abandoned.

In the search for a new course of action, conservation (using less energy) and efficiency measures (to use available energy more wisely) were put into place. Electrical appliances were reengineered to use less power. For example, while on the average today's refrigerators are about 20% larger than those made 30 years ago, they use less than half the electricity of older models. Furthermore, the Public Utility Regulatory Policy Act (PURPA) of 1978 stipulated that the main utilities were required to buy the power produced by certain independent companies which cogenerated electricity and heat with great efficiency, providing the cost of the electricity was less than the cost it would take the utilities to make it for their own use.

What had been intended as an effort to promote energy efficiency, turned out, in the course of the 1980s and 1990s, to be a major instigator of change in the power industry

as a whole. First, the independent power producers increased in size and in number. Then they won the right to sell power not only to the neighboring utility but also to other utilities further away, often over transmission lines owned by other companies. With the encouragement of the Federal Energy Regulatory Commission (FERC), utilities began to sell off their own generators. Gradually the grid business, which for so long had operated under considerable government guidelines since so many utilities were effective monopolies, became a confusing mixture of regulated and unregulated companies.

Opening up the power industry to independent operators, a business reformation underway for some years in places like Chile, Australia, and Britain (where the power denationalization process was referred to as "liberalization"), proved to be a bumpy road in the United States. For example, in 2001 in the state of California, the effort to remove government regulations from the sale of electricity, even at the retail level, had to be rescinded in the face of huge fluctuations in electric rates, rolling blackouts, and amid allegations of price-fixing among power suppliers. Later that year, Enron, a company that had grown immense through its pioneering ventures in energy trading and providing energy services in the new freed-up wholesale power market, declared bankruptcy.

Restructuring of the US power grid continues. Several states have put deregulation into effect in a variety of ways. New technology has helped to bring down costs and to address the need for reducing emission of greenhouse gases during the process of generating electricity. Examples include high efficiency gas turbines, integrated "microgrids" of small generators (sometimes in the form of solar cells or fuel cells), and a greater use of wind turbines.

Much of the interest in restructuring has centered around the generation part of the power business and less on expanding the transmission grid itself. About 25 years ago, the generation capacity margin, the ability to meet peak demand, was between 25 and 30%. It has now reduced to less than half and is currently at about 10–15%. These "shock absorbers" have been shrinking; for example, during the 1990s actual demand in the United States increased by some 35%, while transmission capacity has increased by only 18%. In the current decade, the demand is expected to grow by about 20%, with new transmission capacity lagging behind at under 4% growth.

In the past, extra generation capacity served to reduce the risk of generation shortages in case equipment failed and had to be taken out of production, or in case there was an unusually high demand for power, such as on very hot or cold days. As a result capacity margins, both for generation and transmission, are shrinking. Other changes add to the pressure on the national power infrastructure as well. Increasing interregional bulk power transactions strain grid capacity. New environmental considerations, energy conservation efforts, and cost competition require greater efficiency throughout the grid.

As a result of these "diminished shock absorbers," the network is becoming increasingly stressed, and whether the carrying capacity or safety margin will remain to support anticipated demand is in question. The most visible parts of a larger and growing US energy crisis is the result of years of inadequate investments in the infrastructure. The reason for this neglect is caused partly by uncertainties over what government regulators will do next and what investors will do next.

Growth, environmental issues, and other factors contribute to the difficult challenge of ensuring infrastructure adequacy and security. Not only are infrastructures becoming more complexly interwoven and more difficult to comprehend and control, there is less investment available to support their development. Investment is down in many industries. For the power industry, direct infrastructure investment has declined in an

environment of regulatory uncertainty due to deregulation, and infrastructure R&D funding has declined in an environment of increased competition because of restructuring. Electricity investment was not large to begin with. Presently the power industry spends a smaller proportion of annual sales on R&D than do the dog foods, leather, insurance, or many other industries—less than 0.3% or about $600 million per year.

Most industry observers recognize this shortage of transmission capability, and indeed many of the large blackouts in recent years can be traced to transmission problems, either because of faults in the lines themselves or in the coordination of power flow over increasingly congested lines. However, in the need to stay "competitive," many energy companies, and the regional grid operators that work with them, are "flying" the grid with less and less margin for error. This means keeping costs down, not investing sufficiently in new equipment, and not building new transmission highways to free up bottlenecks.

## 6 CHIEF GRID PROBLEMS

Several cascading failures during the past 40 years have spotlighted our need to understand the complex phenomena associated with power network systems and the development of emergency controls and restoration. In addition to the mechanical failures, overloading a line can create power-supply instabilities such as phase or voltage fluctuations. For an AC power grid to remain stable, the frequency and phase of all power generation units must remain synchronous within narrow limits. A generator that drops 2 Hz below 60 Hz will rapidly build up enough heat in its bearings to destroy itself. So circuit breakers trip a generator out of the system when the frequency varies too much. But much smaller frequency changes can indicate instability in the grid: in the Eastern Interconnect, a 30 MHz drop in frequency reduces power delivered by 1 GW.

According to data from the North American Electric Reliability Corporation (NERC) and analyses from the EPRI, average outages from 1984 to the present have affected nearly 700,000 customers per event annually. Smaller outages occur much more frequently and affect tens to hundreds of thousands of customers every few weeks or months, while larger outages occur every two to nine years and affect millions. Much larger outages affect seven million or more customers per event each decade. These analyses are based on data collected for the US DOE, which requires electric utilities to report system emergencies that include electric service interruptions, voltage reductions, acts of sabotage, unusual occurrences that can affect the reliability of bulk power delivery systems, and fuel problems.

Coupling these analyses with diminished infrastructure investments, and noting that the cross-over point for the utility construction investment versus depreciation occurred in 1995, we analyzed the number and frequency of major outages along with the number of customers affected during 1991–2005. These data from the NERC's Disturbance Analysis Working Group (DAWG) are a subset of the total outages that are required to be reported to DOE's EIA. Going through the more comprehensive data sets from DOE's EIA, during 2001–2005 there were 162 outages of 100 MW or more, and 150 outages affecting >50,000 consumers.

In addition, analyzing outages in 2006 (NERC's data), in 1 year we had: 24 occurrences over 100 MW and 34 occurrences over 50,000 or more consumers.

At the core of the power infrastructure investment problem lie two paradoxes of restructuring, one technical and one economic. Technically, the fact that electricity supply

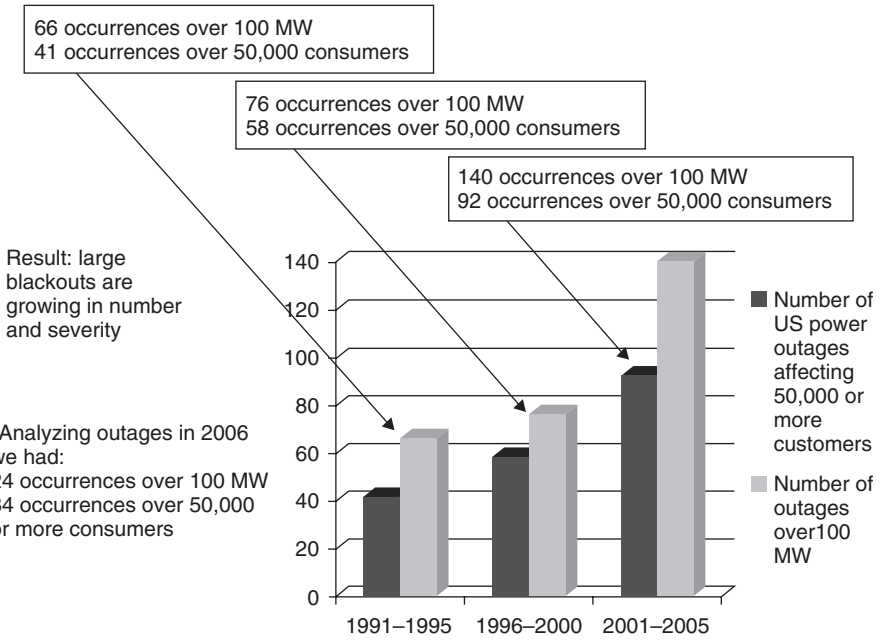



**FIGURE 1** Historical analysis of outages 1991–2005 (please also note that annual increases in load, about 2% per year, and corresponding increase in consumers should also be taken into account). [Data courtesy of NERC's Disturbance Analysis Working Group database.]

and demand must be in instantaneous balance at all times must be resolved with the fact that new power infrastructure is extraordinarily complex, time-consuming, and expensive to construct. Economically, the theory of deregulation aims to achieve the lowest price through increased competition. However, the market reality of electricity deregulation has often resulted in a business-focused drive for maximum efficiency to achieve the highest profit from existing assets, and not resulted in lower prices or improved reliability. Both the technical and economic paradoxes could be resolved by knowledge and technology.

Whether or not the power industry renews its traditional levels of investment in research and in new transmission lines, or the government clarifies its regulatory role in the making and dispatching of electricity, the grid will have to go on functioning. Fortunately, several recent innovations promise to make better use of the existing electrical network.

### Grid Challenges

Power produced in one place and used hundreds of miles away creates new opportunities, especially in terms of encouraging the construction of new power generation, possibly transmission, and in making full use of the power produced, rights of way and assets; but it also creates challenges:

1. *Regulatory Challenges.* More than ever power transmission is an interstate transaction. This has led to numerous conflicts between federal statutes applying

to energy and rules set up by public utility commissions in the various states. Generally the federal goal is to maximize competition, even if this means that traditional utility companies should divest themselves of their own generators. Since the 1990s, the process of unbundling utility services has brought about a major change in the way that energy companies operate. On the other hand, the goal of state regulators has generally been to provide reliable service and the lowest possible prices for customers in state.

2. *Investment Challenge.* Long-distance interstate routing, or "wheeling," of power, much encouraged by the federal government, has put the existing transmission network, largely built in the 1970s and 1980s in a time of sovereign utilities, under great stress. Money spent by power companies on research is much lower than in past decades. Reserve power capacity, the amount of power-making to be used in emergencies, which was 25–30% 25 years ago is now at 10–15%.
3. *Security, Reliability, and Innovation Challenges.* The August 2003 Northeast blackout, when operators did not know of the perilous state of their grid and how a local power shutdown could propagate for hundreds of miles, leaving tens of millions in the dark, demonstrated the need for mandatory reliability rules governing the daily operation of the grid. Such rules are now coming into place.
4. *Marketplace Challenges.* Some parts of the power business operate now without regulations. Other parts, such as the distribution of power to customers might still be regulated in many states, but the current trend is toward removing rules. The hope here is that rival energy companies, competing for customers, will offer more services and keep their prices as low as possible. Unfortunately, in some markets, this has the risk of manipulating the market to create energy shortages, even to the extent of requiring rolling blackouts in an effort to push prices higher.

These are recognized by the power companies and stakeholders in a rapidly changing marketplace. The public, usually at times of dramatic blackouts, and the business community, which suffers losses of over $80 billion per year, have taken notice. Even the Congress, which must negotiate the political fallout of power problems and establish laws governing the industry, takes up the problems of power transmission and distribution on a recurring basis, although usually in the context of the larger debate over energy policy. In the meantime, the US power grid has to be administered and electricity has to be delivered to millions of customers. Fortunately, many new remedies, software and hardware, are at hand.

## 7 OPTIONS AND POSSIBLE FUTURES—WHAT WILL IT TAKE TO SUCCEED?

Revolutionary developments in both information technology and material science and engineering promise significant improvement in the security, reliability, efficiency, and cost-effectiveness of all critical infrastructures. Steps taken now can ensure that critical

infrastructures continue to support population growth and economic growth without environmental harm.

As a result of increased demand, regulatory uncertainty, and the increasing connectedness of critical infrastructures, it is quite possible that in the near future the ability, for example, of the electricity grid to deliver the power that customers require in real time, on demand, within acceptable voltage and frequency limits, and in a reliable and economic manner may become severely tried. Other infrastructures may be similarly tested.

At the same time, deregulation and restructuring have added to the concern about the future of the electric power infrastructure (and other industries as well). This shift marked a fundamental change from an industry that was historically operated in a very conservative and largely centralized way as a regulated monopoly, to an industry operating in a decentralized way by economic incentives and market forces. The shift impacts every aspect of electrical power including its price, availability, and quality. For example, as a result of deregulation, the number of interacting entities on the electric grid (and hence its complexity) has been dramatically increasing while, at the same time, a trend toward reduced capacity margins has appeared. Yet when deregulation was initiated, little was known about its large-scale, long-term impacts on the electricity infrastructure, and no mathematical tools were available to explore possible changes and their ramifications.

It was in this environment of concern that the smart self-healing grid was conceived. One event in particular precipitated the creation of its foundations: a power outage that cascaded across the western United States and Canada on 10 August 10 1996. This outage began with two relatively minor transmission-line faults in Oregon. But ripple effects from these faults tripped generators at McNary dam, producing a 500 MW-wave of oscillations on the transmission grid that caused separation of the primary West Coast transmission circuit, the Pacific Intertie, at the California–Oregon border. The result: blackouts in 13 states and provinces costing some $1.5 billion in damages and lost productivity. Subsequent analysis suggests that shedding (dropping) some 0.4% of the total load on the grid for just 30 min would have prevented the cascading effects and prevented large-scale regional outages (note that load-shedding is not typically a first option for power grid operators faced with problems).

From a broader perspective, any critical national infrastructure typically has many layers and decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the constituent networks to remain operational and even automatically reconfigure in the event of local failures or threats of failure. In any situation subject to rapid changes, completely centralized control requires multiple, high data rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center. But all of these are liable to disruption at the very time when they are most needed (i.e. when the system is stressed by natural disasters, purposeful attack, or unusually high demand).

Had the results of the CIN/SI been in place at the time of the August 2003 blackout, the events might have unfolded very differently. For example, fault anticipators located at one end of the high voltage transmission lines would have detected abnormal signals, and made adaptive reconfigurations of the system to sectionalize the disturbance and minimize impact component failures several hours before the line failed. The look-ahead simulations would have identified the line as having a higher than normal probability of failure. Quickly, cognitive agents (implemented as distributed software and hardware in the infrastructure components and in control centers) would have run failure scenarios on their virtual system models to determine the ideal corrective response. When the

high voltage line actually failed, the sensor network would have detected the voltage fluctuation and communicated the information to reactive agents located at substations. The reactive agents would have executed the predetermined corrective actions, isolating the high voltage line and rerouting power to other parts of the grid. No customer in the wider area would even be aware that a catastrophic event had been impending, or have noticed the lights flickering.

Such an approach provides an expanded stability region with larger operational range. As the operating point nears the limit to how much the grid could have adapted (e.g. by automatically rerouting power and/or balancing by dropping a small amount of load or generation), rather than cascading failures and large-scale regional system blackouts, the system would be reconfigured to minimize severity or size of outages to shorten duration of brownouts or blackouts, and to enable rapid and efficient restoration.

This kind of distributed grid control has many advantages if coordination, communication, bandwidth, and security can be assured. This is especially true when the major components are geographically dispersed, as in a large telecommunications, transportation, or computer networks. It is almost always preferable to delegate as much of the control as is practical, to the local level.

The simplest kind of distributed control would combine remote sensors and actuators to form regulators (e.g. intelligent electronically controlled secure devices), and adjust their set points or biases with signals from a central location. Such an approach requires a different way of modeling—of thinking about, organizing and designing—the control of a complex, distributed system. Recent research results from a variety of fields, including nonlinear dynamical systems, artificial intelligence, game theory, and software engineering have led to a general theory of complex adaptive systems (CAS). Mathematical and computational techniques originally developed and enhanced for the scientific study of CAS provide new tools for the engineering design of distributed control so that both, centralized decision-making and the communication burden it creates, can be minimized. The basic approach to analyzing a CAS is to model its components as independent adaptive software and hardware "agents"—partly cooperating and partly competing with each other in their local operations while pursuing global goals set by a minimal supervisory function.

If organized in coordination with the internal structure existing in a complex infrastructure and with the physics specific to the components they control, these agents promise to provide effective local oversight and control without need of excessive communications, supervision, or initial programming. Indeed, they can be used even if human understanding of the complex system in question is incomplete. These agents exist in every local subsystem—from "horseshoe nail" up to "kingdom"—and perform preprogrammed self-healing actions that require an immediate response. Such simple agents are already embedded in many systems today, such as circuit breakers and fuses as well as diagnostic routines. The observation is that we can definitely account for loose nails and save the kingdom.

Another key insight came out of analysis of forest fires, by researchers at CalTech and UC-Santa Barbara, in the one of the six funded consortia, which I led during 1998–2002. They found forest fires to have "failure-cascade" behavior, similar to electric power grids. In a forest fire the spread of a spark into a conflagration depends on how close together the trees are. If there is just one tree in a barren field and it is hit by lightning, it burns but no big blaze results. But if there are many trees and they are close enough together—which is the usual case with trees because Nature is prolific and efficient in using resources—the single lightning strike can result in a forest fire that burns until it

reaches a natural barrier such as a rocky ridge, river, or road. If the barrier is narrow enough for a burning tree to fall across it, or it includes an inflammable flaw such as a wooden bridge, the fire jumps the barrier and burns on. It is the role of first-response wild-land fire fighters such as smoke jumpers, to contain a small fire before it spreads by reinforcing an existing barrier or scraping out a defensible fire line barrier around the original blaze.

Similar results hold for failures in electric power grids. For power grids, the "one-tree" situation is a case in which every single electric socket had a dedicated wire connecting it to a dedicated generator. A lightning strike on any wire would take out that one circuit and no more. But like trees in Nature, electrical systems are designed for efficient use of resources, which means numerous sockets served by a single circuit and multiple circuits for each generator. A failure anywhere on the system causes additional failures until a barrier—such as a surge protector or circuit breaker—is reached. If the barrier does not function properly or is insufficiently large, the failure bypasses it and continues cascading across the system.

These preliminary findings suggest approaches by which the natural barriers in power grids may be made more robust by simple design changes in the configuration of the system, and eventually show how small failures might be contained by active smoke-jumper-like controllers before they grow into large problems. Other research into fundamental theory of complex interactive systems explored means of quickly identifying weak links and failures within a system.

CIN/SI developed, among other things, a new vision for the integrated sensing, communications, and control of the power grid. Some of the pertinent issues are why or how to develop controllers for centralized versus decentralized control and issues involving adaptive operation and robustness to disturbances that include various types of failures.

Modern computer and communications technologies now allow us to think beyond the protection systems and the central control systems to a fully distributed system that places intelligent devices at each component, substation and power plant. This distributed system will enable us to build a truly smart grid.

One of the problems common to the management of central control facilities is the fact that any equipment changes to a substation or power plant must be described and entered manually into the central computer system's database and electrical one-line diagrams. Often this work is done some time after the equipment is installed and there is thus a permanent set of incorrect data and diagrams in use by the operators. What is needed is the ability to have this information entered automatically when the component is connected to the substation—much as a computer operating system automatically updates itself when a new disk drive or other device is connected.

## 8 THE ROAD AHEAD

A new mega-infrastructure is emerging from the convergence of energy (including the electric grid, water, oil and gas pipelines), telecommunications, transportation, Internet and electronic commerce. Furthermore, in the electric power industry and other critical infrastructures, new ways are being sought to improve network efficiency and eliminate congestion problems without seriously diminishing reliability and security.

Electric power systems constitute the fundamental infrastructure of modern society. Often continental in scale, electric power grids and distribution networks reach virtually every home, office, factory, and institution in developed countries and have made

remarkable, if remarkably insufficient, penetration in developing countries such as China and India.

The electric power grid can be defined as the entire apparatus of wires and machines that connects the sources of electricity and the power plants, with customers and their myriad needs. Once "loosely" interconnected networks of largely local systems, electric power grids now increasingly host large-scale, long-distance wheeling of power from one region to another. Likewise, the connection of distributed resources—at the moment, primarily small generators—are growing rapidly. The extent of interconnectedness, like the number of sources, controls, and loads, has grown with time. In terms of the sheer number of nodes, as well as the variety of sources, controls, and loads, electric power grids are among the most complex networks made.

Global trends toward interconnectedness, privatization, deregulation, economic development, accessibility of information, and the continued technical trend of rapidly advancing information and telecommunication technologies all suggest that the complexity, interactivity, and interdependence of infrastructure networks will continue to grow.

The existing electricity infrastructure evolved to its technology composition today from the convolution of several major forces, only one of which was technologically based. During the past 10 years, we have systematically scanned science and technology, investment, and policy dimensions to gain clearer insight on current science and technology assets when looked at from a consumer-centered future perspective, rather than just incremental contributions to today's electric energy system and services.

The goal of transforming the current infrastructures to self-healing energy-delivery, and computer and communications networks with the unprecedented robustness, reliability, efficiency and quality for customers and our society is ambitious. This will require addressing challenges and developing tools, techniques, and integrated probabilistic risk assessment/impact analysis for wide-area sensing and control for digital-quality infrastructure such as sensors, communication and data management, as well as improved state estimation, monitoring and simulation linked to intelligent and robust controllers leading to improved protection and discrete-event control. These follow-on activities will build on the foundations of CIN/SI and current programs that include self-healing systems and real-time dynamic information and emergency management and control.

More specifically, the operation of a modern power system depends on a complex system of sensors and automated and manual controls, all of which are tied together through communication systems. While the direct physical destruction of generators, substations, or power lines, may be the most obvious strategy for causing blackouts, activities that compromise the operation of sensors, communication and control systems by spoofing, jamming, or sending improper commands could also disrupt the system, cause blackouts, and in some cases result in physical damage to key system components. Hacking and cyber attacks are becoming increasingly common.

Most early communication and control systems used in the operation of the power system were carefully isolated from the outside world, and were separate from other systems such as corporate enterprise computing. However, economic pressures created incentives for utilities to make greater use of commercially available communications and other equipment that was not originally designed with security in mind. Unfortunately from a security perspective, such interconnections with office and electronic business systems through other layers of communications created vulnerabilities. While this problem is now well understood in the industry and corrective action is being taken, we are still in a transition period during which some control systems have been inadvertently exposed

to access from the Internet, intranets, and remote dial-up capabilities that are vulnerable to cyber intrusions.

Many elements of the distributed control systems now in use in power systems are also used in a variety of applications in process control, manufacturing, chemical process controls and refineries, transportation, and other critical infrastructure sectors and hence are vulnerable to similar modes of attack. Dozens of communication and cyber security intrusions, and penetration red-team "attacks" have been conducted by DOE, EPRI, electric utilities, commercial security consultants, KEMA, and others. These "attacks" have uncovered a variety of cyber vulnerabilities including unauthorized access, penetration and hijacking of control.

While some of the operations of the system are automatic, ultimately human operators in the system control center make decisions and take actions to control the operation of the system. In addition, to the physical threats to such centers and the communication links that flow in and out of them, one must also be concerned about two other factors: the reliability of the operators within the center, and the possibility that insecure code has been added to one of the programs in a central computer. The threats posed by "insider" threats, as well as the risk of a "Trojan horse" embedded in the software of one or more of the control centers is real, and can only be addressed by careful security measures both, within the commercial firms that develop and supply this software, and careful security screening of the utility and outside service personnel who perform software maintenance within the center. Today security patches are often not always supplied to end users, or users are not applying the patches for fear of impacting system performance. Current practice is to apply the upgrades or patches after SCADA vendors thoroughly test and validate patches, sometimes incurring a delay of several months in patch deployment.

As an example related to numerous major outages, narrowly programmed protection devices have contributed to worsening the severity and impact of the outage—typically performing a simple on/off logic which locally acts as preprogramme while destabilizing a larger regional interconnection. With its millions of relays, controls and other components, the parameter settings and structures of the protection devices and controllers in the electricity infrastructure can be a crucial issue. It is analogous to the poem "For want of a horseshoe nail . . . the kingdom was lost" that is, relying on an "inexpensive 25 cent chip" and narrow control logic to operate and protect a multibillion dollar machine.

As a part of enabling a smart self-healing grid, we have developed fast look-ahead modeling and simulation, precursor detection, adaptive protection, and coordination methods that minimize impact on the whole system performance (load dropped as well as robust rapid restoration). There is a need to coordinate the protection actions of such relays and controllers with each other to achieve overall stability. A single controller or relay cannot do all, and they are often tuned for worst cases, therefore control action may become excessive from a system-wide perspective. On the other hand, they may be tuned for the best case, and then the control action may not be adequate. This calls for coordinating protection and control—neither agent, using its local signal, can by itself stabilize a system; but with coordination, multiple agents, each using its local signal, the overall system can be stabilized.

It is important to note that the key elements and principles of operation for interconnected power systems were established in the 1960s prior to the emergence of extensive computer and communication networks. Computation is now heavily used in all levels of the power network for planning and optimization, fast local control of equipment, and processing of field data. But coordination across the network happens on a slower

time-scale. Some coordination occurs under computer control, but much of it is still based on telephone calls between system operators at the utility control centers, even (or especially!) during emergencies.

Systems should be motivated by living beings' resilience and robustness to operate to some degree after injury, by developing compensatory behaviors and to autonomously recover from unexpected damage through continuous self-modeling, thus providing increased "situational awareness," and ability to be "damage adaptive," to withstand and possibly recover from "injury," attacks, or unexpected damage.

Grid "self-modeling" could survive emergencies and adapt to new conditions quicker than grids that are not "self-conscious." Enabled by distributed sensing and measurement and combined with Fast Modeling and Simulation we have developed and pilot tested data-driven control and operation of regional power grids, analogous to the continuous self-modeling and compensation of damaged fighter planes and intelligent robots in the face of unexpected damage.

From a broader perspective, any critical national infrastructure typically has many layers and decision-making units and is vulnerable to various types of disturbances. Effective, intelligent, distributed control is required that would enable parts of the constituent networks to remain operational and even automatically reconfigure in the event of local failures or threats of failure. In any situation subject to rapid changes, completely centralized control requires multiple, high data rate, two-way communication links, a powerful central computing facility, and an elaborate operations control center. But all of these are liable to disruption at the very time when they are most needed (i.e. when the system is stressed by natural disasters, purposeful attack, or unusually high demand).

When failures occur at various locations in such a network, the whole system breaks into isolated "islands," each of which must then fend for itself. With the intelligence distributed, and the components acting as independent agents, those in each island have the ability to reorganize themselves and make efficient use of whatever local resources remain to them, in ways consonant with the established global goals to minimize adverse impact on the overall network. Local controllers will guide the isolated areas to operate independently while preparing them to rejoin the network, without creating unacceptable local conditions either during or after the transition. A network of local controllers can act as a parallel, distributed computer, communicating via microwaves, optical cables, or the power lines themselves, and intelligently limiting their messages to only that information necessary to achieve global optimization and facilitate recovery after failure.

Over the last 12 years, our efforts in this area have developed, among other things, a new vision for the integrated sensing, communications, protection and control of the power grid. Some of the pertinent issues are why or how to develop protection and control devices for centralized versus decentralized control, and issues involving adaptive operation and robustness to various destabilizers. However, instead of performing *in vivo* societal tests which can be disruptive, we have performed extensive "wind-tunnel" simulation testing (in Silico) of devices and policies in the context of the whole system along with prediction of unintended consequences of designs and policies to provide a greater understanding of how policies, economic designs and technology might fit into the continental grid, as well as guide in their effective deployment and operation.

Advanced technology now under development or under consideration, holds the promise of meeting the electricity needs of a robust digital economy. The architecture for this new technology framework is evolving through early research on concepts and the necessary enabling platforms. This architectural framework envisions an integrated,

self-healing, electronically controlled electricity supply system of extreme resiliency and responsiveness—one that is fully capable of responding in real time to the billions of decisions made by consumers and their increasingly sophisticated agents. The potential exists to create an electricity system that provides the same efficiency, precision, and interconnectivity as the billions of microprocessors that it will power.

## 9 COST AND BENEFIT

Electricity shall prevail at the quality, efficiency and reliability that customers demand and are willing to pay for. On the one hand the question is who provides it; on the other hand it is important to note that achieving the grid performance, security and reliability are a national profitable investment, not a cost burden on the taxpayer. The economic payback is three to seven times and in some cases an order of magnitude greater than the money invested. Further, the payback starts with the completion of each sequence of grid improvement. The issue is not merely who invests money because that is ultimately the public, whether through taxes or kilowatt hour rates. Considering the impact of regulatory agencies, they should be able to induce the electricity producers to plan and fund the process. That may be the most efficient way to get it in operation. The current absence of a coordinated national decision-making is a major obstacle. State's rights and State PUC regulations have removed the individual State's utility motivation for a national plan. Investor utilities face either collaboration on a national level, or a forced nationalization of the industry.

Simply replicating the existing system through expansion or replacement will not only be technically inadequate to meet the changing demands for power, but will produce a significantly higher price tag. Through the transformative technologies outlined here, the nation can put in place a twenty-first century power system capable of eliminating critical vulnerabilities while meeting intensified consumer demands, and in the process, save society considerable expense.

What is at stake is whether our national critical infrastructures and the underpinning interconnected networks will continue to function reliably and securely or not. This program will produce significant advances in the security, robustness, efficiency, and performance of the power grid and its interdependent infrastructures. The tools indicated will provide unprecedented stability, reliability, efficiency, and service quality. A major outage (affecting 7 million or more customers) occurs about once every decade costing over $2 billion—smaller disturbances are commonplace with very high cost to the customers and our society. On a given day, there are 500,000 customers without power for 2 h or more in the United States. The above programs cost about $170–200 million per year for R&D, and up to about $400 million per year over a decade for fielding, testing and integration into the system. Therefore we can save about five to sevenfold in prevention and mitigation of disturbances. Other benefits include the following:

- builds a smart generation and delivery infrastructure, an "electrinet," with in-built security;
- creates opportunities for a risk-managed integration of diverse risk-managed balanced portfolios of generation sources;
- improves security and observability of system operation and control;
- refines definition of system operating limits'

- serves transmission system market demands;
- minimizes transmission costs;
- reduces utage cost;
- improves system simulation models;
- improves management of system reliability and asset integration (from distributed generators and renewables, to central power plants).

As expressed in the July 2001 issue of *Wired* magazine: "The best minds in electricity R&D have a plan: Every node in the power network of the future will be awake, responsive, adaptive, price-smart, eco-sensitive, real-time, flexible, humming—and interconnected with everything else." The technologies included, for example the concept of self-healing electricity infrastructure, methodologies for fast look-ahead simulation and modeling, adaptive intelligent islanding and strategic power infrastructure protection systems, are of special interest for improving grid security from terrorist attack.

## 10 NEXT STEPS

How to control a heterogeneous, widely dispersed, yet globally interconnected system is a serious technological problem in any case. It is even more complex and difficult to control it for optimal efficiency and maximum benefit to the ultimate consumers while still allowing all its business components to compete fairly and freely. A similar need exists for other infrastructures, where future advanced systems are predicated on the near-perfect functioning of today's electricity, communications, transportation, and financial services.

From a national perspective, a key grand challenge before us is how do we redesign, retrofit, and upgrade the nearly 220,000 miles of electromechanically controlled system into a smart self-healing grid that is driven by a well-designed market approach.

Creating a smart grid with self-healing capabilities is no longer a distant dream; we have made considerable progress. But considerable technical challenges as well as several economic and policy issues remain to be addressed.

Funding and sustaining innovations, such as the self-healing grid, remain a challenge as utilities must meet many competing demands on precious resources while trying to be responsive to their stakeholders, who tend to limit R&D investments to immediate applications and short-term ROI. In addition, utilities have little incentive to invest in the longer term. For regulated investor–owned utilities there is added pressure caused by Wall Street to increase dividends.

Several reports and studies have estimated that for existing technologies to evolve and for the innovative technologies to be realized, a sustained annual research and development investment of $10 billion is required. However, the current level of R&D funding in the electric industry is at an all-time low. The investment rates for the electricity sector are the lowest rates of any major industrial sector with the exception of the pulp and paper industry. The electricity sector invests at most, only a few tenths of a percent of sales in research. This is in contrast to fields such as electronics and pharmaceuticals in which R&D investment rates have been running between 8 and 12% of net sales; all of these industry sectors fundamentally depend on reliable electricity.

A balanced, cost-effective approach to investments and use of technology can make a sizable difference in mitigating the risk. Electricity shall prevail at the quality, efficiency,

and reliability that customers demand and are willing to pay for. On the one hand, the question is, "Who provides it?" on the other hand, it is important to note that achieving the grid performance, security, and reliability are a profitable national investment, not a cost burden on the taxpayer. The economic payback is three to seven times greater than the money invested. Further, the payback starts with the completion of each sequence of grid improvement. The issue is not merely who invests money, because that is ultimately the public, but whether it is invested through taxes or kWh rates. Considering the impact of regulatory agencies, they should be capable of inducing the electricity producers to plan and fund the process; this may be the most efficient way to get it in operation. The current absence of a coordinated national decision-making body is a major obstacle. State's rights and State PUC regulators have removed the individual State's utility motivation for a national plan. Investor utilities face either collaboration on a national level or a forced nationalization of the industry.

## ACKNOWLEDGMENTS

I developed most of the context and many of findings presented here while I was at the EPRI in Palo Alto (during 1998–2003), and for the Galvin Electricity Initiative (during 2005–2006). I gratefully acknowledge the feedback from Mr John Voeller (the editor of this series) and Dr James Peerenboom. The support and feedback from numerous colleagues at EPRI, universities, industry, national laboratories, and government agencies with funding from EPRI, NSF, and the ORNL is gratefully acknowledged.

## REFERENCES

1. Amin, S. M. (2003). North America's electricity infrastructure: are we ready for more perfect storms? *IEEE Secur. Priv. Mag.* **1**(5), 19–25.

## FURTHER READING

Amin, S. M. (2008). For the good of the grid: toward increased efficiencies and integration of renewable resources for future electric power networks. *IEEE Power Energy Mag.* **6**(6), 48–59.

Amin, S. M., and Stringer, J. (2008). The electric power grid: today and tomorrow. *MRS Bull.* **33**(4), 399–407.

Amin, S. M., and Schewe, P. F. (2007). *Preventing Blackouts*. Scientific American, pp. 60–67.

Schewe, P. F. (2007). *The Grid: A Journey Through the Heart of our Electrified World*. Joseph Henry Press.

Amin, S. M. (2005). Scanning the technology: energy infrastructure defense systems. *Spec. Issue Proc. IEEE* **93**(5), 857–871.

Amin, S. M., and Gellings, C. (2006). The North American power delivery system: balancing market restructuring and environmental economics with infrastructure security. *Energy* **31**(6–7), 967–999.

Amin, S. M., Carlson, L. W., and Gellings, C. (2006). *Galvin Electricity Initiative: Technology Scanning, Mapping and Foresight*. Galvin Electricity Project, Inc., EPRI, Palo Alto, CA, Chicago, IL, p. 70.

Amin, S. M., and Wollenberg, B. F. (2005). Toward a smart grid: power delivery for the 21st century. *IEEE Power Energy Mag.* **3**(5), 34–41.

Amin, S. M. (2005). Energy infrastructure defense systems. *Proc. IEEE* **93** (5).

Amin, S. M. (2005). Powering the 21st century: we can—and must—modernize the grid. *IEEE Power Energy Mag.*, 93–96.

Amin, S. M. (2004). Electricity. In *Digital Infrastructures: Enabling Civil and Environmental Systems through Information Technology*, R. Zimmerman, and T. Horan, Eds. pp. 116–140, Chapter 7.

EPRI. (2003). *Complex Interactive Networks/Systems Initiative: Final Summary Report—Overview and Summary Final Report for Joint EPRI and US DoD University Research Initiative*. EPRI, Palo Alto, CA, p. 155.

Amin, S. M. (2001). Special issues of IEEE control systems magazine on control of complex networks. **21** (6), (2002). 22(1).

Amin, S. M. (2001). Toward self-healing energy infrastructure systems. cover feature in the *IEEE Comput. Appl. Power* **14**(1), 20–28.

Amin, S. M. (2000). Toward self-healing infrastructure systems. cover feature in the *IEEE Comput. Mag.* **33**(8), 44–53.

Amin, S. M. (2000). National infrastructures as complex interactive networks. In *Automation, Control, and Complexity: An Integrated Approach*, T. Samad, and J. Weyrauch, Eds. John Wiley and Sons, New York, pp. 263–286, chapter 14.

# NANO-ENABLED POWER SOURCES

ENOCH WANG

*Intelligence Community, Washington, D.C.*

DANIEL H. DOUGHTY

*SION Power Corp, Tucson, Arizona*

## 1 SCIENTIFIC OVERVIEW

As with portable consumer electronics, there is an insatiable demand for more power in most military applications. The exponential growth in integrated circuit performance over the past 30 years, as predicted by the Moore's law, accelerated the demand for power in many consumer electronics and military devices. Unfortunately, the pace of development of electrochemical cells or other power sources cannot keep up with the exponential growth of the integrated circuit and has become a limiting technology for electronic microdevices such as miniaturized communication devices (Fig. 1). Although the number

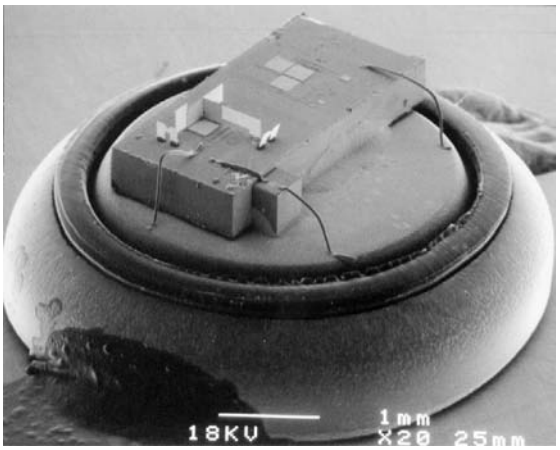



**FIGURE 1** Photograph of a sensor "mote" (only 2 mm × 4 mm) containing a sensor, microprocessor, and communications electronics mounted on top of a much larger coin cell (from www-bsac.eecs.berkeley.edu). The operation of this device is limited by the lifetime of the battery.

of transistors per integrated circuit has been doubled every couple of years since 1970, the performance gain per year for commercial cells is usually a small percentage, depending on the cell chemistry. Battery technology performance has increased about 2% per year. The newer lithium-ion (Li-ion) rechargeable chemistry performance gain in terms of capacity has been about 12% per year since the introduction in 1991, but still has not kept pace with demand. Thus, the accelerating growth in the digital devices has often been limited by the incremental improvement in battery performance.

Nanotechnology offers an opportunity for improvement in power and energy density of power sources [1]. Generally speaking, nanotechnology can be classified either as nanoscale fabrication technology of devices or the revolutionary enhancement of performance by using nanoscale materials. Nanomaterials are usually defined dimensionally, with features such as particle dimension or porosity in the range of 1–100 nm. Fabrication technology for nanodevices is based on the so-called "bottom-up" approach whereby complex structures are self-assembled from the atomic or molecular level, as is found in all biological systems. Progress in this area has been slow due to inadequate control at the atomic level with currently available equipment. On the other hand, much progress has been made in developing nanomaterials as evidenced by commercially available carbon nanotubes from many sources (recent search found >25 websites that claim to be "dedicated to nanotubes"). Nanomaterials hold the potential to be an enabling technology for energy storage and conversion devices by increasing energy storage capacity, discharge rate capability, or stability over the lifetime of the device. Thus, the focus of this article is to review nano-enabled power sources based on judicious implementation of nanostructured materials.

### 1.1 High Power Cells

Increasing power and rate capability of batteries are the important applications of nanoscale materials. By reducing the particle size of the active materials from submicron to nanoscale, one should be able to increase diffusion rates in these solids by two orders of magnitude and improve the power capability. Typical battery active materials

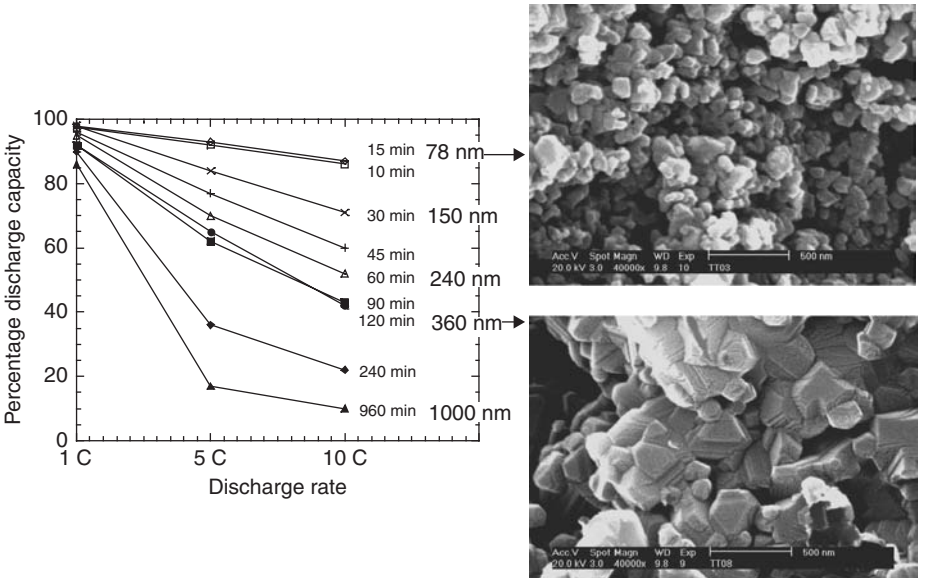



**FIGURE 2** Nano- versus macro-$Li_4Ti_5O_{12}$ capacity utilization under high discharge rates [2].

are on the order of 10 $\mu$m (10,000 nm). Because of the diffusion distance required, full charge and discharge usually require a period of 30 min to 1 h to diffuse through 10,000 nm. According to the diffusion equation, the diffusion time, $t$, is proportional to $r^2/D$, where $r$ is the diffusion length and $D$ is the diffusion coefficient. It is difficult to decrease drastically the intrinsic diffusion coefficient, but one can shorten the diffusion length by 2–3 orders of magnitude through the use of nanomaterials, and achieve minutes or subminutes charge or discharge rates. One such example is the nano-lithium titanate (nano-$Li_4Ti_5O_{12}$) of approximately 30 nm. Nano-$Li_4Ti_5O_{12}$ was demonstrated to have greater than 80% utilization at 10 C (6 min) continuous discharge rate while 1 $\mu$m macro-$Li_4Ti_5O_{12}$ had only about 10% utilization at the same discharge rate [2] (Fig. 2). As anode, nano-$Li_4Ti_5O_{12}$ enabled fast charge Li-ion cells was demonstrated in Toshiba's 1-min charge Li-ion cells [3].

Another example of a nano-enabling material is the olivine lithium iron phosphate, $LiFePO_4$. The low electronic conductivity of $LiFePO_4$ results in very poor rate performance. However, when $LiFePO_4$ is reduced to the nanodomain and coated with nanocarbon particles, the conductivity and power density were improved up to seven and one orders of magnitude, respectively [4]. High power Li-ion cells based on modified nano-$LiFePO_4$ are being commercialized by A123Systems. These cells were claimed to be capable of delivering about one order of magnitude more power (>3000 W/kg) than conventional Li-ion cells [5], similar to that of a supercapacitor but with the energy density of that of a rechargeable battery, albeit lower energy density than conventional Li-ion cells.

Similarly, by reducing the particle size to nanoscale, one can also enhance the high power performance of electrochemical capacitors. In an electrochemical capacitor, charge is stored on the surface of a porous, high-surface-area electrode, and not in the bulk of the material. Very high surface area leads to high power delivery, and capacitances of

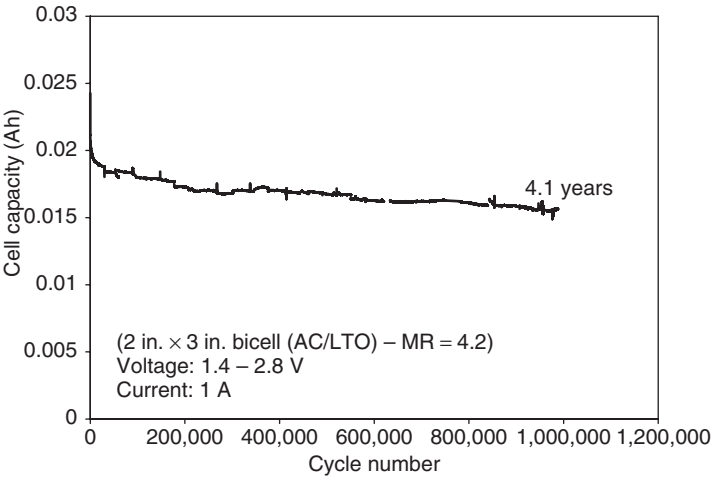



**FIGURE 3** Cycle life of nano-$Li_4Ti_5O_{12}$ versus carbon asymmetric electrochemical capacitor [courtesy of Prof. Amatucci of Rutgers University].

~100 F/g have been measured with carbon foams. Because there is no movement of mass within the electrode material and therefore no change in volume in the anode or cathode during charge and discharge, the cycle life of these systems is essentially infinite with a very poor specific energy, typically less than 1 Wh/kg. However, using asymmetric hybrid configuration, containing one battery electrode and one electrochemical double-layer capacitor electrode, Amatucci et al. have demonstrated energy density greater than 20 Wh/kg at a power density of 3000 W/kg [6]. The asymmetric capacitor was enabled by the nano-$Li_4Ti_5O_{12}$, which not only enabled high power but also high cycle life. Cycle life greater than 1 million cycle was demonstrated using the nano-$Li_4Ti_5O_{12}$ (Fig. 3), which has unique zero volume change during cycling. Thus, the asymmetric capacitors serve to bridge the performance gap between batteries (high energy but low power) and capacitor (high power but low energy).

Nanotech-enabled optimization should also lead to new high power-density electrochemical capacitors as a consequence of the recent determination of the true nature of pseudocapacitance in hydrous ruthenium oxide (designated as $RuO_2 \cdot xH_2O$). For $x=0.5$, 720 F/g can be stored in hydrous ruthenium oxide [7], 5-10 times greater than that stored at high-surface-area carbon supercapacitors. This form of the material appears amorphous to X rays, but upon medium-range structural analysis was shown to form a nanocomposite of metallic, anhydrous rutile-like $RuO_2$ nanocrystallites whose surfaces contain of proton-conductive structural water associated with Ru–O [8]. The competing percolation networks of electronic and protonic conduction pathways provide the optimized multifunctionality of hydrous ruthenium oxide for energy storage. This new structural understanding on the nanoscale can also serve as a new archetype for the design of charge-storage materials.

## 1.2 High Capacity Cells

Nanomaterials open new options in preparing high capacity electrode materials. Today's high energy batteries rely almost exclusively on lithium or lithiated compounds since

lithium is the lightest metal in the periodic table, has a high oxidation potential, large electrochemical equivalence, and good conductance. The energy density of lithium cells, and especially the state of the art (SOA) of Li-ion cells is limited by the energy density of the positive materials. The current SOA positive materials utilized intercalation reactions, which are limited to the amount of lithium transferred, thereby limiting electron transfer to typically less than 1e− per compound such as $LiMeO_2$, where Me is a transition metal.

$$1e^- + 1Li^+ + Me^{4+}O_2 \leftrightarrow LiMe^{3+}O_2$$

An alternative to the intercalation mechanism is to utilize the concept of reversible conversion compounds where multiple electrons can be transferred to the active electrode material to reduce it fully to the metal state and later reoxidize it back to the original compound.

$$3e^- + 3Li^+ + Me^{3+}X_3 \leftrightarrow 3LiF + Me^o$$

In theory, these reactions can lead to a specific energy greater than 1500 Wh/kg, or in a practical cell about 3*x* that of the SOA Li-ion cells based on $LiCoO_2$ positive electrode. Such reactions have been shown to exist for dichalcogenides and nitrides in the reaction range of 0.5–1.5 V [9]. To increase the potential of such reactions by at least 1 V, highly ionic halides are preferred over oxides, which are used in almost all lithium cells. Of the halides, the metal fluorides are most attractive due to their light weight and low solubility in nonaqueous electrolyte solvents relative to the heavier halides such as Cl and Br.

The theoretical attractiveness of metal fluorides as electrodes for primary cells has been known for over four decades. However, metal fluoride electrodes have not often been realized in part due to the fact that metal fluorides are very high bandgap materials resulting in electronic insulator characteristics. Amatucci et al. at Rutgers ESRG have demonstrated the enablement of a variety of high bandgap, insulating metal fluorides as reversible conversion electrodes through the use of nanocomposite technology [10]. By fabricating the desired metal fluoride materials as 20 nm crystallites in a small amount of conducting matrix, the electrochemical activity of these materials has been enabled. The reduction to nanocrystallite size (reducing electron path length by three orders of magnitude) has a threefold effect: developing a large volume of interface that is defect rich, creating surface states that assist both electron and ion diffusion, and enabling a larger portion of the material to be activated via electron tunneling reactions. A number of systems have been enabled, exhibiting near theoretical conversion voltages (2–3.2 V) and specific capacities from 400 to 700 mAh/g. Systems including fluorides and in some cases oxyfluorides of Fe, Ni, Co, Cr, Bi, and Cu have been enabled. Of these, $CuF_2$ has been identified as promising electrode material for primary cells, and $FeF_3$ and $BiF_3$ as promising electrode materials for rechargeable cells (Fig. 4) [11].

Nanotechnology also plays a key role in improving the effectiveness of the negative materials used in lithium cells. Firstly, in addition to aforementioned enhanced power performance, smaller particle sizes mean less internal stress on the electrodes during intercalation/deintercalation (the binder is more compressible and can more effectively tolerate the volume change), which could lead to increased cycle life. Secondly, smoother electrodes may also allow one to use thinner separators and/or electrolyte—again improving battery performance. Finally, one can replace carbon with a material that reversibly binds more than a single lithium atom per six host atoms (for example, Sn or Si). Nanosize composite anodes (e.g. carbon/silicon) offer the potential to take advantage of much

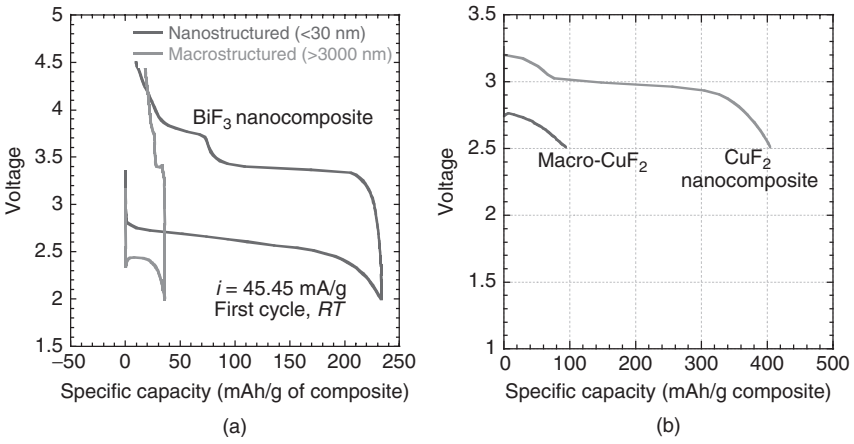



**FIGURE 4** Theoretical capacity utilization enabled in (a) nano-$BiF_3$ and (b) nano-$CuF_2$.

higher capacity anode materials (e.g. $Li_4.Si$ has 10 times the capacity of $LiC_6$) and the smaller particle size can accommodate stresses that would fracture larger particles. This gives both higher capacity and reasonable stability on cycling [12]. The 40 wt% Si composite, which was the most silicon-rich composite that was tested, had a maximum reversible capacity of 1345 mAh/g and it still delivered 745 mAh/g, more than twice the capacity of $LiC_6$ in the 20th cycle.

SONY announced "Nexelion" cell in 2005 with carbon/Sn alloy anode [13], which increased the capacity per volume by 30%. In February 2007, Panasonic announced a further 40% increase in capacity by using alloy anode [14] and, although we do not know the composition, nanomaterials are suspected because they can accommodate the strain produced by the >300% volumetric expansion that accompanies conversion to Li alloy (e.g. conversion of Si to the lithiated compounds $Li_{22}Si_5$ has a 325% expansion). These advances in materials enable the production of high energy cells and batteries—Panasonic claims to have reached 740 Wh/l at the cell level.

## 2 GLOBAL EFFORT ON NANO-ENABLED POWER SOURCE TECHNOLOGIES

Ongoing research programs in the government (e.g. National Nanotechnology Initiative) and commercial sector are likely to benefit energy conversion technology. Fuel cells are of worldwide commercial interest, and DARPA has existing programs in thermoelectric materials development. The Department of Homeland Security should analyze and exploit these developments if nanotech-related breakthroughs appear that are relevant to their special needs.

Outside the United States, the most publicized R&D effort on nanotechnologies for power sources is the European consortium, Alistore [15]. Launched in 2004, the main objective of Alistore is to develop high power and high energy lithium cells based on nanomaterials. The consortium consisted of 16 European university research groups and University of Picardie at Amiens, France, was the program administrator. Other European companies are also very active in developing nanomaterials for fuel cells

and energy harvesting technologies such as photovoltaic cells and thermoelectric energy harvester.

Government-sponsored nanotechnology efforts for power sources are not as well publicized among the Asian countries. However, there is already a strong effort by Japanese companies to commercialize nanomaterials such as carbon nanotubes for energy-related applications [16]. On the basis of the open literatures, we anticipated that other Asian countries such as Japan, China, and South Korea will become major players in nano-enabling materials for power sources within the next few years. NEDO in Japan has committed 2B ¥ for developing carbon nanotubes for high performance capacitors.

## 3 CRITICAL NEEDS ANALYSIS

Improved energy storage technology will benefit homeland security by providing increased performance across a wide range of portable electronic, including sensors, transmitters, and communication devices. Nanotechnology has strong potential to enable the development of batteries, capacitors, and hybrid systems with enhanced power and/or energy performance, which will enable the fabrication of micropower sources. In addition to the high power and high energy cells that were discussed above, technical areas that could be impacted by improvements in nanomaterials are other types of battery materials (e.g. electrolytes and separators) and fuel cells. The advent of micromachining and now nanomachining technology, combined with new and improved materials, provides opportunities for improving the performance of energy harvesting schemes.

### 3.1 3D Battery Architecture and Novel Fabrication Methods

Micropower sources capable of providing reliable rechargeable power under extreme conditions are critical to the development of security applications such as small autonomous distributed sensors. However, as Figure 5 illustrates, the energy density of the batteries decreases almost linearly as the size of the batteries decreases due to decreasing packaging efficiency. In addition, as batteries are reduced to the microscale,

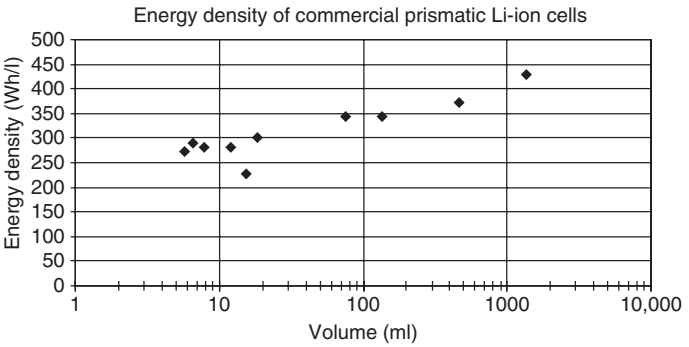



**FIGURE 5** Energy density decreases with cell size in commercial prismatic Li-ion cells. ((Table 35.13) D. Linden, and T. B. Reddy, Eds. *Energy Density Calculated Based on Data in Handbook of Batteries*, 3rd ed., McGraw Hill, New York, p. 35.36.)

it becomes impractical (and almost impossible) to assemble cell stacks via the conventional layer-by-layer stacking approach. Extreme alignment precision is required in order to avoid any shorting between the microelectrodes. This necessitates the use of microelectronic fabrication techniques such as vacuum deposition. To date, the most mature microbattery is based on the all solid-state thin-film technology, first developed by Bates et al. [17]. The active components are typically less than 20 $\mu$m thin and the solid-state lithium phosphorus oxynitride (LiPON) separator is only a few micrometers thick in order to compensate for the low conductivity of the LiPON electrolyte. However, because of poor packaging, most of the cells exhibit poor energy density (Wh/l). The core concept behind the 3D battery is to develop novel nanoarchitecture by more efficient use of available space in the $z$ direction, resulting in interpenetrating electrodes. The concepts, shown schematically in Figure 6, are the topics of current research. Scaling of these architectures to realistic battery sizes is not yet proven. 3D architectures are clearly optimal when one is constrained in volume (e.g. for thin-film cells or smart motes). Fabrication strategies play a key role here; novel techniques such as the use of Langmuir–Blodgett thin films, layer-by-layer self-assembly, template synthesis, and semiconductor processing (e.g. lithography and etching to define microstructures followed by and deposition to add materials) are not yet available or are prohibitively expensive. It is important to note that the periodic arrangements of 3D configured anodes and cathodes lead to nonuniform current distributions [18], while interpenetrating, conformal, aperiodic arrangements do not.

Finally, Belcher et al. in MIT [20] reported virus assembled electrochemically active cobalt oxide for use in lithium batteries. However, the complex command and control needed for viruses to self-assemble themselves to form the positive and negative electrodes remain to be demonstrated, in order to achieve the ultimate goal of virus self-assembled microbattery.

### 3.2 Membranes, Separators, and Electrolytes

Self-assembly of nanostructures may produce advanced functional materials for this application as well. Shape control can allow synthesis of tubular structures with enhanced ionic conductivity. Surfactant templating methods [21] have produced interesting materials for battery electrolytes and the same technology could be used for fuel cell electrolytes. This approach could also be applied to membranes in metal/air batteries (sometimes termed *semi-fuel cells*) to allow selective transport of oxygen while rejecting carbon dioxide and water. Additionally, commercialization of high energy rechargeable systems (e.g. Li/sulfur and Li/air) would be enabled by stabilizing the lithium interface, which results in cycle life and safety improvements.

Although nanotechnology may not play a role in the chemistry of liquid electrolytes, it can be potentially exploited to improve separator performance. For example, new separator materials designed with large numbers of nanoscale pores may allow for thinner materials with enhanced ionic conductivity. Opportunities also include tailoring the separator nanostructure using organic/inorganic composite electrolytes to improve both physical stability (i.e. prevent physical contact of the electrodes) and conductivity [22]. Self-assembly processes may also be effective in depositing extremely thin separator layers on anode and cathode surfaces. If both the pore size/shape and the pore chemistry could be controlled effectively, one can envision ions rapidly moving through empty channels, thereby forming a “liquid-like” separator without any liquid.

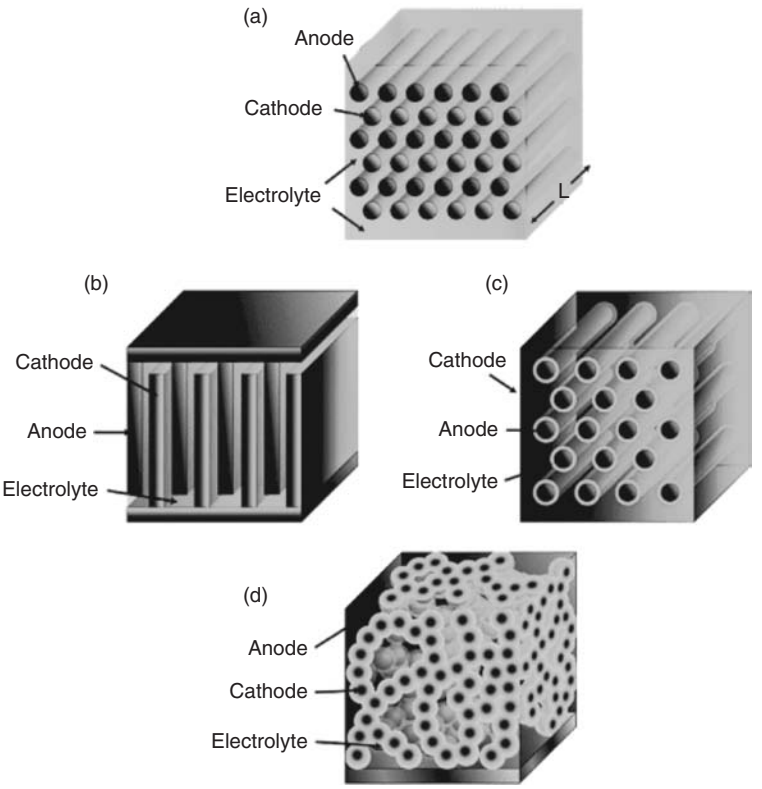



**FIGURE 6** Schematic representation of 3D architectures including (a) an array of interdigitated cylindrical cathodes and anodes; (b) an interdigitated plate array of cathodes and anodes; (c) a rod array of cylindrical anodes (cathodes) with a thin layer of ion conducting electrolyte with the remaining free volume filled with cathode (anode) material; (d) a sponge architecture in which the solid network of the "sponge" serves as both the cathode and the current collector, it is coated with a thin electrolyte and the remaining free volume is filled with an interpenetrating, continuous anode. [See Figure 2 in Reference 19, page 4466].

The ionic conductivity of solid-state electrolytes is generally far less than that of liquid electrolytes due to limited ion mobility and the hopping of charge from one unit cell to the next. However, by making the electrolyte layers extremely thin and stable, effective (albeit low power density) batteries can be made; for example, LiPON functions as a micrometer-scale electrolyte in rechargeable thin-film lithium batteries [23]. Optimization of the nanostructure of these materials may lead to increased conductivity (grain boundary/defect diffusion) and thinner layers without shorting (again leading to enhanced conductivity), and thus to improved power capability.

### 3.3 Electrodes and Electrocatalysts for Fuel Cells

These components are critical to the function of a fuel cell since they catalyze the electrochemical reduction of oxygen at the cathode and the oxidation of fuel at the anode. Breakthroughs in electrocatalysts might revolutionize fuel cells by giving them fuel flexibility and increasing power output, as well as by increasing their tolerance to

chemical species that tend to poison them (e.g. carbon monoxide or sulfur-containing moieties).

New synthetic methodologies might allow for the control of fuel cell electrode microstructures. Nanostructured catalysts may enhance reaction kinetics by dramatically increasing electrode surface area and restricting reactions to confined regions of the active surface. In one study, high catalytic activity resulted from high active surface area of the catalysts supported within an ultraporous electrode nanoarchitecture [24]. High-surface-area materials are extremely reactive, which often causes problems during synthesis (e.g. nanophase metals are often capped with organic ligands after synthesis to prevent sintering reactions). The goal is to maintain the high surface area of nanostructured catalysts, while avoiding agglomeration, sintering, or restructuring during use. Self-assembly on the nanoscale using shape control of catalytic materials (e.g. bimetallic catalysts) might also be important [25].

### 3.4 Thermoelectric Devices

Temperature differences can be used to generate power. The power density scales with temperature difference. A 5 $^{\circ}$C temperature difference can generate 40-80 $\mu$W/cm$^2$ with existing thermoelectric technology. This temperature difference can be generated from man-made sources (parasitic devices placed on warm surfaces such as automobile engines, pipelines, and heaters), environmental gradients (in the soil, water, or at their interface), and within animals (one company has announced one such device for human implantation) [26].

While static conversion of heat into electricity has been an area of research for many decades, the promise of producing tailored nanostructures has prompted renewed interest in several energy conversion schemes. Nanotechnology offers the potential for improved efficiencies, since shrinking the characteristic dimensions of a device to nanometer length scales influences electron and phonon behavior. The efficiency of thermoelectric devices can also be characterized by the figure of merit, $ZT$, where $Z$ is the power factor and $T$ is the absolute temperature. A limitation of thermoelectrics designed around standard bulk materials is that most metallic conductors (high $\sigma$ materials) have low Seebeck coefficients (a few microvolt per kelvin, whereas $\geq$100 $\mu$V/K would be more desirable), while the electron and phonon contributions to thermal conductivity make it difficult to achieve both high $\sigma$ and low $\kappa$ in the same material. As a result, the $ZT$ remained at 1 or less for the last 40 years. Recently, researchers from Research Triangle Institute were able to increase the $ZT$ to about 2.4 in p-type thin-film superlattices of $Bi_2Te_3/Sb_2Te_3$ [27]. The nanostructured superlattice layers vary from 1 to 5 nm. The thermal conductivity and the electrical resistivity are reduced due to blocked phonon transmission and enhanced carrier mobility, respectively, in the nanothick superlattice layer.

Quantum confinement of electronic charge carriers within regions of reduced dimensionality has the potential to increase the power factor [28]. Increased phonon scattering that occurs when interfaces are separated by distances compared to phonon wavelengths can reduce the lattice thermal conductivity [27]. These approaches require tailored nanometer-scale materials synthesis techniques, as the critical dimension for confinement is $\sim$10 nm. One can reduce dimensionality in one dimension (confinement in a plane) to three dimensions (confinement in a "quantum dot"). Improved materials synthesis and characterization techniques on the nanoscale, as well as advances in the theory and characterization of nanodimensional solids, are required.

### 3.5 Photovoltaics

The energy conversion efficiency of photovoltaics (including thermophotovoltaic or TPV devices) may also be increased by effects associated with reduced dimensionalities on the nanometer scale. Photonic lattices have sharp absorption and emission peaks at their photonic band edges. By tuning the emission peak of a photonic crystal (emitter) to the bandgap energy of a photodiode (energy conversion device), one could increase the overall conversion efficiency of TPVs [29]. The conversion efficiency might also be increased by evanescent coupling of an infrared emitter to a photodiode in very close (subwavelength) proximity [30]. Another approach to improve the photovoltaic (PV) efficiency is by increasing the intrinsic quantum efficiency of the PV material via the use of quantum dots. The exact mechanism for the quantum dot enhancement is still not well understood, though it is speculated to be related to enhanced electron–hole interaction due to quantum confinement. In conventional PV material such as Si, one electron–hole pair (or exciton) is generated per photon. The feasibility of generating multiple excitons per photon was demonstrated in various quantum dots materials such as PbSe quantum dots, leading to multiple increase in quantum efficiency [31]. However, it remains a challenge to design high efficiency PV devices based on the quantum dots, and PV device efficiency enhancement over 100% has yet to be demonstrated. Nanoscale optimization of the interfaces between disparate materials in organic light-emitting diodes (OLEDs), organic solar cells, and thin-film solar cells represents another opportunity. Nanosize oxide particles (e.g. $TiO_2$ or ZnO) with organic sensitizers bound to the surface are proposed as a new class of solar cells, and controlled interfaces are the key to improving the efficiency of these devices [32]. Modeling advancements are required to direct the materials synthesis and processing efforts.

## 4 RESEARCH DIRECTIONS

Nanotechnology enables the rational design of power source devices and structures with optimized storage, conductivity, density, and optical and electronic properties. The potential for tailoring of chemical composition and morphology at the nanometer scale will provide the opportunity for unprecedented control of materials properties. The following are specific areas that need to be investigated:

1. Nanomaterial synthesis and characterization.
   - Performance optimization is a balancing act between electron/ion/mass transport and electrode kinetics, but independent control of transport multifunction is difficult to do with bulk materials. In batteries, disorder improves mass transport of insertion ions, but sufficient order (even on the nanoscale) must be retained to move electrons. As the particle size is reduced, the relative fraction of atoms at the surface significantly increases, to the point that three-dimensional particles begin to exhibit the characteristics of two-dimensional objects.
   - By creating 2D structures with specific surface chemistry and morphology, one can control the interface between materials or phases, so as to elicit the desired behavior. Nanomaterials plus interface chemical approach have enabled the rapid implementation of the insulating $LiFePO_4$ phase in practical Li-ion cells and allowed us to foresee the use of Si as an alternative to the nanostructured

Sn-graphite-based negative electrode. There exists also the possibility to tailor the optical and electronic characteristics of a material, which strongly influence energy conversion processes, allowing us to envision the production of improved catalysts and electrolytes for fuel cells, as well as improved thermoelectrics and photovoltaics.

2. Nanoarchitectures to develop novel energy conversion and storage devices.
   - Nanotechnology will enable realization of devices with increased energy or power. For example, by maximizing the interfacial area between the anode and cathode while minimizing their separation, one can increase the power density of a cell dramatically. Improvements in energy density are attained by processing very thin electrolytes and better packing of materials. Such multifunctional concepts have the potential to further decrease the size and weight of a system for a given mission.
   - Nanomachining technology, combined with new and improved materials, opens up opportunities both for improving the performance of energy harvesting schemes and for realizing highly miniaturized versions of systems that are familiar at a larger scale.

Creation of exciting new materials and architectures for batteries, electrochemical capacitors, fuel cells as well as other energy conversion devices holds the potential to meet the intense need for increased energy and power for electronic devices of interest to homeland security community.

## REFERENCES

1. National Academy of Science. *Nanotechnology for the Intelligence Community*, National Research Council of the National Academies, National Academy Press, Washington, DC, May 2005.
2. Plitz, I., Dupasquier, A., Badway, F., Gural, J., Pereira, N., Gmitter, A., and Amatucci, G. G. (2006). The design of alternative nonaqueous high power chemistries. *Appl. Phys.* **A82**, 615–626. DOI: 10.1007/s00339-005-3420-0.
3. http://www.technewsworld.com/story/hardware/41889.html [March 30, 2005].
4. Herle, P. S., Ellis, B., Coombs, N., and Nazar, L. F. (2004). Nano-network electronic conduction in iron and nickel olivine phosphates. *Nat. Mater.* **3**, 147–152.
5. http://www.a123systems.com/newsite/index.php#/products/cells26650/, 2008.
6. Amatucci, G. G., Badway, F., Du Pasquier, A., and Zheng, T. (2001). An asymmetric hybrid nonaqueous energy storage cell. *J. Electrochem. Soc.* **148**, A930–A939.
7. Zheng, J. P., Cygan, P. J., and Jow, T. R. (1995). Hydrous ruthenium oxide as an electrode material for electrochemical capacitors. *J. Electrochem. Soc.* **142**, 2699–2703.
8. Dmowski, W., Egami, T., Swider-Lyons, K. E., Love, C. T., and Rolison, D. R. (2002). Local atomic structure and conduction mechanism of nanocrystalline hydrous $RuO_2$ from X-ray scattering. *J. Phys. Chem. B* **106**, 12677–12683.
9. Winter, M., and Besenhard, J. O. (1999). Rationalization of the low-potential reactivity of 3d-metal-based inorganic compounds toward Li. *Electrochim. Acta* **45**, 31. See also Poizot, P., Laruelle, S., Grugeon, S. Dupont, L., and Tarascon, J.-M. (2000). Nano-sized transition-metal oxides as negative-electrode materials for lithium-ion batteries. *Nature* **407**, 496–499.

10. Amatucci, G. G., and Pereira, N. (2007). Fluoride based electrode materials for advanced energy storage devices. *J. Fluor. Chem.* **128**(4), 243–262. DOI:10.1016/j.jfluchem.2006.11.016.
11. (a) Badway, F., Mansour, A., Plitz, I., Pereira, N., Weinstein, L., Yourey, W., and Amatucci, G. G. (2006). Enabling aspects of metal halide nanocomposites for reversible energy storage. *J. Electrochem. Soc.* **153**, A799; (b) Bervas, M., Yakshinskiy, B. Klein, L. C., and Amatucci, G. G. (2006). Soft-chemistry synthesis and characterization of bismuth oxyfluorides and ammonium bismuth fluorides. *J. Am. Ceram. Soc.* **89**, 645–651.
12. Roberts, G. A., Gross, K. J., Ingersoll, D., Spangler, S. W., and Wang, J. C. (2003). *Silicon/Carbon Composite Negative Electrode Materials*, Sandia National Laboratories SAND Report for Unlimited Release, SAND2002-8627. See also Kevin Bullis, Technology Review Published Online, (25 October 2006) http://www.technologyreview.com/Energy/17653/page2/.
13. http://www.sony.net/SonyInfo/News/Press/200502/05-006E/index.html, 2008.
14. http://www.dailytech.com/Article.aspx?newsid=6094, 2008.
15. http://www.u-picardie.fr/alistore/new_page_2.htm, 2008.
16. http://www.smalltimes.com/Articles/Article_Display.cfm?ARTICLE_ID=267721&p=109, 2008.
17. Bates, J. B., Dudney, N. J., Gruzalski, G. R., and Luck, C. F. (1994). Thin film battery and method for making same. US Patent 5338625.
18. Hart, R. W., White, H. S., Dunn, B., and Rolison, D. R. (2003). 3-D microbatteries. *Electrochem. Commun.* **5**, 120–123.
19. Long, J. W., Dunn, B., Rolison, D. R., and White, H. S. (2004). Three-dimensional battery architectures. *Chem. Rev.* **104**, 4463–4492. DOI 10.1021/cr020740l.
20. Nam, K., Kim, D.-W., Yoo, P. J., Chiang, C.-Y., Meethong, N., Hammond, P. T., Chiang, Y.-M., and Belcher, A. (2006). Sciencexpress/ www.sciencexpress.org/06 April.
21. Kim, H. J., Lee, H. C., Rhee, C. H., Chung, S. H., Lee, K. H., and Lee, H. C. (2003). Alumina nanotubes containing Li of high ion mobility. *J. Am. Chem. Soc.* **125**, 13354–13355.
22. Bronstein, L. M., Joo, C., Karlinsey, R., Ryder, A., and Zwanziger, J. W. (2001). Solid hybrid polymer electrolyte networks: nano-structurable materials for lithium batteries. *Chem. Mater.* **13**, 3678.
23. (a) Bates, J. B., Dudney, N. J., Gruzalski, G. R., Zuhr, R. A., Choudhury, A., Luck, C. F., and Robertson, J. D. (1992). Effects of deposition condition on the ionic conductivity and structure of amorphous lithium. *Solid State Ionics* **647**, 53–56.; (b) Bates, J. B., Dudney N. J., Neudecker, B., Ueda, A., and Evans C. D. (1997). Thin-film lithium and lithium-ion batteries. *J. Electrochem. Soc.* **144**, 524.
24. Anderson, M. L., Stroud, R. M., and Rolison, D. R. (2002). Enhancing the activity of fuel-cell reactions by designing three–dimensional nanostructured architectures: catalyst-modified carbon-silica composite aerogels. *Nano Lett.* **2**, 235–240; correction: *Nano Lett*. 2003, 3, 1321.
25. Approaches to Combat Terrorism (ACT) (2003). *Opportunities for Basic Research, Joint Workshop by The Directorate of the Mathematical and Physical Sciences, NSF and the Intelligence Community*, National Science Foundation, http://www.mitre.org/public/act/10_22_final.pdf).
26. http://adsx.com/prodservpart/thermolife.html, 2008.
27. Venkatasubramanian, R., Silvola, E., Colpitts, T., and O'Quinn, B. (2001). Thin-film thermoelectric devices with high room-temperature figures of merit. *Nature* **413**, 597–602. DOI: 10.1038/35098012.
28. (a) Hicks, L. S. and Dresselhaus, M. S. (1993). Effect of quantum-well structures on the thermoelectric figure of merit. *Phys. Rev. B* **47**, 12727–12731. **DOI:** 10.1103/PhysRevB.47.12727;

(b) Majumdar, A. (2004). Thermoelectricity in semiconductor nanostructures. *Science* **303**, 777–7778.

29. Fleming, J. G., Lin, S. Y., El-Kady, I., Biswas, R., and Ho, K. M. (2002). All-metallic three-dimensional photonic crystals with a large infrared bandgap. *Nature* **417**, 52–55.
30. DiMatteo, R. S., Greiff, P., Finberg, S. L., Young-Waithe, K. A., Choy, H. K. H., Masaki, M. M., and Fonstad, C. G. (2001). Enhanced photogeneration of carriers in a semiconductor via coupling across a nonisothermal nanoscale vacuum gap. *Appl. Phys. Lett.* **79**, 1894.
31. Schaller, R. D., and Klimov, V. I. (2004). High efficiency carrier multiplication in PbSe nanocrystals: implications for solar energy conversion. *Phys. Rev. Lett.* **92**, 186601. DOI:10.1103/PhysRevLett.92.186601.
32. Grätzel, M. (2001). Sol-gel processed $TiO_2$ films for photovoltaic applications. *J. Sol-Gel Sci. Technol.* **22**, 7–13.

# PUBLIC HEALTH

# THREAT FROM EMERGING INFECTIOUS DISEASES

ROGER W. PARKER
*DoD Veterinary Food Analysis and Diagnostic Laboratory, Fort Sam Houston, Texas*

## 1 AGROTERRORISM POTENTIAL OF EMERGING INFECTIOUS DISEASES

The US National Strategy for Homeland Security identifies agriculture, food, and water among the critical infrastructure sectors that must be protected. Agroterrorism is an intentional criminal act perpetrated on some segment of the agriculture or food industry intended to inflict harm (e.g. public health crisis or economic disruption). Although the use of biological weapons against targets by state-sponsored terrorists, rouge terrorist groups, and even isolated individuals is highly unpredictable, there have been attempts to assess risks [1]. In June 1999, the US Centers for Disease Control and Prevention (CDC) convened a meeting of national experts to review potential general criteria for selecting the bioagents that pose the greatest threats to civilians, concluding in a list divided into three categories (A, B, and C) based on such criteria as threat to national security, public health impact (disease and death), production and delivery potential, public perception as related to public fear and potential civil disruption, and special public health preparedness needs [2]. Many of the agents are associated with emerging infectious diseases [3], an important subset because of potential limited experience in management of cases or outbreaks and lack of appropriate resources [4]. Emerging infectious diseases are those in which incidences have recently increased as a result of the introduction of a new agent, recognition of an existing disease that has previously gone undetected, a reappearance (reemergence) of a known disease after a decline in incidences, or an extension of the geographic range of a known disease [4].

## 2 THREAT DEVELOPMENT

This article offers description of risk factors involved in threats on agriculture and food systems critical for a nation's revenue or defense. It is important to predict plausible

targets and credible events to avoid being surprised by and be unprepared for terrorist attacks [1, 5]. Although examples used are kept to a minimum, considering the abundant possibilities as can be found in public literature, the threat risks from glanders and melioidosis are presented in more detail.

## 2.1 Availability and Cost

For many decades, widely published sources have identified the bioagents suitable for nefarious applications and have provided the technical information on how to produce them in bulk [6]. Despite efforts to restrict the acquisition of dangerous bioagents, it is likely that terrorists and criminals, with some microbiological expertise, will be able to obtain an agent that they want when they want it [7]. Agents have been rated as most available if readily obtainable from soil, animal, insect, or plant sources; somewhat available if mainly available only from clinical specimens, clinical laboratories, or regulated commercial culture suppliers; and, least available if only from nonenvironmental, noncommercial, or nonclinical sources such as high-level security research laboratories [2, 6].

Some examples of soil-borne pathogens include *Bacillus anthracis*, *Clostridium botulinum*, *Clostridium perfringens*, *Burkholderia mallei*, and *Burkholderia pseudomallei*. The ease with which such naturally occurring agents can be acquired varies among geographic regions, according to specific prevalence [1]. The anthrax agent, *B. anthracis*, can be found worldwide in areas of predominately alkaline soils. Endemic anthrax in nature characteristically occurs in herbivores grazing contaminated land or eating contaminated feed [8, 9]. Also, there can be contamination of naturally occurring *B. anthracis* in the wool, hair, or hides of these herbivores. Other environmental sources for pathogens include surface and coastal waters, the ecology of which can serve as reservoirs for *Giardia*, *Cryptosporidium*, *Naegleria fowleri*, *Vibrio cholerae*, and *Vibrio vulnificus*.

Zoonotic bioagents (transmissible from animal hosts or reservoirs to humans) naturally available in animals include *Yersinia pestis* (rodents), *Brucella melitensis* (small ruminants), *Francisella tularensis* (rodents, rabbits, and hares), *B. mallei* (equine), and Nipah virus (porcine). Naturally sourced foreign animal disease threats to US agriculture include foot-and-mouth disease (FMD) virus (in ungulates), hog cholera (porcine), rinderpest virus (bovine), African swine fever virus (porcine), African horse sickness virus (equine), and velogenic Newcastle disease virus (avian).

Among the plant pathogens available in nature, which could threaten agriculture production are *Candidatus Liberibacter americanus* (citrus greening disease), *Peronosclerospora philippinensis* (Philippine downy mildew of maize), *Phakopsora pachyrhizi* (Asian soybean rust), *Ralstonia solanacearum* (southern bacterial wilt in many plants), *Xanthomonas oryzae* (bacterial leaf blight in rice), *Xylella fastidiosa* (citrus variegated chlorosis strain), *Tilletia indica* (karnal bunt of wheat), and *Puccinia* fungi (stem rust for cereals and wheat).

It is not uncommon for biological weapons to be referred to as the "poor man's weapon of mass destruction." Bacterial pathogen and toxin production can use basic and easily available equipment (e.g. culture media, flasks, vials, incubators or fermenters, and microscopes) in facilities ranging from crude makeshift labs to advanced, state-run facilities [10]. Viral production using egg or cell cultures requires more advanced technology. It has been estimated that less than a few hundred thousand dollars would be needed for bioagent research, testing, production, and weaponization. However, Kathleen Bailey, a national security analyst and a former assistant director of the US Arms Control and Disarmament Agency, has speculated that it may only require tens of thousands of dollars,

using a modestly equipped 15 × 15 ft room [6]. Among the cost for terrorists to consider would be risk of self-inoculation of virulent organisms like *F. tularensis* and *B. anthracis*.

### 2.2 Ease and Route of Dissemination

The bioagent must be collected in sufficient quantities or cultured to reach the dose required to cause harm, and additional procedures may be necessary in the preparation of the final product in a gaseous, liquid, or solid form [1]. Because a bioagent may be inconspicuous during delivery, the first evidence of a biological attack may be the onset of disease, days or even weeks later, making it difficult or impossible to determine that an outbreak resulted from an intentional act [7]. Other dissemination factors to consider are the stability of the agent and potential for host-to-host transmission of the agent [2]. A contagious microorganism may be disseminated at lower doses because it could spread in secondary waves of infection following its multiplication in the infected hosts [1].

Of potentially greater impact but smaller probability (because of very complex technology) is terrorist dissemination of a bioagent in an aerosol cloud [7, 11]. During biological warfare defense programs, it was calculated that an ideal aerosol cloud should consist of particles of 1–5 μm in size, as particles much larger than 5 μm do not penetrate into the lungs (they tend to settle out of the air relatively quickly and are filtered out by the upper respiratory tract) and smaller particles do not remain in the lungs (they are likely to be breathed out) [12]. Intentional aerosol contamination of production crops would be less complicated in that plant pathogens could be disseminated by a crop duster or even hand spray pumps [13].

Terrorists can also spread bioagents by contaminating food anywhere in the food system's continuity. Tommy Thompson, former Secretary of the US Department of Health and Human Services, stated in 2004, "For the life of me, I cannot understand why the terrorists have not attacked our food supply, because it is so easy to do [14]." Contamination at a centralized facility may affect large numbers of people down the distribution chain. Contamination at the retail outlet may have more limited direct population reach but still escalate because of the terror aspect. Contamination of food that will not be subject to further cooking is the most vulnerable, unless a heat-resistant bioagent or toxin is used. The most successful recent foodborne attack was perpetrated by a religious cult, known as the Rajneeshees, employing *Salmonella typhimurium* in restaurant salad bars against the people of The Dalles, a small town in Oregon, in August and September 1984 [7]. Deliberate contamination of municipal water systems is also a target of concern but fortunately direct harmful effects would be limited by dilution, disinfection, filtration, and nonspecific inactivation [15]. Smaller water sources are more vulnerable as evidenced in 1990 when nine people in Edinburgh, United Kingdom, were infected with *Giardia lamblia* when the water-supply tank of their apartment building was deliberately contaminated with fecal material [16].

A reliable mode for small-scale dissemination of bioagents would be direct application or injection of victims with a pathogen or toxin [7]. On a larger scale, infected food handlers could maliciously serve as modern-day "Typhoid Mary(s)", purposely harboring and transmitting *Shigella*, *Salmonella*, *Campylobacter*, *V. cholerae*, *Giardia*, *Cryptosporidium parvum*, *Cyclospora cayetanensis*, *Balantidium coli*, *Entamoeba histolytica*, *Ascaris lumbricoides*, hepatis A virus, norovirus, and rotavirus. It would seem that nature does not need assistance from terrorists as one highly cited source estimates that foodborne diseases cause approximately 76 million illnesses, 325,000 hospitalizations, and 5000 deaths in the United States each year [17].

Intentional transmission of diseases through insect vectors is also a potential risk. Some examples include plague (transmitted by certain flea species), yellow fever (carried by a specific mosquito species, *Aedes aegypti*), and typhus (spread by the body louse, *Pediculus humanus corporis*) [7]. During World War II, Japanese planes were suspected of dropping plague-infected fleas in advance of plague epidemics affecting China and Manchuria [18]. Among the challenges to overcome is establishing a program to breed and infect the necessary vectors and controlling them following release [7].

An example of an agent that is potentially harmful regardless of its route of dissemination is *B. anthracis*. Anthrax in humans is frequently classified as per the route by which the disease is acquired: cutaneous anthrax acquired through a skin lesion, gastrointestinal tract anthrax contracted from ingestion of contaminated food (primarily meat from an animal that died of the disease), and pulmonary (inhalation) anthrax from breathing in airborne anthrax spores [9, 19].

It is commonly considered that FMD virus can be introduced into a free area by various means: direct or indirect contact with infected animals through aerosols, feeding contaminated garbage, and contact with contaminated objects. After a susceptible animal becomes infected, rapid and exponential spread via respiratory aerosols can occur.

### 2.3 Virulence and Susceptible Host Range

Biological agents can be used to attack a wide variety of targets including humans, animal herds, and food at any point during the farm-to-food continuum (including stored or processed food) [20]. The pathogens considered and attempted over history have involved a wide spectrum of virulence, from those with little ability to cause disease or disability to some of the agents deemed most deadly [7, 11]. The CDC Category A agents generally have the potential to cause high morbidity and mortality with Category B agents threatening moderate morbidity and mortality [2].

Many of the diseases in the CDC bioterrorism categories are of zoonotic nature. For example, apparently all warm-blooded species can be infected by *B. anthracis* [9]. While it appears that humans are moderately resistant to anthrax [9], such innate resistance can be overcome by sufficient exposure level, poor prior health or immune status of the exposed individual, or by the use of a strain of *B. anthracis* possessing critical virulence factors [7, 19].

Concerning susceptible animal populations, it has been recommended that farm operators and veterinarians maintain expertise in recognizing and reporting suspected foreign animal diseases [21]. Among the educational resources is the list published by the Office International des Epizooties (OIE) (available at http://www.oie.int/eng/maladies/en_classification.htm) concerning animal diseases that are highly infectious, capable of rapidly spreading across international borders, and having the potential to inflict catastrophic economic losses and social disruption. As an example, there are many subtypes of FMD virus of varying virulences, which can sicken cloven-hoofed domestic and wild animals. An FMD outbreak can widely spread through an area using sheep as maintenance hosts, pigs as amplifiers, and cattle as indicators.

### 2.4 Impact and Public Perception

Depending upon the efficiency of an aerosol dissemination system and the population density of targets, a biological weapon could produce up to hundreds of thousands of casualties [6]. Even without inflicting an actual illness or physical injury, a terrorist can achieve objectives of fear, societal disruption, and/or economic damage (considering the

usage of hoaxes) [1]. Notoriety of a bioagent can influence the public perception from its use or threatened use. The fearsome anthrax agent is the most frequent pathogen of recent historical use or threat. Dr W. Seth Carus has researched nearly 270 alleged bioterrorism or biocrime cases involving biological agents used in crimes and found *B. anthracis* associated with at least 113 cases, largely due to the growing popularity of anthrax threats [7]. Confirmation of an anthrax attack would result in expensive and time-, labor-, and resource-consuming control and decontamination measures to include treatment of human cases, isolation of animal cases, quarantine of exposed animals, animal carcass disposal, and environmental decontamination [9]. One published estimate of economic impact of an aerosolized anthrax attack scenario against humans reached $26.2 billion per 100,000 persons exposed [22]. Because of the uncertainty and fear surrounding anthrax attacks, it has been estimated that for every exposed person, an additional 15 may request medical intervention because of exposure concerns [22]. To a lesser extent but of still significant burden, will be the resulting control and recovery measures for confirmed agroterrorism events with any other agents.

Because agriculture disease outbreaks have the potential to cause economic chaos, plants and livestock are an attractive target to potential terrorists [13, 23]. In 2001, the US Food and Fiber system (FFS) provided employment for 23.7 million Americans (e.g. farmers, processors, manufacturers, wholesalers, retailers, restaurateurs, and transporters) and was a supplier of products worldwide [24]. The total FFS economy added $1.24 trillion to the nation's gross domestic product (GDP); 12.3% of the nation's total GDP [24]. Briefly, concerning economic downstream instability, every bushel of wheat, corn, or soybeans in addition to beef carcasses and pork bellies, has a futures contract written in United States and foreign exchanges, meaning multidimensional financial losses on unfulfilled contracts, including damage on handling and transportation commerce [13]. The scale of nationwide FMD outbreaks is mind-boggling (e.g. in 1997, Taiwan slaughtering over 8 million pigs, over $20 billion estimated total cost; in 2001, the United Kingdom destroying 4.2 million animals, approximately $9.6 billion in direct compensation payments) [13]. Similarly, introduction of foreign animal diseases in the United States would require drastic rapid measures, usually disease eradication, to reopen agriculture exports. Eradication efforts are costly. For example, in 1983–1984 the control and eradication of a highly pathogenic avian influenza outbreak cost the US Department of Agriculture $60 million and the average cost of one dozen eggs increased by 5% [25]. To complete hog cholera eradication during the 1971–1977 outbreak, the US government spent $79 million [26]. Because animals have special places in families and society, any animal disease tragedy reflects on and in people. For example, the 2001 FMD outbreak in England was accompanied and followed by human distress, feelings of bereavement, fear of a new disaster, and loss of trust in authority and control systems [27].

## 3 GLANDERS AND MELIODOSIS

The agents causing glanders (*B. mallei*) *and* melioidosis (*B. pseudomallei*) are closely related mesophilic (optimal temperature for growth is 37°C), gram-negative rods. Glanders is primarily a disease affecting equines, involving the upper respiratory tract (purulent nasal discharge) and the lungs (pneumonia). Farcy is the cutaneous form (nodules, pustules, and ulcers) of the equine disease. Melioidosis is primarily a human disease ranging from asymptomatic pulmonary consolidation to localized cutaneous or visceral abscesses, necrotizing pneumonia, or rapidly fatal septicemia [28].

### 3.1 Availability and Cost

The glanders agent has either disappeared or been eradicated from most areas of the world. Of particular concern is that recent reports of glanders are mostly from Middle Eastern and Asian countries such as Turkey, United Arabic Emirates, Iraq, Iran, India, Pakistan, Mongolia, and China [29]. Rogue or state-sponsored terrorists could acquire this agent via natural sources. The melioidosis organism can likewise be acquired by terrorists as it is free-living on dead organic material in certain soils, mud, and waters in many tropical and subtropical areas of Africa, America, Asia, Australia, Pacific Islands, India, and the Middle East [28, 30]. In Thailand it is considered to be a disease of rice farmers [28]. Both of the *Burkholderia* organisms can be cultured on simple media, including nutrient, blood, and MacConkey agar [31]. Bulk culture of the agents would expose laboratory workers to significant occupational disease risk [32]. Because both are Category B select agents, acquisition from laboratory sources would require theft or other illegal activities.

### 3.2 Ease and Route of Dissemination

Historically, *Burkholderia* agents were viewed as suitable bioweapons because of their ability to initiate infection in normal individuals via aerosol [31]. Inhalation delivery would require complex technical work by terrorists with uncertain success. Because wound infections are common in nature, a terrorist may be able to induce disease by contaminated wound-inducing debris or shrapnel. Oral exposure may be a concern because it is thought that ingestion could cause clinical disease especially in immunocompromised or overwhelmed hosts. Despite the apparent ease with which melioidosis may be acquired from the environment, there is little evidence of the secondary spread from cases of the disease [31].

### 3.3 Virulence and Susceptible Host Range

Glanders primarily affects horses, donkeys, and mules, but can be naturally contracted by goats, dogs, and cats [33]. Various animals, including sheep, goats, horses, swine, monkeys, and rodents can become infected with melioidosis [28]. Human clinical melioidosis is uncommon, generally occurring in individuals with impaired immunocompetence whose nonintact skin had intimate contact with contaminated soil or surface water [28]. Approximately two-thirds of melioidosis cases have a predisposing medical condition such as diabetes, cirrhosis, alcoholism, or renal failure [28]. Four clinical forms of glanders and melioidosis are generally described: localized infection (skin, brain, or visceral abscesses, lymphadenitis, osteomyelitis, septic arthritis), pulmonary infection, septicemia, and chronic suppurative infections of the skin, soft tissues, or viscera [33]. Of these two diseases, glanders is ranked as a higher threat than melioidosis because of a greater likelihood of death if not treated [2].

### 3.4 Impact and Public Perception

Although terrorism from the *Burkholderia* agents may not cause widespread direct clinical illnesses, there would still be significant psychological impact because of the infamous history of these biothreats. It is known that during World War I, Germany distributed cultures of *B. mallei* to undercover agents who attempted to infect livestock that were

to be shipped to Allied countries [34]. Glanders was among the agents used to infect human victims by Japan's notorious Unit 731 in Manchuria under the direction of Ishii Shiro [35]. Purported victims may worry for a long time because although the incubation period for melioidosis can be as short as 2 days, there are cases where years have elapsed between presumed exposure and appearance of clinical disease [28].

As an intentionally introduced foreign animal disease, the US agricultural system and horse-owning population would be significantly disaffected with required quarantine, test, and eradication programs for glanders. It may take time before it is recognized in a previously uninfected region. Initial cases may be misdiagnosed and animal carriers would spread the disease in the regular course of commerce and movement. It is a notifiable disease to the OIE and export restrictions would be placed on US origin equines. Environmental contamination or threatened contamination by *Burkholderia* agents may involve troublesome detection procedures to separate these agents from other ubiquitous microbiological relatives, including other *Burkholderia* spp. and the *Pseudomonas* spp.

## REFERENCES


1. Elad, D. (2005). Risk assessment of malicious biocontamination of food. *J. Food Prot.* **68**(6), 1302–1305.
2. Rotz, L. D., Khan, A. S., Lillibridge, S. R., Ostroff, S. M., and Hughes, J. M. (2002). Public health assessment of potential biological terrorism agents. *Emerg. Infect. Dis.* **8**(2), 225–230.
3. Whitehouse, C. A., Schmaljohn, A. L., and Dembek, Z. F. (2007). Emerging infectious diseases and future threats. In *Medical Aspects of Biological Warfare*, Z. F. Dembek, Ed. Borden Institute, Washington, DC, pp. 579–607.
4. Feldmann, H., Czub, M., Jones, S., Dick, D., Garbutt, M., Grolla, A., and Artsob, H. (2002). Emerging and re-emerging infectious diseases. *Med. Microbiol. Immunol.* **191**(2), 63–74. DOI: 10.1007/s00430-002-0122-5.
5. Tucker, J. B. (2004). Biological threat assessment: is the cure worse than the disease? *Arms Control Today.* **34**(8), 13–19.
6. Falkenrath, R. A., Newman, R. D., and Thayer, B. A. (1998). *America's Achilles' Heel: Nuclear, Biological, and Chemical Terrorism and Covert Attack*, MIT Press, Cambridge, MA.
7. Carus, W. S. (2002). *Bioterrorism and Biocrimes: The Illicit Use of Biological Agents Since 1900*, Fredonia Books, Amsterdam.
8. Purcell, B. K., Worsham, P. L., and Friedlander, A. M. (1997). Anthrax. In *Medical Aspects of Biological Warfare*, Z. F. Dembek, Ed. Borden Institute, Washington, DC, pp. 69–90.
9. Turnbull, P. C. B. (1998). *Guidelines for the Surveillance and Control of Anthrax in Human and Animals*, 3rd ed., World Health Organization, Geneva.
10. Frerichs, R. L., Salerno, R. M., Vogel, K. M., Barnett, N. B., Gaudioso, G., Hickok, L. T., Estes, D., and Jung, D. F. (2004). *Historical Precedence and Technical Requirements of Biological Weapons Use: a Threat Assessment*, Sandia Report. May, 1854, pp. 1–76.
11. Kortepeter, M. G., and Parker, G. W. (1999). Potential biological weapons threats. *Emerg. Infect. Dis.* **5**(4), 523–527.
12. Eitzen, E. M. (1997). Use of biological weapons. In *Medical Aspects of Chemical and Biological Warfare*, F. R. Sidell, E. T. Takafuji, and D. R. Franz, Eds. Borden Institute, Washington, DC, pp. 437–450.
13. Gilmore, R. (2004). US food safety under siege? *Nat. Biotechnol.* **22**(12), 1503–1505.
14. Neild, B. (2006). *Agroterrorism: How Real is the Threat?* Sep 25. Available at http://www.cnn.com/2006/WORLD/americas/09/25/agroterrorism/, accessed March 7, 2009.

15. Anonymous (2004). Precautions against the sabotage of drinking-water, food, and other products. In *Public Health Response to Biological and Chemical Weapons—WHO Guidance*, J. P. P. Robinson, Exec. Ed. 2nd ed., World Health Organization, Geneva, pp. 294–319.
16. Ramsay, C. N., and Marsh, J. (1990). Giardiasis due to deliberate contamination of water supply. *Lancet* **336**, 880–881.
17. Mead, P. S., Slutsker, L., Dietz, V., McCaig, L. F., Bresee, J. S., Shapiro, C., Griffin, P. M., and Tauxe, R. V. (1999). Food-related illness and death in the United States. *Emer. Infect. Dis.* **5**(5), 607–625.
18. Anonymous (2001). History of biological warfare and current threat. In *USAMRIID's Medical Management of Biological Casualties Handbook*, M. Kortepeter, G. Christopher, T. Cieslak, R. Culpepper, R. Darling, J. Pavlin, J. Rowe, K. McKee, and E. Eitzen, Eds. 4th ed. U.S. Army Medical Research Institute of Infectious Diseases, Fort Detrick, MD, pp. 3–10.
19. Anonymous (2001). Anthrax. In *USAMRIID's Medical Management of Biological Casualties Handbook*, M. Kortepeter, G. Christopher, T. Cieslak, R. Culpepper, R. Darling, J. Pavlin, J. Rowe, K. McKee, and E. Eitzen, Eds. 4th ed., U.S. Army Medical Research Institute of Infectious Diseases, Fort Detrick, MD, pp. 26–35.
20. Dembek, Z. F., and Anderson, E. L. (2007). Food, waterborne, and agricultural diseases. In *Medical Aspects of Biological Warfare*, Z. F. Dembek, Ed. Borden Institute, Washington, DC, pp. 21–38.
21. Noah, D. L., Noah, D. L., and Crowder, H. R. (2002). Biological terrorism against animals and humans: a brief review and primer for action. *J. Am. Vet. Med. Assoc.* **221**(1), 40–43.
22. Kaufmann, A. E., Meltzer, M. I., and Schmid, G. E. (1997). The economic impact of a bioterrorist attack: are prevention and postattack intervention justifiable? *Emerg. Infect. Dis.* **3**(2), 83–94.
23. Ashford, D. A., Gomez, T. M., Noah, D. L., Scott, D. P., and Franz, D. R. (2000). Biological terrorism and veterinary medicine in the United States. *J. Am. Vet. Med. Assoc.* **217**(5), 664–667.
24. Edmondson, W. (2004). Economics of the food and fiber system. *Amber Waves* **2**(1), 12–13.
25. Lasley, F. A., Short, S. D., and Henson, W. L. (1985). *Economic Assessment of the 1983-84 Avian Influenza Eradication program*, United States Department of Agriculture, Economic Research Service, National Economics Division. U.S. Government Printing Office, Washington, DC.
26. Wise, G. H. (1981). *Hog Cholera and its Eradication: A Review of U.S. Experience*, U.S. Department of Agriculture, Animal and Plant Health Inspection Service. U.S. Government Printing Office, Washington, DC.
27. Mort, M., Convery, I., Baxter, J., and Bailey, C. (2005). Psychosocial effects of the 2001 UK foot and mouth disease epidemic in a rural population: qualitative diary based study. *Br. Med. J.* **331**, 1234–1238. DOI:10.1136/bmj.38603.375856.68.
28. Plant, A. (2004). Melioidosis. In *Control of Communicable Diseases Manual*, D. L. Heymann, Ed. 18th ed., American Public Health Association, Washington, DC, pp. 386–388.
29. Neubauer, H., Sprague, L. D., Zacharia, R., Tomaso, H., Al Dahouk, S., Wernery, R., Wernery, U., and Scholz, H. C. (2005). Serodiagnosis of *Burkholderia mallei* infections in horses: state-of-the-art and perspectives. *J. Vet. Med. B Infect. Dis. Vet. Public Health.* **52**(5), 201–205.
30. Inglis, T. J., Rolim, D. B., and Sousa Ade, A.A. (2006). Melioidosis in the Americas. *Am. J. Trop. Med. Hyg.* **75**(5), 947–954.
31. Dance, D. A. B. (2005). Melioidosis and glanders as possible biological weapons. In *Bioterrorism and Infectious Agents: A New Dilemma for the 21st Century*, I. W. Fong, and K. Alibek, Eds. Springer Science+Business Media, Inc., New York, pp. 99–145.

32. Srinivasan, A., Kraus, C. N., DeShazer, D., Becker, P. M., Dick, J. D., Spacek, L., Bartlett, J. G., Byrne, W. R., and Thomas, D. L. (2001). Glanders in a military research microbiologist. *N. Engl. J. Med.* **345**(4), 256–258.

33. Bossi, P., Tegnell, A., Baka, A., Van Loock, F., Hendriks, J., Werner, A., Maidhof, H., and Gouvras, G. (2004). Bichat guidelines for the clinical management of glanders and melioidosis and bioterrorism-related glanders and melioidosis. *Euro. Surveill.* **9**(12), 1–6.

34. Wheelis, M. (1998). First shots fired in biological warfare. *Nature* **395**, 213.

35. Harris, S. (1999). The Japanese biological warfare programme: an overview. In *SIPRI Chemical and Biological Warfare Studies. 18. Biological and Toxin Weapons: Research, Development and Use from the Middle Ages to 1945*, E. Geissler, and J. E. van Courtland Moon, Eds. Oxford University Press, Oxford, pp. 127–152.

## FURTHER READING

Anonymous (1998). Foreign Animal Diseases. In *The Gray Book*, W. W. Buisch, J. L. Hyde, and C. A. Mebus, Eds. 6th ed., U.S. Animal Health Association, Pat Campbell & Associates and Carter Printing Company, Richmond, VA.

Dembek, Z. F., Kortepeter, M. G., and Pavlin, J. A. (2007). Discernment between deliberate and natural infectious disease outbreaks. *Epidemiol. Infect.* **135**(3), 353–371. DOI:10.1017/S0950268806007011.

Riemann, H. P., and Cliver, D. O. (2005). *Foodborne Infections and Intoxications*, 3rd ed., Academic Press, Amsterdam.

# FOREIGN DENGUE VIRUS PRESENTS A LOW RISK TO U.S. HOMELAND

TERRY CARPENTER, KATHRYN L. CLARK, R. KEVIN HANSON, AND MICHAEL SARDELIS
*National Center for Medical Intelligence, Frederick, Maryland*

## 1 INTRODUCTION

Widespread dengue virus transmission in the continental United States is very unlikely. Media reporting in early 2008 [1, 2] speculating that the dengue virus may soon be

introduced and spread nationwide, as West Nile virus (WNV) did previously, have grossly overstated the threat. Once WNV was imported into the United States, many factors facilitated its spread and long-term establishment, which do not apply to dengue virus [3]. While sustained dengue virus transmission is unlikely, isolated cases or small case clusters of local transmission resulting from sporadic introduction by infected travelers will continue to occur in limited areas of the country where competent mosquito vectors are present. Such cases will likely be identified and contained by effective US public health responses.

## 2 BACKGROUND OF DENGUE AND WEST NILE VIRUSES

### 2.1 Worldwide Dengue Distribution

Dengue fever is transmitted at high levels year round throughout most tropical areas worldwide, including Central and South America, the Caribbean, southern and southeast Asia, the south Pacific, and parts of Africa. An estimated 50–100 million cases occur each year and the geographic distribution of dengue fever continues to expand (Fig. 1) [4].

### 2.2 History of Dengue Virus in the United States

Dengue fever, which was once endemic in the United States, was eliminated around 1950. No known outbreaks occurred between 1950 and 1980. However, small outbreaks of locally acquired dengue fever have been reported recently in southern Texas, usually in association with epidemic dengue spillover from adjacent Mexican states [5].

### 2.3 History of West Nile Virus in the United States

WNV has reemerged in the United States every year since 1999 and has expanded its range to include all states in the continental United States (Fig. 2). [6]. The spread of WNV has been aided by its ability to "overwinter" in birds and mosquitoes [7].

WNV has become widespread because it is maintained in nature principally in a mosquito-bird cycle [3]. Historically, migrating birds have spread WNV over a large are of the world, most recently in North America [6]. The spread and establishment of WNV has been assisted by the ability of the virus to infect many different bird and mosquito species [6].

**(U) Clinical dengue fever and WNV**

(U) Dengue virus causes dengue fever, dengue hemorrhagic fever, and dengue shock syndrome in humans.

(U) West Nile virus causes West Nile fever and neuroinvasive disease labeled as West Nile encephalitis, West Nile meningitis, or West Nile poliomyelitis.

(U) No vaccine is currently available to prevent any of these diseases.

**FIGURE 1** Clinical dengue fever and West Nile Virus.

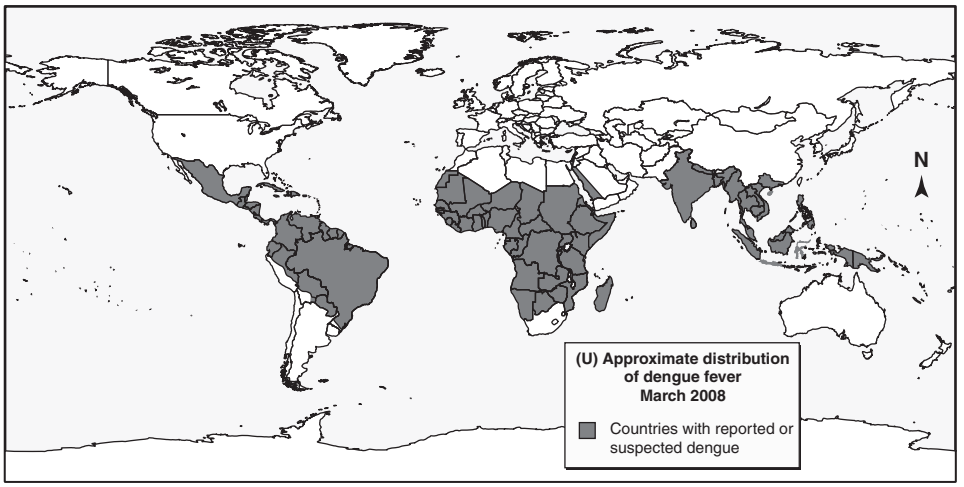



**FIGURE 2** Approximate worldwide distribution of dengue virus.

## 3 SEVERAL FACTORS REDUCE THE LIKELIHOOD OF SUSTAINED DENGUE VIRUS TRANSMISSION IN THE UNITED STATES AS COMPARED TO WNV

### 3.1 Disease Promulgation Multifactorial

For dengue virus to be transmitted in the United States, an infected traveler must arrive in the United States within the incubation period, typically 4–7 d (range 3–14 d) [4]. Persons already experiencing symptoms are unlikely to be well enough to travel. This relatively narrow time window reduces the odds that a traveler will arrive while incubating infection. Once in the United States, infected individuals must be bitten by a competent mosquito vector during the 3–5 d of viremia. Bites before or after this period, will not infect the mosquito. During viremia, the great majority of dengue fever patients will be severely debilitated or bedridden and unable to sustain normal activities, further limiting outdoor contact with mosquitoes. In order to transmit infection, the infected mosquito vector must bite another person 8–12 d after taking the blood meal from the original infected patient. The predominant competent mosquito vector in the United States is relatively inefficient at passing the infection to other humans, because it tends to feed only once, and also tends to bite other animals instead of humans [4].

### 3.2 Dengue Virus Mosquito Vectors Differ from those of WNV

Dengue virus mosquito vectors are not as numerous or as widely distributed in the United States as are WNV mosquito vectors (Fig. 3) [8]. WNV is transmitted by more than 60 species of mosquitoes, including the *Culex* species, which are distributed throughout the continental United States. Dengue virus is transmitted by *Aedes aegypti* and *Aedes albopictus*, which leave much of the United States uncovered. The overwhelming majority of dengue-infected people who travel to the United States do not encounter the mosquito vector to begin the transmission cycle.


**FIGURE 3** Approximate distribution of vectors of dengue virus and West Nile virus in the United States.

### 3.3 The Natural Ecology of Dengue Virus Differs from that of WNV in Ways that do not *Favor* Spread and Long-Term Establishment

Dengue viruses use humans as reservoir hosts. Neither migratory birds, nor any other bird species, have a role in the natural cycle and spread of dengue [9]. WNV has become widespread because it is principally maintained in a mosquito-bird cycle. Migrating birds act as vehicles to spread WNV over a large area [6]. The long-term establishment of WNV has been aided by its ability to "overwinter" in birds and mosquitoes, which allows WNV outbreaks to occur year after year in an area without reintroduction of the virus [7]. Dengue virus is transmitted in a mosquito-human cycle; birds have no role in the natural cycle and spread Table 1 [3].

In addition to dengue virus, other pathogens maintained exclusively in mosquito-man cycles (yellow fever virus and malaria) have been eliminated from the United States [10–12]. Socioeconomic development (improved housing, piped water systems, and air conditioning), sociobiological changes (people are indoors during early daylight hours, and late afternoon until dusk, the peak biting times), and vector control efforts have helped interrupt transmission of these pathogens despite the continued presence of the mosquito vectors, highlighting the requirement for a high level of mosquito-human contact to maintain dengue virus transmission.

## 4 OBSERVED DENGUE VIRUS IN THE UNITED STATES

### 4.1 Historical Importation

Despite frequent importation of dengue virus into the United States over the past 60 years by travelers to dengue virus endemic areas, no reports have surfaced of substantial outbreaks initiated by these travelers [13, 14]. An estimated 14 million travelers come to the

**TABLE 1 Comparison of Selected Aspects of West Nile and Dengue Viruses**

| Characteristics | West Nile Virus | Dengue Virus |
|---|---|---|
| Natural cycle | Mosquito-bird | Mosquito-human |
| Means of importation | Infected mosquitoes or migratory birds | Infected humans |
| Reservoir | Birds; nearly 300 native species found infected in the United States | Humans |
| Vector | Over 60 species of mosquito, principally *Culex* species | *Aedes aegypti* and *Aedes albopictus* |
| Natural evidence of ability to "overwinter" (e.g. survive during the winter in temperate regions, persist in nature during interepidemic periods) | Yes, using mechanisms involving birds and mosquitoes | None |
| Efficacy of mosquito control programs | Moderate; can be difficult because of the number of mosquito species that serve as vectors and their varied (and some times large) breeding habitats | Good; only two species of mosquitoes serve as vectors, and their breeding habitats (small containers) are readily accessible |

United States from dengue virus endemic areas each year, in addition to tens of millions of migrants who cross into the United States through Mexico. During 1980–2007, five small outbreaks (less than 40 confirmed cases each) occurred in Texas near the border with Mexico [15]. The origins of these outbreaks were associated with spillover from adjacent Mexican states. In addition, Florida has not reported an incident of local dengue virus transmission since 1934 [10]. Indigenous transmission is very rare.

### 4.2 Importation through Military Redeployment

The likelihood of military personnel redeploying from dengue-endemic areas and initiating local transmission of dengue virus in the United States is very low. Military personnel do deploy and travel to highly endemic areas, and in rare instances a limited number have contracted dengue fever while deployed (e.g. Haiti, Somalia) [16, 17]. Dengue fever outbreaks have not been observed in the United States upon redeployment because the deployed population is thoroughly screened for illness, consistent with established requirements for the military health system to conduct deployment health assessments.

## 5 UNITED STATES COUNTERMEASURES MITIGATE RISK

Public health readiness and public awareness of the threat of vector-borne viruses have been heightened, largely as a result of the introduction of WNV. Dengue fever outbreaks that do occur in the United States are relatively small and are quickly identified and contained by effective public health practices. Areas with increased risk for dengue introduction, such as Florida and Texas, have very well-developed and proven surveillance systems that remain alert for dengue cases [18]. Public health countermeasures

will prohibit transmission from progressing far enough to reach a sufficiently large enough reservoir of infected humans necessary to sustain a large outbreak.

## 6 SUMMARY AND CONCLUSIONS

Myriad infectious diseases exist throughout the world and conceivably could enter the United States. Careful identification and prioritization of significant foreign infectious disease threats which could be imported into the United States and develop into considerable public health challenges are critical to developing and maintaining appropriate Homeland Security countermeasures. A methodological scientific approach involving the cooperation of the intelligence community (with their assessments of diseases in foreign countries) and domestic agencies (with their knowledge of existing mitigating factors such as airport screening, vaccination, and vector control) would provide defensible rationale for allocation of countermeasure resources and establishment of homeland security procedures.

## REFERENCES

1. Ricardo, A.-Z. (2008). Dengue fever is not quite dead. *Los Angeles Times*, 10.
2. Fox, M. (2008). Tropical dengue fever may threaten U.S.: report. *Reuters*, http://www.reuters.com/article/scienceNews/idUSN08478564200801 08?sp=true.
3. Glaser, V. (2001). Dengue West Nile virus—an interview with Duane Gubler Sc.D. *Vector Borne and Zoontoic Dis*. **1**(1), 81–88.
4. Heymann, D. L. (Ed.) (2004). Dengue fever. *Control of Communicable Diseases Manual*. American Public Health Association, Washington, DC, pp. 146–149.
5. Reiter, P., Lathrop, S., Bunning, M., Biggerstaff, B., Singer, D., Tiwari, T., Baber, L., Amador, M., Thirion, J., Hayes, J., Seca, C., Mendez, J., Ramirez, B., Robinson, J., Rawlings, J., Vorndam, V., Waterman, S., Gubler, D., Clark, G., and Hayes, E. (2003). Texas lifestyle limits transmission of dengue virus. *Emerg. Infect. Dis*. **9**(1), 86–89.
6. Gubler, D. (2007). The continuing spread of West Nile virus in the Western Hemisphere. *Clin. Infect. Dis*. **45**, 1039–1046.
7. Reisen, W. K., Fang, Y., Lothrop, H. D., Martinez, V. M., Wilson, J., O'Connor, P., Carney, R., Cahoon-Young, B., Shafii, M., and Brault, A. C. (2006). Overwintering of West Nile virus in Southern California. *J. Med. Entomol*. **43**(2), 344–355.
8. Moore, C. G., and Mitchell, C. J. (1997). Aedes albopictus in the United States: ten-year presence and public health implications. *Emerg. Infect. Dis*. **3**(3), 329–334.
9. Weaver, S. C., and Barrett, A. D. (2004). Transmission cycles, host range, evolution and emergence of arboviral disease. *Nature* **2**, 789–801.
10. Ehrenkranz, N. J., Ventura, A. K., Cuadrado, R. R., Pond, W. L., and Porter, J. E. (1971). Pandemic dengue in Caribbean countries and the Southern United States-past, present and potential problems. *N. Engl. J. Med*. **285**(26), 1460–1469.
11. Thwing, J., Skarbinski, J., Newman, R. D., Barber, A. M., Mali, S., Roberts, J. M., Slutsker, L., and Arguin, P. M. (2007). Malaria surveillance—United States, 2005. *MMWR* **56**(SS06), 23–38.
12. World Health Organization (1986). Present status of yellow fever. *Bull. World Health Organ*. **64**(4), 511–524.
13. Abell, A., Smith, B., Fournier, M., Betz, T., Gaul, L., Robles-Lopea, J. L., Carrillo, C. A., Rodriguez-Trujillo, A., Rabelly-Moya, C., Velasquez-Monroy, O., Alvarez-Lucas, C.,

Kuri-Morales, P., Anaya-Lopez, L., Hayden, M., Zielinski-Butierrez, E., Munoz, J., Beatty, M., Sosa, I., Wenzel, S., Excobedo, M., Waterman, S., Ramos, M., Kapella, B. K., Mohammed, H., Taylor, R., and Brunkard, J. (2007). Dengue hemorrhagic fever—U.S. Mexico border, 2005. *MMWR* **56**(31), 785–789.

14. Rawlings, J., Burgess, C., Tabony, L., Campman, R., Hendricks, K., Stevenson, G., Vela, L., Simpson, D., Tapia-Conyer, R., Matus, C. R., Gomez-Dantes, H., Montesanos, R., Flisser, A., Briseno, B., Bernal, S. I., Medina, C. C., Flores, G., Coello, G. C., Hayes, J., Craig, G. B., Blackmore, M. S., and Mutebi, J. P. (1996). Dengue fever at the U.S. Mexico border, 1995-1996. *MMWR Morb. Mortal. Wkly. Rep*. **45**(39), 841–844.
15. Ayala, A., Rivera, A., Johansson, M., Munoz, J., Ramos, M., and Mohammed, H. (2006). Travel-associated dengue—United States, 2005. *MMWR* **55**(25), 700–702.
16. Defraites, R., Smoak, B., Trofa, A., Hoke, C., Kanesa-thasan, N., King, A., MacArthy, P., Putnak, J., Burrous, J., Oster, C., Redfield, R., Aronson, N., Brown, M., Fishbain, J., Deal, V. T., Quan, J., Jollie, A., Long-acre, J., Shuette, J., Logan, T., Jahrling, P., and Rossi, C. (1994). Epidemiologic notes and reports dengue fever among U.S. military personnel—Haiti, September-November, 1994. *MMWR* **43**(46), 845–848.
17. Sharp, T. W., Wallace, M. R., Hayes, C. G., Sanchez, J. L., DeFraites, R. F., Arthur, R. R., Thornton, S. A., Batchelor, R. A., Rozmajzl, P. J., and Hanson, R. K. (1995). Dengue fever in U.S. troops during Operation Restor Hope, Somalia, 1992-1993. *Am. J. Trop. Med. Hyg.* **53**(1), 89–94.
18. Lister S. A. (2005). *An Overview of the U.S. Public Health System in the Context of Emergency Preparedness*, Congressional Research Service http://www.fas.org/sgp/crs/homesec/RL31719.pdf.

# DATA SOURCES FOR BIOSURVEILLANCE

RONALD A. WALTERS

*Pacific Northwest National Laboratory, Richland, Washington*

PETE A. HARLAN, NOELE P. NELSON, AND DAVID M. HARTLEY

*Division of Integrated Biodefense, Imaging Science and Information Systems, Georgetown University Medical Center, Washington, D.C.*

## 1 INTRODUCTION

As recognized recently in the 2005 revision of the International Health Regulations, early detection of disease is vital in responding to dangerous situations in a timely manner [1]. Researchers have explored the potential for identifying distinctive environmental [2–4],

climatic [5–7], and human behavior [8–10] signatures for rapid identification of outbreaks and epidemics [11]. Biosurveillance is the discipline in which diverse data streams such as these are characterized in real or near–real-time to provide early warning and situational awareness of events affecting human, plant, and animal health. Biosurveillance is distinct from the traditional public health surveillance; in that biosurveillance does not rely on classical epidemiologic studies or clinical data, the availability of which can be limited and nearly always lag the events they describe by days or months.

Many biosurveillance systems provide graded alerting of potential infectious disease outbreaks and refine the degree of confidence in these alerts as additional data becomes available. In this way, systems support graded response by public health, agriculture, and other decision makers [12]. Within such a process, evidence suggesting that an infectious disease outbreak is nascent in a particular region or locale cues a biosurveillance system (or perhaps a collection of systems) to search for additional information clarifying disease status. As more data are collected, surveillance becomes more directed and more actionable, ultimately leading to an evidence-based awareness of the situation. In such a way, public health and related organizations are postured to react in proportion to the degree of confidence inferred from biosurveillance and other surveillance activities as time evolves. Such a picture highlights the connectedness of biosurveillance and situational awareness.

## 2 SURVEY OF EXTANT BIOSURVEILLANCE SYSTEMS

This section provides brief descriptions of a sampling of current biosurveillance and situational awareness systems. Some are dedicated solely to global biosurveillance while others have biosurveillance as a component of their primarily domestic missions. Some are available and open to the general public while others limit user access. There is variability among capabilities for archiving and free-text searching, and these systems vary according to the languages included in sources. Each system was designed for a specific purpose, and each uses a customized approach to capture information useful to end users. In as much as this publication is dedicated to providing a resource for addressing homeland security issues, the compilation below should not be considered an exhaustive listing as similar, although largely domestic programs sponsored by many of the nearly 200 nations in the world are not included. There are systems (e.g. the US government BioWatch network of environmental sensors [13]) that are not included in this study because of a paucity of available information describing them. The systems are listed alphabetically; no ranking should be inferred from the order of presentation. This paper deals with systems that employ event-based unstructured data as opposed to structured data similar to that usually associated with syndromic surveillance.

### 2.1 Animal and Plant Health Inspection Service

Animal and Plant Health Inspection Service (APHIS) is a US Department of Agriculture organization, and its mission is to protect the health and value of American agriculture and natural resources.

- For animal health (http://www.aphis.usda.gov/animal_health/index.shtml), APHIS provides laboratory information services. It also has monitoring and surveillance components that include the National Animal Health Surveillance Systems

(NAHSS), the National Animal Health Reporting Systems (NAHRS), the National Animal Health Laboratory Network (NAHLN), the National Aquaculture Program (NAP), Emerging Animal Disease Notices, and the National Surveillance Unit.

- For plant health (http://www.aphis.usda.gov/plant_health/index.shtml), APHIS includes prevention (plant import regulations and permits, international safeguarding activities, and pest protection) and preparedness (Pest Identification & Diagnostics National Identification Service and National Plant Diagnostic Network) as well as response and recovery activities.

### 2.2 Argus

This project is a prototype biosurveillance system designed to detect and track biological events that may threaten global human, plant, and animal health. It is a cueing and alerting capability complementing both traditional and experimental biosurveillance activities. Argus examines real-time, local native-language media reports posted on the Internet to detect abnormal functioning of social systems; it is a taxonomy-based approach on the basis of direct, indirect, and enviroclimatic indication and warnings [3]. (An ontology is a set of concepts and keywords that are relevant to infectious disease surveillance. A taxonomy is a hierarchical organization of such concepts.) Analysts fluent in approximately 40 languages monitor the output of a large number of media sources and prepare approximately 40,000 reports per year. Argus scans about 1,000,000 articles per day of which 25% are archived. Argus reports can be accessed via http://www.opensource.gov.

### 2.3 BioCaster

BioCaster [14] is an experimental system for global health surveillance under development at the National Institute of Informatics in Japan and is a collaborative research project among five institutes in three countries (http://www.biocaster.org). The system is fully automated using Really Simple Syndication (RSS) feeds from over 1700 sources with no human analysts. Human analysis is assumed to take place downstream by the recipients of its output. BioCaster focuses on the Asia-Pacific region posting approximately 90 articles per day in three languages (English, Japanese, and Vietnamese) with plans for expansion to Thai, Chinese, and other regional languages. Article capture and dissemination is done every hour. Until recently the primary sources were Google News, Yahoo! News, and European Media Monitor, but the system is now expanding to include sources from a commercial news aggregation company which greatly increases its coverage. BioCaster produces an ontology [15] in eight languages (Chinese, English, French, Japanese, Korean, Spanish, Thai, and Vietnamese) that is openly available and is the basis for the Global Health Monitor [16], an open access Web portal for displaying maps and graphs of health events to users (http://www.aclweb.org/anthology-new/I/I08/I08-2140.pdf). The ontology covers approximately 117 infectious diseases of humans and animals as well as six syndromes. Future objectives include extending language and health threat coverage.

### 2.4 Centers for Disease Control and Prevention

The US Centers for Disease Control and Prevention (CDC) supports many resources dedicated to domestic and global public health issues, a number of which are described below (http://cdc.gov).

- Global Disease Detection Centers (http://www.cdc.gov/cogh/gdd/gddCenters.htm). This network of centers is being developed around the world in partnership with Ministries of Health. Six centers, many with regional collaborations, are currently in place (China, Egypt, Guatemala, Kenya, Thailand, and Kazakhstan). These centers will assist CDC in coordinating its resources and expertise more effectively including CDC intramural programs such as the Field Epidemiology Training Program (FETP) (http://www.cdc.gov/cogh/dgphcd/), the International Emerging Infections Program (IEIP) (http://www.cdc.gov/ieip/), and influenza activities (http://www.cdc.gov/flu). They also support implementation of the International Health Regulations (2005) by assisting countries with developing the required core capacities for surveillance and response.
- Global Disease Detection Operations Center (GDDOC). This center serves as the clearing house and coordination point for international outbreak information acquisition and response. It collects information from the GDDOC, other CDC programs, and a wide range of public and private sources. The GDDOC consolidates and interprets information from all its sources to assess severity of outbreaks and to determine and facilitate the appropriate CDC response.
- Early Aberration Reporting System (EARS) (http://emergency.cdc.gov/surveillance/ears/). This domestic capability was established as a method for monitoring bioterrorism and was put into operation in New York City and the national capital region after the terrorist attacks of September 11, 2001. It is used to acquire information about syndromic data, 911 calls, physician data, school and business absenteeism, and over-the-counter drug sales.
- Early Warning Infectious Disease Surveillance (EWIDS) (http://emergency.cdc.gov/surveillance/ewids/) EWIDS is an early warning infectious disease biosurveillance program for the states bordering Canada and Mexico. It is a collaboration of state, federal, and international partners to provide rapid and effective laboratory confirmation of urgent infectious disease case reports in the border regions. Regional collaborations include the Eastern Border Health Initiative, the Great Lakes Border Health Initiative, the Pacific Northwest Alliance, and the US-Mexico Border Region Group.
- Epi-X (http://www.cdc.gov/epix/) initiated in December 2000, is the CDC's secure web-based communications application for public health professionals. The network's primary goal is to provide timely information to health officials about important public health events, to help them respond to public health emergencies, and to encourage professional growth and exchange of information. The main features of Epi-X include scientific and editorial support by CDC personnel, controlled user access, digital credentials and authentication, rapid outbreak reporting, and peer-to-peer consultation. Epi-X access is limited to public health professionals designated by each health agency. Health officials have posted about 6700 reports to date and approximately 4200 users are notified routinely of these postings by e-mail or additionally by pager and telephone depending on the acuteness of the event. Event postings and support are provided 24 h per day, 7 days per week. Epi-X also provides communications to the public through the Morbidity and Mortality Weekly Report (MMWR) and other sources.
- National Electronic Disease Surveillance System (NEDSS) (http://www.cdc.gov/nedss/). NEDSS was developed to rapidly detect outbreaks, monitor the nation's

health and facilitate the electronic transfer of information from clinical information systems to public health departments. It promotes the use of data and information system standards for development of integrated and interoperable surveillance systems at the federal, state, and local levels. It is a major component of the Public Health Information Network (PHIN) (http://www.cdc.gov/phin/).

- BioSense (http://www.cdc.gov/Biosense/) is a national human health surveillance capability developed and hosted by the CDC. It is system of systems that links data from a variety of largely domestic sources to provide a unified national view. It is designed to assist in validating the existence of an outbreak, monitor its status and provide local, state, and national situational awareness.

### 2.5 Emergency Prevention Program for Transboundry Animal Diseases

This global animal health information system compiles, stores, and verifies animal disease outbreak information from many sources (http://empres-i.fao.org/empres-i/). For verification, Emergency Prevention Program for Transboundry Animal Diseases (EMPRES-i) uses both official and nonofficial sources and generates and disseminates early warning messages.

### 2.6 European Center for Disease Control and Prevention

The European Center for Disease Control and Prevention (ECDC), a European Union (EU) agency, was established in 2005 and is based in Stockholm, Sweden (http://ecdc.europa.eu/en/). Its mission (http://ecdc.europa.eu/en/Activities/Epidemic_Intelligence/) is to identify, assess, and communicate current and emerging threats to human health from infectious diseases. A number of information services/systems are operating or being developed at the ECDC that includes the following:

- the ECDC web site (http://ecdc.europa.eu);
- the Eurosurveillance journal (http://www.eurosurveillance.org);
- TESSy—the integrated European communicable disease surveillance system;
- EPIS—the epidemic intelligence portal developed to support outbreak detection, risk assessment, outbreak investigation, and control measures at EU level;
- Knowledge and Information service (KISatECDC)—the content management system for scientific documents produced at the ECDC;
- Preparedness and Response Unit (PRU)—working in partnership with member states across Europe to develop surveillance and early warning systems, the ECDC maintains a staff with 24/7 duty officers and has an emergency operations center. It develops threat tracking tools and issues daily reports collated from a variety of sources numbering among which is the Unit that monitors emerging threats. http://ecdpc.europa.eu/About_us/Preparedness&Response.html

### 2.7 European Influenza Surveillance Scheme

European Influenza Surveillance Scheme (EISS) collects data on influenza in Europe and shares the information with 30 member countries via weekly surveillance reports (http://www.eiss.org/. The reports are derived from information reported by 25,750 sentinel

physicians. EISS objectives are described in more detail at http://www.eiss.org/html/lb_objectives.html, and its methods are summarized at http://www.eiss.org/html/introduction.php.

### 2.8 Global Emerging Infections System

Global Emerging Infections System (GEIS) was established in 1996 within the Department of Defense (DoD) for prevention, surveillance, and response to infectious diseases that could threaten military personnel or their dependents, reduce medical readiness or affect national security (http://www.geis.fhp.osd.mil/). It has a global reach, a number of partners within the DoD, and working relationships with other US and international health agencies. Electronic Surveillance for the Early Notification of Community-based Epidemics (ESSENCE), first developed within GEIS, is a web-based system in support of the DoD health mission (http://www.ehcca.com/presentations/hithipaa414/4_06_1.ppt). It tracks ambulatory and pharmacy data from the US military treatment facilities and alerts users to possible outbreaks of infectious disease and biological incidents.

### 2.9 Global Public Health Intelligence Network

Global Public Health Intelligence Network (GPHIN) was established in 1997 and is managed by the Public Health Agency of Canada's Center for Emergency Preparedness and Response (http://www.phac-aspc.gc.ca/gphin/index-eng.php). It uses the Internet to gather information on eight topics of public health interest. It has global reach and acquires articles from newsfeeds Al Bawaba and Factiva using keywords and terms within a specific taxonomy. Articles about events that may have serious public health consequences are sent to users as e-mail alerts. Machine translation is provided for nine languages (Spanish, French, Russian, Arabic, Farsi, Chinese Simplified and Traditional, Portuguese, and English). GPHIN functions on a near–real-time basis with 24/7 coverage and is staffed with analysts who provide linguistic and interpretive expertise. Customers include the World Health Organization (WHO) and other public and private sector organizations [17].

### 2.10 Health Emergency Disease Information System

Based in Italy, Health Emergency Disease Information System (HEDIS) was developed by the European Commission (EC) to support Directorate General for Health and Consumer Protection (DG SANCO) and public health authorities in Member States (http://hedis.jrc.it/). Its emphasis is crisis management rather than biosurveillance. It provides situational awareness and as such is a central jumping off point for crisis communication. It has approximately 300 users (users are Member States responsible for communicable diseases, CBRN [chemical, biological radiological, nuclear], and communicators) and provides capabilities and tools to assist its customers in dealing with an identified health threat. Included among the rapid alert mechanisms linking Member States with the EU are the following:

- Early Warning and Response System (EWRS) is a web-based system linking the EC with public health authorities in Member States responsible for communicable disease control measures. (http://ec.europa.eu/health/ph_threats/com/early_warning_en.htm)

- Rapid Alert System for Biological and Chemical Agent Attacks (RAS BICHAT) is a system for information exchange on health threats from deliberate release of CBRN agents. (http://ec.europa.eu/health/ph_threats/com/preparedness/rapid_alert_en.htm)
- Rapid Alert System for Food and Feed (RASFF) facilitates information exchange on measures taken to ensure food safety. (http://ec.europa.eu/food/food/rapidalert/index_en.htm)
- Animal Disease Notification System (ADNS) provides detailed information on infectious disease outbreaks in animals in Member States. (http://ec.europa.eu/food/animal/diseases/adns/index_en.htm)
- European Food Safety Authority (EFSA) provides risk assessment advice on existing and emerging risks in food and feed safety. (http://www.efsa.europa.eu/EFSA/efsa_locale-1178620753812_home.htm).

### 2.11 HealthMap

HealthMap is a fully automated resource that collects information from 14 sources (representing about 20,000 web sites) including Google News, ProMED, WHO, and others (http://www.healthmap.org/about.php). It was created as a unified and comprehensive resource for information on infectious disease and public health events in humans, animals, and plants and is freely available with sources and user interface in English, Chinese, Spanish, Russian, and French. Data are aggregated by disease and displayed by location with a link to the original text. HealthMap processes approximately 300 alerts per day and has documented 141 unique infectious disease categories from 174 countries. The HealthMap web site has approximately 1000–10,000 visitors per day with about 200,000 visitors since its launch [18].

### 2.12 *Institute de Veille Sanitaire*

Among a number of other responsibilities, the French Institute for Public Health Surveillance, *Institute de Veille Sanitaire* (INVS) provides surveillance and alerts of infectious diseases (http://www.invs.sante.fr/presentations/presentation_anglais.htm). The INVS collaborates with other national networks and international organizations. It is part of the EWRS that links health ministries and surveillance organizations in EU Member States. Sources include WHO, ProMED, GPHIN, and OIE. Posting only verified news events, it has approximately 1400 subscribers.

### 2.13 Medical Information System

The EC's Medical Information System (MedISys) (http://medusa.jrc.it/medisys/aboutMediSys.html) is a fully automated 24/7 public health surveillance system run and maintained by the Joint Research Center (JRC) at the Institute for the Protection and Security of the Citizen (IPSC), in Ispra, Italy [19]. The developer team collaborates with the Health Threats Unit at the Directorate General for Health and Consumer Protection (DG SANCO) and University of Helsinki (PULS system).

MedISys covers infectious human and animal diseases, bioterrorism, chemical, biological, and CBRN threats reported in open source news media. Approximately 80,000 to 90,000 articles from 5000 news sites in 45 languages are screened. Currently, 26 languages are available via the Web portal, but news in 45 languages is processed in

predefined categories. MedISys started operating in August 2004 and is one of the several JRC-developed media monitoring applications that process news gathered by the Europe Media Monitor (EMM, on-line since 2002). MedISys provides daily automated e-mail alerts to subscribers and offers users a tool called *Rapid News Service* (RNS) to manage newsletters, e-mail distribution lists, and alerts via e-mail and/or mobile phone messages.

### 2.14 World Organization for Animal Health

Created in 1924, the Organization for Animal Health (OIE) is an intergovernmental organization with 172 member countries and territories and charged with improving animal health worldwide (http://www.oie.int/eng/en_index.htm). It maintains permanent relationships with other international and regional organizations. The World Animal Health Information Database (http://www.oie.int/wahis/public.php?page=home) provides access to OIE's World Animal Health Information System (WAHIS) data. The reports include immediate notifications and follow-up reports from Member States, country biannual reports on OIE-listed diseases, and annual reports on animal health, laboratory, and vaccine production. The OIE is a participating partner in WHO's Global Warning system for Major Animal Diseases, including Zoonoses (GLEWS) for early warning and responses to animal diseases.

### 2.15 Pattern-based Understanding and Learning System

Pattern-based Understanding and Learning System (PULS) is an information system at the University of Helsinki (http://puls.cs.helsinki.fi/medical/) that in partnership with the EC's JRC extracts metadata from MedISys articles [19, 20]. It is a fully automated global biosurveillance system designed to provide early warning of infectious and noninfectious disease outbreaks and its coverage will soon be extended to CBRN. Its focus is information retrieval, extraction, aggregation, and visualization, and it uses text mining and natural language processing to analyze incoming documents. Key attributes determined from text include disease/condition (if known), location, date, number of victims, whether human or animal, and victim survival.

### 2.16 Program for Monitoring Emerging Diseases

Program for Monitoring Emerging Diseases (ProMED)-mail (http://www.promedmail.org) was established in 1994 and currently operates as a program of the International Society for Infectious Diseases with contributing corporate, foundation, and individual donor support [21, 22]. With the goal of promoting rapid communication within the international infectious disease community, it is an Internet-based reporting system for disease outbreaks and toxin exposures affecting humans, animals, and plants. Sources include local observers, media and official reports, and others. In a nonautomated process, reporting is screened and comments provided by subject-matter experts prior to posting to subscribers of which there are over 50,000 in 188 countries. ProMED-mail sends an average of 7–10 reports per day and is available in English, Spanish, Portuguese, French, and Russian languages. ProMED-mail has five regional programs with a staff in 15 countries.

### 2.17 Real-time Outbreak and Disease Surveillance

As its name implies, Real-time Outbreak and Disease Surveillance (RODS) was created to investigate methods to detect disease outbreaks in real-time (https://www.rods.pitt.edu/site/index.php?option=com_content&task=view&id=14&Itemid=77). With support from US federal agencies and the State of Pennsylvania, its public health bioinformatics research includes outbreak detection algorithms, free-text classification, systems design, system evaluation, policy analysis, and outbreak simulation. RODS software has been made available to academia and health departments, and RODS operates the National Retail Data Monitor for information on sale of over-the-counter healthcare products [23]. RODS is currently in use in many cities, states, and countries and has served as a partner in the Department of Homeland Security's BioWatch program.

### 2.18 National Association of Radio-Distress Signaling and Infocommunications Emergency and Disaster Information Service (RSOE-EDIS)

Based in Hungary, the Havaria Information Service (http://www.oasis-open.org/events/ITU-T-OASISWorkshop2006/slides/rafael.pdf) was established to monitor catastrophic events in Hungary, Europe, and the world and to forward information to stakeholders via e-mail alerts and RSS feeds (http://visz.rsoe.hu/alertmap/index.php?lang=). The service collects information from approximately 600 Internet portals among which are numbered inputs from EISS for European influenza status, WHO, and the US CDC for global epidemic events.

### 2.19 World Health Organization

WHO has put into place or provides administrative assistance to a number of resources which contribute to the detection of disease outbreaks and the response thereto (http://www.who.int/en/).

- Epidemic and Pandemic Alert and Response (EPR, http://www.who.int/csr/en/). In addition to other services and capabilities, EPR provides Member States epidemic intelligence in the form of event verification, alerting, and coordinated outbreak responses within the framework of the International Health Regulations (2005). EPR seeks to ensure appropriate communications among stakeholders.
- Global Outbreak Alert and Response Network (GOARN) (http://www.who.int/csr/outbreaknetwork/en/). WHO provides administrative assistance and an organizational umbrella for GOARN although GOARN is not a formal component of WHO. GOARN is an association whose members and networks are brought together to assist in and enable early detection, identification, confirmation, and response to disease events with international implications.

## 3 ANALYSIS OF SYSTEMS

Public health markers providing indications and warning (I&W) of new and emerging infectious disease events can be conveniently segregated into direct and indirect components [24]. The I&W paradigm provides a useful framework for interpreting the landscape of international biosurveillance defined by the systems described above. For the purpose of this article, the following classifications of I&W types are used as follows:

- *Direct indicators* are those commonly used in traditional disease reporting and include data derived from public health, clinical, and laboratory sources. Examples of direct indicators are reports of unknown human disease (i.e. syndromes and diseases of unknown etiology), geographical features (i.e. extent of affected area such as city, region, nation, etc.), noncontiguous geographic involvement, unique or unexpected clinical presentation, high morbidity/mortality, unexpected appearance of disease in relation to season, discrete population(s) involved (e.g. specific ethnic group, nosocomial [hospital] setting, healthcare workers, patients contracting unusual disease while in a medical facility, specific age groups, and specific occupations). While some specific features of direct indicators of animal disease may be different, their pattern is similar to those of human disease [24].
- *Indirect indicators* include human responses to infectious disease outbreaks that are expressed as social behavior. Other indirect indicators include environmental and climate/meteorological trends such as temperature and precipitation variations. Social behavior deviating from the norm in a particular group or society [24] include such items as (i) public health response including preparedness, implementation of countermeasures, activation of biosurveillance or screening, and demand for medical services; (ii) other government reaction such as official acknowledgment or denial of the bioevent, official action, information suppression, or criminal prosecution; (iii) business/organizational changes including business practice changes and integrity of infrastructure; and (iv) other social behavior such as local perception of threat.

While extensive details regarding specific ontologies and taxonomies are not publically available for all the systems described above, it is possible to think of them within an I&W paradigm. When that is done for examples of direct and indirect indicators described in the preceding paragraph, some interesting features emerge that are illustrated in Figures 1–3.

As shown in Figure 1, all systems monitor and report on direct I&W of disease. Fewer systems utilize indirect I&W markers, and those include Argus, GPHIN, HealthMap, ProMED, RODS, and RSOE.

Figure 2 illustrates the results when direct I&W elements are broken down into specific categories. Not surprisingly, all the systems utilize public health information and 11 of the 19 systems collect clinical and laboratory information as well. While the direct I&W categories in Figure 2 are not inclusive of all that might be considered, they serve to both: (i) illustrate the diversity of the systems and (ii) suggest areas for capitalizing on system complementarities.

Figure 3 suggests that coverage of indirect indicators is much less complete than coverage of direct indicators. As might be expected, "Public Health Response" is the most frequently used indirect I&W followed by "Meteorological Data." Although the potential value of enviroclimatic indicators is yet to be demonstrated for a large class of diseases, compelling evidence for the role climate issues play for particular diseases can be found in the literature [25–27].

The lack of coverage of any particular direct or indirect I&W marker in any given system should not be considered a criticism or fatal system flaw, but rather as an opportunity to exploit complementarities between systems. It can also be argued that, since no system is perfect, some redundancy can be a positive attribute. The systems described above were designed to serve varying missions and stakeholder populations, and therefore, no one

| System | Direct I & W | Indirect I & W |
|---|---|---|
| APHIS | ■ | |
| Argus | ■ | ■ |
| BioCaster | ■ | |
| CDC | ■ | |
| EMPRES-i | ■ | |
| ECDC | ■ | |
| EISS | ■ | |
| GEIS | ■ | |
| GPHIN | ■ | ■ |
| HealthMap | ■ | ■ |
| HEDIS | ■ | |
| INVS | ■ | |
| MedISys | ■ | |
| OIE | ■ | |
| PULS | ■ | |
| ProMED | ■ | ■ |
| RODS | ■ | ■ |
| RSOE | ■ | ■ |
| WHO | ■ | |

**FIGURE 1** Summary of system usage of direct and indirect I&W markers.

| | Direct I & W | | | |
|---|---|---|---|---|
| Systems | Public Health | Clinical | Lab | Vet Records |
| APHIS | ■ | ■ | ■ | ■ |
| Argus | ■ | | | |
| BioCaster/GHM | ■ | | | |
| CDC | ■ | ■ | ■ | |
| EMPRES-i | ■ | ■ | ■ | ■ |
| ECDC | ■ | ■ | ■ | |
| EISS | ■ | ■ | ■ | |
| GEIS | ■ | ■ | ■ | |
| GPHIN | ■ | | | |
| HealthMap | ■ | ■ | ■ | |
| HEDIS | ■ | | | |
| INVS | ■ | ■ | ■ | |
| MedISys | ■ | | | |
| OIE | ■ | ■ | ■ | ■ |
| PULS | ■ | | | |
| ProMED | ■ | ■ | ■ | ■ |
| RODS | ■ | | | |
| RSOE | ■ | | | |
| WHO | ■ | ■ | ■ | |

**FIGURE 2** System usage of direct I&W subdivided by category. "Public Health" denotes data reported to public health authorities (e.g. notifiable diseases and conditions), "Clinical" denotes acute or long-term healthcare facility data (e.g. clinical lab tests and information recorded in patient data records), "Lab" denotes public health laboratory surveillance records, practices and standards (e.g. the Laboratory Response System in the United States), and "Vet" denotes veterinary records.

| | Indirect I&W | | | | |
|---|---|---|---|---|---|
| Systems | Public Health Response | Other Government Reaction | Business/Organization Changes | Other Social Behavior | Meteorological Data |
| APHIS | | | | | |
| Argus | | | | | |
| BioCaster/GHM | | | | | |
| CDC | | | | | |
| EMPRES-i | | | | | |
| ECDC | | | | | |
| EISS | | | | | |
| GEIS | | | | | |
| GPHIN | | | | | |
| HealthMap | | | | | |
| HEDIS | | | | | |
| INVS | | | | | |
| MedISys | | | | | |
| OIE | | | | | |
| PULS | | | | | |
| ProMED | | | | | |
| RODS | | | | | |
| RSOE | | | | | |
| WHO | | | | | |

**FIGURE 3** System usage of indirect I&W subdivided by category. "Public Health Response" is action by health officials to contain a disease event (e.g. health alerts and quarantine), "Other Government Reaction" denotes an official action in response to a disease event (e.g. implementation of countermeasures and official investigations), "Business/Organization Changes" refers to changes in normal business or organization practices (e.g. profiteering, business closure and black market formation), "Other Social Behavior" denotes societal anxiety or panic (e.g. fleeing and stockpiling of commodities), "Meteorological Data" refers to enviroclimatic, satellite and vegetation, and other data that could be used to identify favorable conditions for a biological event (e.g. flooding, abnormal temperature, and water contamination).

system can or should be expected to deliver insight into all possible variables associated with effective biosurveillance, especially, on a global scale where the need is greatest.

## 4 RESEARCH AND DEVELOPMENT NEEDS

A dynamic approach to risk assessment and public health reaction remains difficult given current limitations in both early warning and real-time situational awareness of emerging biological events. If the paradigm of graded public health response is to be viable, a capability must exist to detect evidence of outbreak activity at the earliest stages and monitor them accurately and precisely as they progress. Such a capability would likely be a "systems of systems," composed of discrete and complementary components acting in concert. Included in any such system would be a component that provides I&W of potential events. This I&W component would provide the first cueing and alerting of a potential disease event (or, potentially, risk of a future event). It is expected that with time after the event, additional information provided by other components in the graded alerting and response chain will refine and better characterize the event. The systems listed in this study (and potentially others not included here) likely provide the basic ingredients for such a system of systems.

Important technological and methodological challenges remain in constructing a system providing comprehensive, dynamic situational awareness [28]. For both individual systems as well as systems of systems, some of the more prominent challenges facing surveillance systems include interoperability, interface customizability, scalability, and event traceability. Integration of geospatial visualization, event mapping, modeling, and

trending tools are important for establishing metrics and baselines necessary for data interpretation and analysis. Additionally, expansion of the current biosurveillance capabilities via incorporation of emerging media such as video, digital audio, images, blogs, Short Message Service (SMS), and others is critical.

### 4.1 Source Assessment

The value of various data sources must be defined. There are a massive number of sources on the Web (e.g. news media text, images, audio, and video; blogs; social networking sites; traditional public health; syndromic [29, 30], and laboratory surveillance [31]). Each source type will likely have associated with it varying degrees of confidence and geographic coverage, and at some point the value of each component in biosurveillance systems must be assessed. Quantifying variation in source reporting standards as well as catchment (i.e. the regions from which a source collects) and target population will be a critical first step toward understanding how these issues affect the validity of biosurveillance system output. Metrics must be defined, and these metrics need to be generalized to individual systems that may use different data and take a variety of analytical approaches.

### 4.2 Standards Development

Approaches to integrating complementary systems must be investigated. Since the biosurveillance systems described in this study were created to address specific issues and utilize different methods and standards, integration of these systems will be challenging. No standards for collecting, processing, and exploiting biosurveillance products exist that can be applied across the spectrum of systems described here. Such standards, once agreed upon and implemented, would facilitate communication between international and domestic systems alike.

### 4.3 System Metrics

Techniques for evaluating system performance must be developed. It is unclear how to evaluate the impact of biosurveillance on spatiotemporal detection and monitoring (i.e. situational awareness) of infectious disease outbreaks. In addition, standardized metrics quantifying the performance of different biosurveillance systems are needed to understand how different systems complement and add value to one another. Such metrics are also needed if end users are able to understand the performance of a given system, let alone any aggregation of systems.

### 4.4 System Communication

Efficient and meaningful ways of communicating system outputs and findings must be identified. Current systems display and present the results of biosurveillance differently. How to present best results to the broader user community, which includes researchers as well as public health workers and decision makers, is an issue that will have to be addressed. Many unknowns remain including identifying the most appropriate interactive visual interfaces; best practices regarding techniques for visually synthesizing biosurveillance data; and how to present dynamic, ambiguous, and potentially conflicting information to consumers of biosurveillance. Can a biologically common operating system be developed that effectively addresses the needs of different users?

There are nearly 200 countries in the world. Although much effort has been devoted to the automated acquisition of massive amounts of relevant information (e.g. from the Internet), global biosurveillance must sooner or later have the ability to capture and analyze information in many languages. In the future, the most informative and useful systems will likely have access to an analyst cadre collectively fluent in many languages and cultures.

## 5 ASSESSMENT OF THE CURRENT GLOBAL BIOSURVEILLANCE LANDSCAPE

That rapid reporting of disease outbreaks is vital for both the public health and national security communities is not disputed. It is also clear that this can only be accomplished with an effective, integrated global biosurveillance capability with a near–realtime reporting component. While such a capability does not yet exist, similarities and differences among systems such as those described in this work suggest that exploiting system complementarities could provide a very powerful global biosurveillance resource.

In 2003, Woodall and Aldis reported "enormous gaps in terms of geographical and disease coverage and timeliness of reporting" and concluded that open source on-line reporting with an emphasis on speed would likely heavily use the Internet [32]. More recently, Morse [33] reviewed the gaps that hindered progress to global biosurveillance, and those gaps included among others, political will, resources for reporting, and improved coordination and sharing information; he also noted that increased availability of communications and information technologies offered new opportunities for reporting. These observations are certainly consistent with the analysis of the biosurveillance systems presented in Section 2 above and with the recent results of studies using Internet search engines to track influenza [34–36].

With the appropriate communication and data sharing regimes, there do not appear to be technical barriers to integrating existing global and regional biosurveillance systems, biosurveillance systems dedicated to single diseases, and open source reporting into an effective global biosurveillance capability. Even a cursory examination of the systems presented here shows a tremendous reservoir of creative thought and achievement that, if policy and political barriers were to be eliminated, could be the foundation of global biosurveillance in the not too distant future. Although, each of the individual systems examined here have different missions and approaches, most complement the others. There is no obvious reason why a hierarchal system of systems could not be assembled with currently existing biosurveillance systems. This would require enlightened leadership and the will to cooperate, not new technology. Although much remains to be done that will require dedication of the appropriate financial and intellectual resources, there is a solid foundation upon which to build.

## ACKNOWLEDGMENTS

The authors thank system owners Drs John Brownstein (HealthMap), Nigel Collier (Biocaster), Jens Linge (MedISys), Larry Madoff (ProMed-mail), Abla Mawudeku (GPHIN), Germain Thinus (HEDIS), and Roman Yangarber (PULS) for their gracious review and helpful comments during preparation of this manuscript. CDC's Dr Ray Arthur provided valuable insights and comments on this manuscript.

## REFERENCES


1. World Health Organization. (2007). *International Health Regulations (2005)*. http://www.who.int/mediacentre/news/releases/2007/pr31/en/index.html.
2. Institute of Medicine. (2003). *Microbial Threats to Health: Emergence, Detection, and Response*. National Academy Press, Washington, DC.
3. Koch, D. E., Mohler, R. L., and Goodin, D. G. (2007). Stratifying land use/land cover for spatial analysis of disease ecology and risk: an example using object-based classification techniques. *Geospat Health* **2**(1), 15–28.
4. Beck, L. R., Lobitz, B. M., and Wood, B. L. (2000). Remote sensing and human health: new sensors and new opportunities. *Emerg. Infect. Dis.* **6**, 217–227.
5. Gage, K. L., Burkot, T. R., Eisen, R. J., and Hayes, E. B. (2008). Climate and vectorborne diseases. *Am. J. Prev. Med.* **35**, 436–450.
6. Linthicum, K. J., Anyamba, A., Tucker, C. J., Kelley, P. W., Myers, M. F., and Peters, C. J. (1999). Climate and satellite indicators to forecast Rift Valley fever epidemics in Kenya. *Science* **285**, 397–400.
7. Cazelles, B., and Hales, S. (2006). Infectious diseases, climate influences, and nonstationarity. *PLoS Med.* **3**, e328. DOI: 10.1371.
8. Barrett, R., and Brown, P. J. (2008). Stigma in the time of influenza: social and institutional responses to pandemic emergencies. *J. Infect. Dis.* **197**, S34–S37.
9. McGrath, J. W. (1991). Biological impact of social disruption resulting from epidemic disease. *Am. J. Phys. Anthrop.* **84**, 407–419.
10. Lombardo, J., Burkom, H., Elbert, E., Magruder, S., Lewis, S. H., Loschen, W., Sari, J., Sniegoski, C., Wojcik, R., and Pavlin, J. (2003). A systems overview of the electronic surveillance system for the early notification of community-based epidemics (ESSENCE II). *J. Urban Health.* **80**, i32–i42.
11. National Academy Press (2007). *Institute of Medicine Infectious Disease Surveillance and Detection: Assessing the Challenges—Finding Solutions*. National Academy Press, Washington, DC.
12. Wilson, J. M., Parker, M. F., Hartley, D. M., McEntee, T., Tilton, E. L., and Cardwell, K. (2004). Proceedings integrated research team workshop on the role of indications and warnings for prediction and surveillance of catastrophic biological events. *U.S. Army Medical Research and Materiel Command*, Fort Detrick, Maryland, pp. 9–10.
13. Fitch, J. P., Raber, E., and Imbro, D. R. (2003). Technology challenges in responding to biological or chemical attacks in the civilian sector. *Science* **302**, 1350–1354.
14. Collier, N., Doan, S., Kawazoe, A., Goodwin, R. M., Conway, M., Tateno, Y., Ngo, Q. H., Dien, D., Kawtrakul, A., Takeuchi, K., Shigematsu, M., and Taniguchi, K. (2008). Biocaster: detecting public health rumors with a Web-based text mining system. *Bioinformatics*, Oxford: Oxford University Press, DOI: 10.1093/bioinformatics/btn534.
15. Collier, N., Kawazoe, A., Lihua, J., Shigematsu, M., Dien, D., Barrero, R., Takeuchi, K., and Kawtrakul, A. (2007). A multilingual ontology for infectious disease outbreak surveillance: rationale, design, and challenges. *J. Lang. Resour. Eval.* **40**, 405–413.
16. Doan, S., Hung-Ngo, Q., Kawazoe, A., and Collier, N. (2008). Global Health Monitor-a web-based system for detecting and mapping infectious diseases. *Proceedings of the 3rd International Joint Conference on Natural Language Processing (IJCNLP)*, Companion Volume, pp. 951–956.
17. Blench, M. (2008). Global public health intelligence network (GPHIN). *Eighth Conference of the Associatin for Machine Translation in the Americas*, USA, pp. 299–303.

18. Brownstein, J. S., Freifeld, C. C., Reis, B. Y., and Mandl, K. D. (2008). Surveillance Sans Frontieres: internet-based emerging infectious disease intelligence and the HealthMap Project. *PLoS Med.* **5**(7), e151. DOI: 10.1371/journal.pmed.0050151, 1019–1024.
19. Steinberger, R., Fuart, F., van der Goot, E., Best, C., von Etter, P., and Yangarber, R. (2008). Text mining from the web for medical intelligence. In *Mining Massive Data Sets for Security*, F. Fogelman-Soulie, D. Perrotta, J. Piskorski, and R. Steinberger, Eds. IOS Press, Amsterdam, The Netherlands, pp. 295–310.
20. Yangarber, R., von Etter, P., and Steinberger, R. (2008). Content collection and analysis in the domain of epidemiology. *Proceedings of First International Workshop on Describing Medical Web Resources: the 21st International Congress of the European Federation for Medical Informatics*, Göteborg, Sweden.
21. Madoff, L. C. (2004). ProMED-mail: an early warning system for emerging diseases, Clin. *Infect. Dis.* **39**, 227–232.
22. Madoff, L. C., and Woodall, J. P. (2005). The internet and global monitoring of emerging diseases: lessons from the first 10 years of ProMED-mail. *Arch. Med. Res.* **36**, 724–730.
23. Espino, J. U., Wagner, M. M., Tsui, F. C., Su, H. D., Olszewski, R. T., Lie, Z., Chapman, W., Zeng, X., Ma, L., Lu, Z. W., and Dara, J. (2004). The RODS open source project: removing a barrier to syndromic surveillance. *Stud. Health Technol. Inform.* **107**, 1192–1196.
24. Wilson, J. M., Polyak, M. G., Blake, J. W., and Collmann, J. (2008). A heuristic indication and warning staging model for detection and assessment of biological events. *J. Am. Med. Inform. Assoc.* **15**, 158–171.
25. Pavlovsky, E. N. (1966). *Natural Nidality of Transmissible Disease*. N. D. Levine, translated by F. K. Plous, Ed., University of Illinois Press, Urbana and London.
26. Vora, N. (2008). Impact of anthropogenic environmental alterations on vector-borne diseases. *Medscape J. Med.* **10**(10), 238.
27. Peterson, A. T. (2008). Biogeography of diseases: a framework for analysis. *Naturwissenschaften* **95**, 483–491.
28. Brownstein J. S., Freifeld, C. C., and Reis, B. Y. (2007). HealthMap: internet-based emerging infectious disease intelligence. In *Global Infectious Disease Surveillance and Detection: Assessing the Challenges-Finding Solutions. Forum on Microbial Threats*, S. M. Lemon, M. A. Hamburg, F. Sparling, E. R. Choffnes, and A. Mack, Eds. Rapporteurs. The National Academy Press, http://www.nap.edu/catalog/11996.html, pp. 122–135.
29. Buehler, J. W., Berkelman, R. L., Hartley, D. M., and Peters, C. J. (2003). Syndromic surveillance and bioterrorism-related epidemics. *Emerg. Infect. Dis.* **9**, 1197–1204.
30. Buehler, J. W., Sonricker, A., Paladini, M., Soper, P., and Mostashari, F. (2008). Syndromic surveillance practice in the United States: findings from a survey of state, territorial, and selected local health departments. *Adv. Dis. Surveill.* **6**, 1–20.
31. Cantón, R. (2005). Role of the microbiology laboratory in infectious disease surveillance, alert and response. *Clin. Microbiol. Infect.* **11**(Suppl 1), 3–8.
32. Woodall, J., and Aldis, R. (2003). *Gaps in Global Surveillance*. Bioweapons Prevention Project Occasional Paper, 1, pp. 1–15.
33. Morse, S. S. (2007). Global infectious disease surveillance and health intelligence. *Health Affairs* **26**, 1069–1077.
34. Eysenbach, G. (2006). Infodemiology: tracking flu-related searches on the web for syndromic surveillance. *Am. Med. Inform. Assoc.* 2006 Proceedings, 244–248.
35. Polgreen, P. M., Chen, Y., Pennock, D. M., and Nelson, F. D. (2008). *Clin. Infect. Dis.* **47**, 1443–1448.
36. Hulth, A., Rydevik, G., and Linde, A. (2009). Web queries as a source for syndromic surveillance. *PLoS ONE* **4**(2), e4378.

## FURTHER READING

Beatty, A., Scott K., and Tsai, P. (2008). *Rapporteurs, Achieving Sustainable Global Capacity for Surveillance and Response to Emerging Diseases of Zoonotic Origin*. The National Academy Press. http://books.nap.edu./catalog.php?record_id=12522#toc.

Bravata, D. M., McDonald, K. M., Smith, W. M., Rydzak, C., Szeto, H., Buckeridge, D. L., Haberland, C., and Owens, D. K. (2004). Systemic review: surveillance systems for early detection of bioterrorism-related diseases, *Ann. Intern. Med.* **140**, 911–922.

Buehler, J. W., Hopkins, R. S., Overhage, J. M., Sosin, D. M., and Tong, V. (2004). Framework for evaluating public health surveillance systems for early detection of outbreaks. *Morb. Mortal. Wkly. Rep.* **53**(RR05), 1–11. http://www.cdc.gov/mmwr/preview/mmwrhtml/rr5305a1.htm.

Hitchcock, P., Chamberlain, A., Van Wagoner, M., Inglesby, T. V., and O'Toole, T. (2007). Challenges to global surveillance and response to infectious disease outbreaks of international importance. *Biosecur. Bioterror.: Biodefense Strategy, Pract. Sci.* **5**, 206–227.

Ostfield, M. L. (2008). Strengthening biodefense internationally: illusion and reality. *Biosecur. Bioterror.: Biodefense Strategy, Pract. Sci.* **6**, 261–267.

Wagner, M. M., Moore, A. W., and Aryet, R. M. editors. (2006). *Handbook of Biosurveillance*. Elsevier Academic Press, London.

# BIOSURVEILLANCE TRADECRAFT

JAMES M. WILSON AND CRAIG KIEBLER

*Georgetown University Medical Center, Argus Research Operations Center, Imaging Science and Information Systems Center, Washington, D.C.*

RONALD A. WALTERS

*Pacific Northwest National Laboratory, Richland, Washington, D.C.*

JOHN DAVIES-COLE

*Center for Policy, Planning and Epidemiology, DC Department of Health, Washington, D.C.*

## 1 INTRODUCTION

The term "biosurveillance" is not currently associated with a universally accepted definition [1]. For the purposes of this article, we consider the definition of biosurveillance to be the detection and tracking of biological events that represent a deviation of what is considered normal endemic baseline. A "biological event" refers to disease events affecting humans, animals, and/or plants; here we focus primarily on biological events

affecting humans or animals. The prospect of rapid detection of socially disruptive biological events that are triggered through natural, accidental, or intentional mechanisms is of interest not only to the public health community but to the agricultural, law enforcement, intelligence, and homeland security communities as well.

From a public health perspective, biosurveillance must embrace grounded public health surveillance methodology as well as near-real-time situational awareness (i.e. event detection). The public health community has traditionally focused on health-related information such as patient care, disease reporting, and diagnostic information. This represents but a small portion of the necessary data potentially useful to detect and track an evolving biological event [1].

## 2 EMERGENCE OF THE BIOSURVEILLANCE TRADECRAFT

At the time of writing this manuscript, there did not exist a formalized professional discipline in operational biosurveillance with rigorous research, education, and training support. Biosurveillance requires a synthesis of analytic approaches derived from the natural disaster, intelligence, public health, epidemiological, medical, veterinary, agricultural, meteorological, anthropological, and sociological communities, among others. Functional modes of biosurveillance analysis span the tactical, strategic, and forensic domains.

The tradecraft of biosurveillance follows similar tenets of the intelligence cycle, which is a useful construct to codify operations. Figure 1 displays an overview of the biosurveillance cycle.

Data collection is driven by a comprehensive targeting analysis, which stems from a mission analysis (see below). Targeting enables identification of the key required information elements and what sources can provide such information in a timely and credible manner. Analysis of the information is driven by mission objectives (see below).

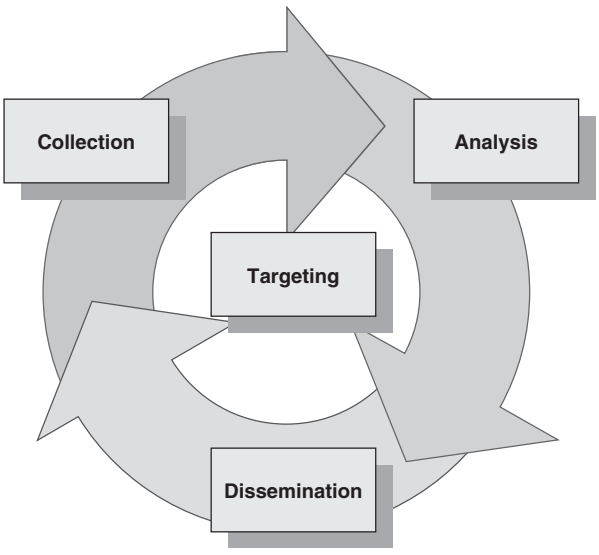



**FIGURE 1** The biosurveillance cycle.

Dissemination is an important step; control of information flow can be as much an asset to an operations team performing biosurveillance as well as a detriment if information is not controlled appropriately. Feedback provided from customers of the information enables refinement of the overall process through never-ending targeting analysis. Targeting is a perpetual component of operational biosurveillance that ensures improvement.

## 3 MISSION ANALYSIS

An operational biosurveillance organization, especially if it is to function in the tactical environment, must exist as a highly disciplined entity. The creation of such an organization begins with a mission analysis, which comprises a mission statement, critical information requirements (CIRs), targeting analysis, and operations plan that eventually evolves into standard operating procedures (SOPs). It is the operations plan that codifies the process of data collection, analysis, and information dissemination.

The mission statement is an important first step. It defines the customer(s), the product outputs and operational objective, and implies the eventual CIRs and primary operational tempo (tactical, strategic, and forensic). An example of a mission statement might be the following:

> The ACME Biosurveillance Organization provides decision makers early recognition of biological events of potential local and regional significance, to include natural disease outbreaks, accidental, or intentional use of biological agents, and emergent biohazards through the acquisition, integration, analysis, and dissemination of information from existing human disease, food, water, meteorological, and environmental surveillance systems and relevant threat information.

The CIRs are typically a list of 5–10 (preferably five) statements that define the key items the customer is primarily concerned about. An example of a CIR is *any credible evidence of an act of intentional biological agent release*.

Targeting analysis refers to defining the data collection requirements and implied social networks and information providers needed to obtain the data. For national, state, and local considerations, reporting requirements are legally mandated for specific diseases such as plague. These requirements have not traditionally included indication and warning (I&W) reporting, which are additional important considerations. I&Ws fall into two categories: direct and indirect. Direct indications refer to explicit local reporting of disease in humans, animals, or plants that may describe epidemiological features of the event [2]. Here, it is important to monitor with a species-agnostic approach. Species tropism exhibited by diseases may give important initial clues as to the diagnosis. For example, prairie dog illness in Colorado is an important indicator of the possible presence (and imminent threat to human health) of plague. Indirect indicators are further subdivided into additional categories such as official acknowledgement, official action, local perception of threat, business practice changes, and integrity of infrastructure. The indicators within these categories are numerous and beyond the scope of this article, however, they enable approximation, over time, of social functioning in the context of a biological event. The key objective in the use of indirect indicators is to provide an assessment of containment status and concurrent level of social disruption [2]. When considered as a whole, these reporting requirements enable operational monitoring of an entire society as though it were a patient in a hospital bed.

Once a combined disease-specific and I&W reporting requirement table has been established, the next step involves prioritization. For example, a report of diarrhea in a day care center may take lower precedence than reports of the primary trauma care hospital for the city reporting a sudden inundation of its infrastructure with an unidentified influenza-like illness. Such prioritization will naturally lead to categorization of reporting requirements into classes that are easily understood by the user community, such as "warning", "watch", and "advisory". Note, this prioritization is dependent upon, and partly defined by the user community, whether for internal monitoring purposes or to provide reporting to the health care community or the general public. Examples of this process are highlighted in Table 1.

Once prioritized reporting requirements have been established, an examination of social networking is required that attempts to cross-match the requirements to data and information sources; the product of this analysis is referred to as a *targeting matrix*. For example, if a key direct indicator is *reports of disease in rodents*, then one may need to consider building a network of reporting that includes the local sanitation authority. If a key indirect indicator is *local depletion of ventilator supplies*, then one may need to build a relationship with the local distributor of ventilators as well as medical facilities that use ventilators.

Prioritized reporting requirements drive the operations tempo, where "warning" implies a tactical, near-real-time reaction by the analyst versus an "advisory" that may be monitored over the course of a week. In other words, this categorization is an easy way to impart the severity and importance of the report to the user community.

The operations plan draws together all of these components into a document that precisely defines how the mission will be executed, from mission statement to CIRs, prioritized reporting requirements, operation tempo modes, communication channels that

**TABLE 1 Example of Prioritized Reporting Requirements**

| Events | Warning | Watch | Advisory |
|---|---|---|---|
| Any indication of intentional use of any biological agent or a biowarfare attack | X | | |
| Any indication of public health system failure or social collapse associated with a biological event involving humans or animals | X | | |
| A biological event associated with illness of health care, veterinary, or laboratory workers | X | | |
| Public panic documented by local media in context with an active biological event (includes mass evacuations and conflict with officials) | X | | |
| Any incident of unexplained illness requiring additional response or assistance, especially of health care, veterinary, or laboratory workers | | X | |
| Any acute cluster (>3) of unexplained illness in humans | | X | |
| Any acute cluster (>10) of unexplained illness in animals | | X | |
| Vaccine accident triggering a biological event | | | X |
| Any increased demand for ventilator or intensive care unit support | | | X |
| Vaccine or therapeutic failure or compromise | | | X |

include the social network of reporting, and so on. While the document itself eventually becomes a desk reference for the biosurveillance analyst, it is a living document that is modified to reflect changes in operational requirements and refinements in the analytic process.

## 4 BIOLOGICAL EVENT EVOLUTION

Investigators have attempted to define event evolution as a function of media reporting. Cieri and colleagues [3] proposed that an event be defined as "a specific thing that happens at a specific time and place along with all necessary preconditions and unavoidable consequences" [3]. Makkonen [4] observed that a seminal event can lead to various related events and outcomes, and the initial cause of these events may become less obvious over time [4]. Chen and colleagues proposed that a media-reported event can be considered "a life form with stages of birth, growth, decay, and death"; maintenance of the reported event is dependent on sensationalism [5]. We propose that biological events are reported through various data inputs as increasingly complex phenomena over time, whose "nourishment" is dependent on whether the biological agent in question continues to transmit above what is locally considered baseline disease [2].

For example, in 2002, the emergence of severe acute respiratory syndrome (SARS) in the People's Republic of China (PRC) appeared to be largely unnoticed by the international community. I&Ws of "unseasonal bad flu" appeared in September in local Chinese vernacular media. Diagnosis of the pathogen in question would not have been apparent beyond "bad flu"; however, "unseasonal" indicated a local awareness of a potential departure from local baseline disease. In October, social anxiety was reported. By November, official concern was expressed regarding potential public panic. In December, an abrupt decrease in reporting, indicating possible information suppression, was a key indicator of a change in local awareness of this novel threat. In January, reports of supply depletions and mobilization of resources appeared, indicating severe shifts in supply and demand. By April, reports documented martial law and rioting due to SARS-related social disruption. This event likely was a complex event involving a variety of respiratory pathogens; to date, there remains uncertainty as to precisely when SARS emerged within this context. In any case, reports of "unseasonal bad flu" in September and, more important, of social anxiety in October would have been key to the analyst's assessment of whether unusual disease was present. The overall pattern was one of recurrence, elevation, and diversification of the I&Ws of a biological event declared unusual followed by reports of containment loss [6].

As recent history has shown, SARS was not recognized to be a transnational threat until it had translocated through the air traffic grid to eight countries including the United States. The challenge revolved around near-real-time access to transparent disease reporting, understanding of what were indications of social disruption due to containment loss, and effective analysis to determine the nature of what ultimately constituted a true transnational issue [6].

The 1995 epidemic of Venezuelan equine encephalitis (VEE) in Venezuela and Colombia presented a complex picture of flood-induced infrastructure collapse; the presence of a disease affecting horses and humans (i.e. VEE), and possibly the presence of other diseases as well, such as dengue fever. In March and April 1995, flooding was reported in local vernacular Venezuelan media. In April, equine health evaluations were reported,

but there was no explicit declaration of an outbreak of disease. By June, enough information was available to note the presence of a multifocal biological event in equines, co-occurring with at least a unifocal event in humans. In July, infrastructure strain was reportedly related to equine disease (e.g. depletion of local vaccine supplies), along with indications of a multifocal human disease also present. In August, strain on the medical infrastructure was reported (e.g. hospitals overrun with infected individuals), followed by signs of social collapse in September. Flooding was a key factor promoting the vigorous progression of this epidemic because of not only its effects on expansion of the vector population, but also its direct effect of disrupting multiple sectors of Venezuela's local infrastructure, such as power lines, roadways, and communication. In this example, although documentation of infrastructure collapse due to flooding appeared as early as June, local reporting of social collapse specifically due to disease did not appear until September. It could easily be argued that the effects of flooding on local infrastructure greatly increased the probability of rapid loss of containment. It was later hypothesized that this epidemic was due to a possible laboratory accident, highlighting the time-delays inherent in determination of attribution [7].

The VEE epidemic represented a possible translocation issue for the United States given air traffic from Maracaibo, Venezuela, connected directly to Miami (with unknown connector flights to other destinations within the United States) that seasonally peaked during the month of containment loss. To date, it is unknown whether it would have been possible that VEE could translocate to Miami, trigger an outbreak that progressed to an epidemic, ecological establishment, and repeated seasonal transmission thereafter for years to come. A comprehensive assessment of the transmission competency of endemic mosquito species in Miami would be necessary to determine if this was a valid hazard concern [7].

In 1979, a laboratory accident involving aerosolized anthrax occurred in Sverdlovsk, Russia. From April 14 to May 18, 1979, local media in Sverdlovsk explicitly reported the occurrence of a series of human cases of inhalation anthrax along with draconian countermeasures as officials sought to rapidly contain and conceal the true etiology of the event. In 1992 and 1993, a team of American and Russian researchers led by Meselson and colleagues traveled to Sverdlovsk to investigate evidence for two hypotheses of anthrax epidemic of 1979, the official USSR version that infected meat caused the outbreak and the US intelligence claims that the true etiology of the epidemic was an accidental release of aerosolized anthrax spores from the Compound 19 within the Voyenny Gorodok 47 biological weapons laboratory located in the city. The Meselson team concluded that an accidental aerosol release had indeed occurred on April 2, 1979, resulting in what is thought to be the largest documented outbreak of human inhalation anthrax in history. Declassified US intelligence archives suggest that the intelligence community was unaware of this event until months after the fact [8].

This example highlights the requirement for a tactical approach to detect biological events and baseline not only the epidemiological data for the disease itself, but social responses as well. Identifying "unusual" biological events that are evolving rapidly, with an attendant recurrence, elevation, and diversification of the I&Ws, may assist in a time-sensitive evaluation of whether there may be questions of attribution [8].

In each of these case scenarios, the biological event in question produced a "ripple effect" whereby I&Ws appeared in media. However, to fully capture the range of indications that appear over time, other sources of data produced through a wide variety of scientific disciplines and mechanisms are needed.

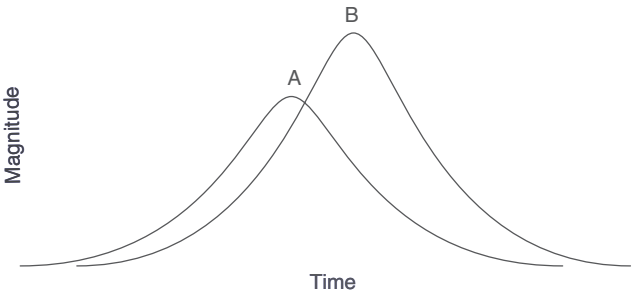



**FIGURE 2** Naturally occurring epidemic with attendant social disruption [A = epidemic and B = social disruption]. The *y* axis represents time and the *x* axis represents magnitude (case count for curve A and number of reports of social disruption for curve B).

**TABLE 2 Surveillance Modes and Example Data Sources Required to Detect and Track the Hypothetical Biological Event Shown in Figure 2**

| | Surveillance Mode | Example Data Source |
|---|---|---|
| Human epidemic (curve A) | Syndromic, voluntary reporting | Clinical encounter data and public health hotlines |
| Social disruption (curve B) | Tactical open source monitoring, infrastructure status monitoring | Pharmaceutical purchase information, real-time hospital census data, real-time ambulance diversion data, and media |

## 5 TARGETING THE ANATOMY OF A BIOLOGICAL EVENT

Figure 2 shows a hypothetical naturally occurring biological event. Table 2 shows example data necessary to detect and track the event. Syndromic surveillance is considered an important asset. Originally funded in the early 1990s as a means to rapidly detect acts of biological terrorism, syndromic surveillance utilizes hospital data thought to contain early disease information such as patient chief complaints and emergency department-generated diagnostic codes for disease. To date, however, no public health organization in the United States has demonstrated consistent operational validation of the use of syndromic surveillance as a means to rapidly detect first appearance of a biological event. The astute clinician is still considered the primary source of this information [9–12]. Our team's observations, however, indicate perhaps a different reality, where public health organizations utilize a wide variety of sources that "tip" the analyst; provide context and relevancy; enable decisions to increase sensitivity of their network of sources (e.g. health care provider advisories); or enable a decision to engage in a full epidemiological investigation or response campaign.

In Figure 3, a naturally occurring zoonotic epidemic for pathogens such as VEE (i.e. an epidemic affecting both animals and humans) may produce essentially two time-lagged periods of disease with attendant social disruption. Experientially, our team has noted that social disruption for animal disease tends not to be of the same magnitude as social disruption caused by human disease. Table 3 outlines example modes of surveillance and data sources. Note that some zoonotic diseases such as the example of VEE above, require monitoring of meteorological, environmental, and vector insect species.

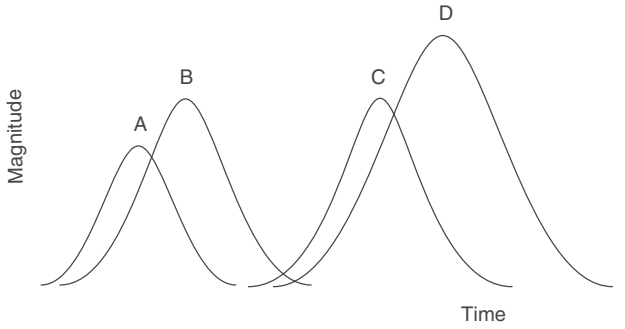



**FIGURE 3** Naturally occurring zoonotic epidemic with attendant social disruption (A = animal epidemic, B = social disruption due to animal epidemic, C = human epidemic, and D = social disruption due to human epidemic).

**TABLE 3 Surveillance Modes and Example Data Sources Required to Detect and Track the Hypothetical Biological Event Shown in Figure 3**

| | Surveillance Mode | Example Data Source |
|---|---|---|
| Animal epidemic (curve A) | Syndromic, voluntary reporting | Veterinary encounter data, agricultural and public health hotlines, and media |
| Human epidemic (curve B) | Syndromic, voluntary reporting | Clinical encounter data, public health hotlines, and media |
| Social disruption (curves B and D) | Tactical open source monitoring, infrastructure status monitoring | Agricultural commodity monitoring, pharmaceutical purchase information, real-time hospital census data, real-time ambulance diversion data, and media |
| Other Parameters | Meteorological, vector, environmental | Meteorological data, satellite imagery, mosquito surveillance data |

"Other parameters" would become important if the pathogen in question is a mosquito-transmitted virus such as VEE.

These modes of surveillance provide such information, for example, as identification of conditions favorable for mosquito emergence and whether the mosquito pools are increasingly positive over time for the pathogen in question. It is known that for some mosquito-transmitted viruses, ambient environmental temperature is an important driver of transmission. Obviously, it is important to determine up front whether local endemic mosquitoes are transmission competent for the pathogen in question.

What is poignant to note in this example is the anticipatory information potentially available when tracking animal illness. Die-offs or illness in different species of animals may portend eventual presence of disease in humans. Understanding the signs of disease and apparent tropism expressed through the involvement of different animal species can provide valuable clues to the possible diagnosis. In the case of mosquito-vectored viral disease such as VEE, an awareness of when ambient temperature optimization will occur provides anticipatory information regarding when the height of human cases may be observed.

Figure 4 and Table 4 shows a hypothetical biological event that followed a natural disaster such as flooding. This is often the case in equatorial regions of the world involving

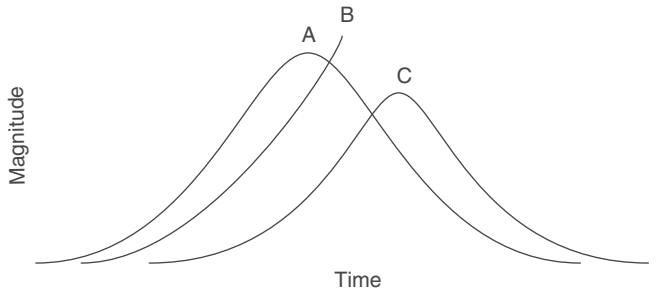



**FIGURE 4** Natural disaster-induced social disruption preceding biological event (A = flooding, B = epidemic, and C = social disruption).

**TABLE 4 Surveillance Modes and Example Data Sources Required to Detect and Track the Hypothetical Biological Event Shown in Figure 4**

| | Surveillance Mode | Example Data Sources |
|---|---|---|
| Natural disaster (curve A) | Tactical open source monitoring, meteorological, disaster reporting services, environmental sensors | Disaster response community listservs, satellite imagery, disaster and humanitarian emergency reporting, seismic sensors, and media |
| Social disruption (curve B) | Tactical open source monitoring, infrastructure status monitoring | Agricultural commodity monitoring, pharmaceutical purchase information, real-time hospital census data, real-time ambulance diversion data, and media |
| Human epidemic (curve C) | Syndromic, voluntary reporting | Clinical encounter data and public health hotlines |

countries with poor access to safe drinking water. For example, in many parts of India, seasonal monsoon rains result in reports of heavy rainfall, followed by flooding, civil infrastructure and crop damage, and attendant social disruption. This information can be captured in local media sources, nongovernmental organization reporting, meteorological data, and satellite imagery. In time, public anxiety about possible increase in waterborne illness such as cholera beings to appear, followed by scattered reports of cholera that may or may not represent true excession of baseline disease. If an outbreak is triggered by compromised sanitation, then reports of high cholera case counts with attendant social disruption are observed. In this case, we see natural disasters potentially accelerating the time to local loss of containment of a biological event that may have international public health implications. As with the example in Figure 3, anticipatory information is present should the operator be sensitive to which areas of the world report this kind of phenomenon. Each piece of anticipatory information is a driver for increased analytic sensitivity to the evolving event.

In Figure 5 and Table 5, a hypothetical foreign biological event, with its attendant social disruption, is translocating to the United States to generate a domestic biological event. In this case, tactical detection and tracking of the foreign biological event can provide anticipatory information regarding a potential transnational issue. The challenge

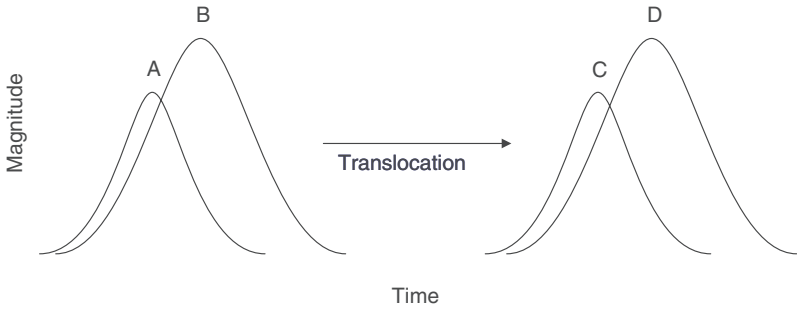



**FIGURE 5** Naturally occurring epidemic translocating from one site to another with attendant social disruption (A = epidemic at the donor site, B = social disruption at the donor site, C = epidemic at the recipient environment, and D = social disruption at the recipient community).

**TABLE 5 Surveillance Modes and Example Data Sources Required to Detect And Track The Hypothetical Biological Event Shown in Figure 5**

| | Surveillance Mode | Example Data Sources |
|---|---|---|
| Foreign epidemic (curve A) | Tactical open source monitoring, voluntary reporting, international public health surveillance | CDC advisories, WHO Global Outbreak Alert and Response Network, and media |
| Social disruption (curve B) | Tactical open source monitoring | Media |
| Translocated domestic epidemic (curve C) | Syndromic, voluntary reporting | Clinical encounter data and public health hotlines |
| Social disruption (curve D) | Tactical open source monitoring, infrastructure status monitoring | Agricultural commodity monitoring, pharmaceutical purchase information, real-time hospital census data, and real-time ambulance diversion data |
| Other parameters | Transportation and commerce monitoring | Commodities trade and transportation data |

CDC, United States Centers for Disease Control and Prevention; WHO, World Health Orginization.

is determination of the criteria for declaring a true translocation advisory, whom to advise (i.e. which local departments of health or agriculture), and advise regarding how they should respond. Nevertheless, anticipatory information resides in detection of the foreign biological event for which containment has been lost; in other words, indicators of this event are essentially pre-event indicators from the perspective of the United States given the event is not directly affecting the domestic infrastructure yet. On the other hand, US assets deployed in the same countries may become directly or indirectly affected by this event, whether or not translocation takes place.

Figure 6 and Table 6 displays a hypothetical intentional release of a biological agent (curve A), followed by an epidemic (curve B) with attendant social disruption (curve C). In this particular example, biosensors become an important asset to rapidly detect a possible release and cue local public health response before human cases actually present

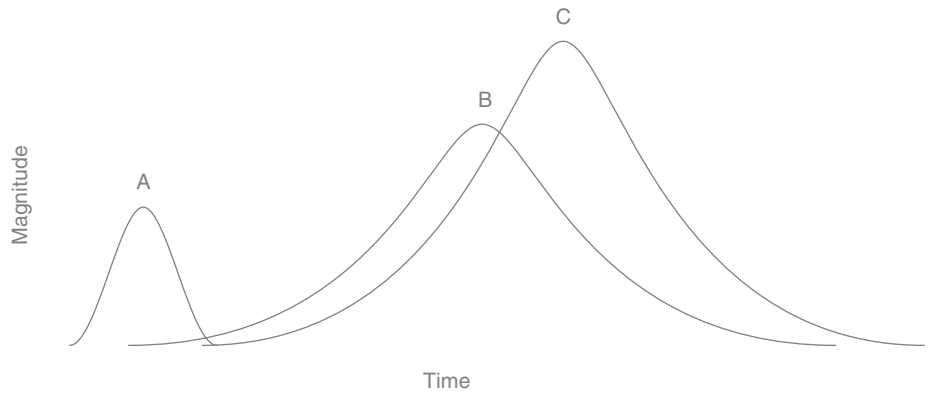



**FIGURE 6** Intentional release of biological event, followed by epidemic and social disruption (A = biological agent released, B = epidemic, and C = social disruption).

**TABLE 6 Surveillance Modes and Example Data Sources Required to Detect and Track the Hypothetical Biological Event Shown in Figure 6**

| | Surveillance Mode | Example Data Sources |
|---|---|---|
| Release of biological agent (curve A) | Biosensor | BioWatch |
| Human epidemic (curve B) | Syndromic, voluntary reporting | Clinical encounter data and public health hotlines |
| Social disruption (curve C) | Tactical open source monitoring, infrastructure status monitoring | Pharmaceutical purchase information, real-time hospital census data, real-time ambulance diversion data, and media |
| Other parameters | Meteorological | Meteorological data |

to health care providers. Thus, detection of a biological agent by a biosensor can prompt sensitization of the entire surveillance network and possibly cue response planning ahead of reports of actual human casualties.

In summary, a wide variety of data sources are required for biosurveillance, which have varying usefulness in biological event detection, providing context and relevance of the information, enabling outbreak alert and verification, and determination of attribution. Table 7 displays a summary table of example data sources required for biosurveillance.

Discussion of data requirements for biosurveillance would be incomplete without consideration of how the data would be used and whether data or information derived from data is more operationally relevant. Process and operational requirement definition is a critical consideration. This includes consideration of whether the organization in question is functioning at the national, state, or local level and whether the operations tempo is tactical, strategic, or forensic. How the information is to be used, by whom, and under what distribution control are additional considerations. Although biological events themselves cause social disruption, improperly managed risk communication stemming

**TABLE 7 Summary of Example Data Sources and Functional Modes of Biosurveillance**

| Surveillance Mode | Primary Function | Example Data Sources |
|---|---|---|
| Disaster reporting services | Anticipatory information regarding conditions favorable for rapid containment loss should a biological event appear; anticipatory information regarding environmental conditions favorable for disease emergence | International: disaster response listservs; domestic: National Geological Survey reporting and seismic sensors |
| Environmental sensors | Anticipatory information regarding environmental conditions favorable for disease emergence | International and domestic: satellite imagery |
| Biosensor | Anticipatory information regarding possible act of biological terrorism | Domestic: BioWatch |
| Threat reporting | Anticipatory information regarding potential for act of biological terrorism | International and domestic: intelligence |
| Meteorological | Anticipatory information regarding transmission rate influencing by meteorological conditions | National Weather Service meteorological data |
| Infrastructure status monitoring | Biological event detection and tracking | Domestic: pharmaceutical purchase information, real-time hospital census data, and real-time ambulance diversion data |
| International public health surveillance | Biological event detection and tracking | International: CDC advisories, WHO Global Outbreak Alert and Response Network, FAO and OIE reporting, and nongovernmental organization reporting |
| Tactical open source monitoring | Biological event detection and tracking | International: media; domestic: media |
| Voluntary reporting | Biological event detection and tracking | Domestic: public health and agricultural community hotlines |
| Syndromic surveillance (animal) | Context | Domestic: veterinary encounter data and laboratory data |
| Syndromic surveillance | Context | Domestic: clinical encounter data and laboratory data |
| Vector surveillance | Context | Domestic: local department of health mosquito surveillance reporting |
| Transportation and commerce monitoring | Determination of hazard relevance | International and domestic: commodities trade and transportation data |

This is not an all-inclusive list but meant to provide an illustrative example. FAO, Food and Agriculture Organization; QIE, World Animal Health Organization.

from biosurveillance information can generate social disruption as well to the detriment of the organization seeking to maintain resources for their activities.

## 6 SOCIAL NETWORKING FOR SOURCE MANAGEMENT

The "astute clinician", be they a human or animal health care provider, is generally thought to be the primary source of valuable biosurveillance data. It is through the astute clinician that the first case of what may eventually be a health catastrophe is most likely reported. As mentioned above, there are other indicators that may precede human cases such as animal die-offs or runs of over-the-counter drug purchases. This requires engineering a complex social network of reporting that is heavily based on human–human interactions, regardless of whatever information technology may or may not be supporting the particular data source. Several important considerations should be kept in mind when utilizing social networks.

It is important to understand the incentive, or abject lack thereof, to report. Physicians, while socially conscientious, may not have the time in a resource-constrained clinical environment to report on a list of over a hundred reporting requirements. However, a health care data management system that can be configured to automatically report certain infrastructure indicators such as ventilator census would be nonintrusive to the busy clinician. Pet store owners, fearing regulatory intervention, may not be inclined to report rodent illness in their stock. However, if they could be educated about the potential risks of importing exotic rodents, it may result in protection of their business' assets.

Social networks can function both passively and actively against reporting requirements. Detection of a key indicator such as avian die-offs in the city park may prompt a health care advisory to "be on the lookout" for human encephalitis, other animal species illness, and refer to mosquito surveillance data due to a concern for the potential presence of actively transmitting West Nile virus in the local environment. Thus, indications of a potential problem may prompt a verification cycle. A social network of partners who can reliably and credibly report is essential to the biosurveillance analyst.

Reporter fatigue is a major consideration that is mitigated through a careful management of the social network that includes judicious use of network sensitization. A health care provider network that has received frequent advisories of what are deemed inconsequential reports may be less likely to pay attention to the organization in times of a serious need to report. Further, social network development that leads to timely reporting may, in some cases, require a monitoring group to assure a reporting source of a certain level of anonymity depending upon that source's personal considerations, much like a media reporter protects his/her sources.

Finally, components of a social network report in different ways that can be considered from the standpoint of specificity, credibility, reliability, and timeliness. For example, a report from a sanitation worker suggesting that the sewer is full of dead rats is associated with a different specificity than a laboratory reporting a plague-positive rat. One may receive the information earlier from the laboratory; however, this depends on sampling location and frequency versus reliable reporting from a sanitation worker who monitors the sewers on a daily basis. These considerations will influence the circumstances and degree to which the network will need to be "pinged" to obtain more specific information. Table 8 provides an example of an indicator cross-matched to sources associated with information type, credibility scores, and estimated reliability of reporting.

**TABLE 8 Example Indicator Cross-Matched to Sources and Source Characteristics**

| Indications and Warnings | Potential Source? | Information Type (Event Tipping, Clinical/Syndromic, Diagnostics or ALL OF THE ABOVE) | Credibility (1 is LOW, 5 is HIGH) | % Probability of Receiving Daily Report IF There is a Perceived Issue |
|---|---|---|---|---|
| Reports of disease or death in: | | | | |
| Birds (including poultry) | General public | Event tipping | 4 | 100 |
| Birds (including poultry) | Fish and Wildlife Service | All of the above | 5 | 100 |
| Birds (including poultry) | Animal hospital | All of the above | 5 | 100 |
| Birds (including poultry) | Poultry farmers | Event tipping and clinical | 5 | 50 |
| Birds (including poultry) | Local zoo | All of the above | 5 | 50 |
| Birds (including poultry) | Birdwatchers/ naturalists | Event tipping | 5 | 100 |
| Birds (including poultry) | Veterinarians | All of the above | 5 | 100 |

## 7 CONCEPTUALIZING OPERATIONS: THE PERSPECTIVE OF LOCAL PUBLIC HEALTH

Until the anthrax attack of 2001, the US public health and agriculture communities had not conceived of a concept of biosurveillance operations that functioned in a near-real-time environment. Their operations were, up to that point, focused on preventive strategies coupled loosely to response and recovery operations within a highly reactive, versus proactive, organizational posture. The idea of coupling graded biosurveillance I&Ws to graded response remained highly experimental.

Figure 7 displays an actual decision-making framework for the District of Columbia Department of Health (DC DOH). Of interest is the number of sources of information and how the information is actually used. Each source either tends to function as an event detection (or "tipping") source or as a source that provides context after a tip is received. As event information from sources such as laboratory notification of a select agent is discovered, DC DOH analysts engage in discussion as to the relevance of the information, whether a shift from a passive to active surveillance posture is warranted, and whether health care providers should be sensitized.

Decisions made at one point in the process may be reassessed as new information becomes available. Gradual shifts in local network sensitivity in reaction to biosurveillance information may be considered a form of response in effect, acting as a feedback loop to further refine reporting and response. It is within this framework that biosurveillance influences tactical situational awareness within local public health.

The investigative process is typically one of increasing specificity of information over time. Thus, depending on the timeliness, validity, and access to information, the process

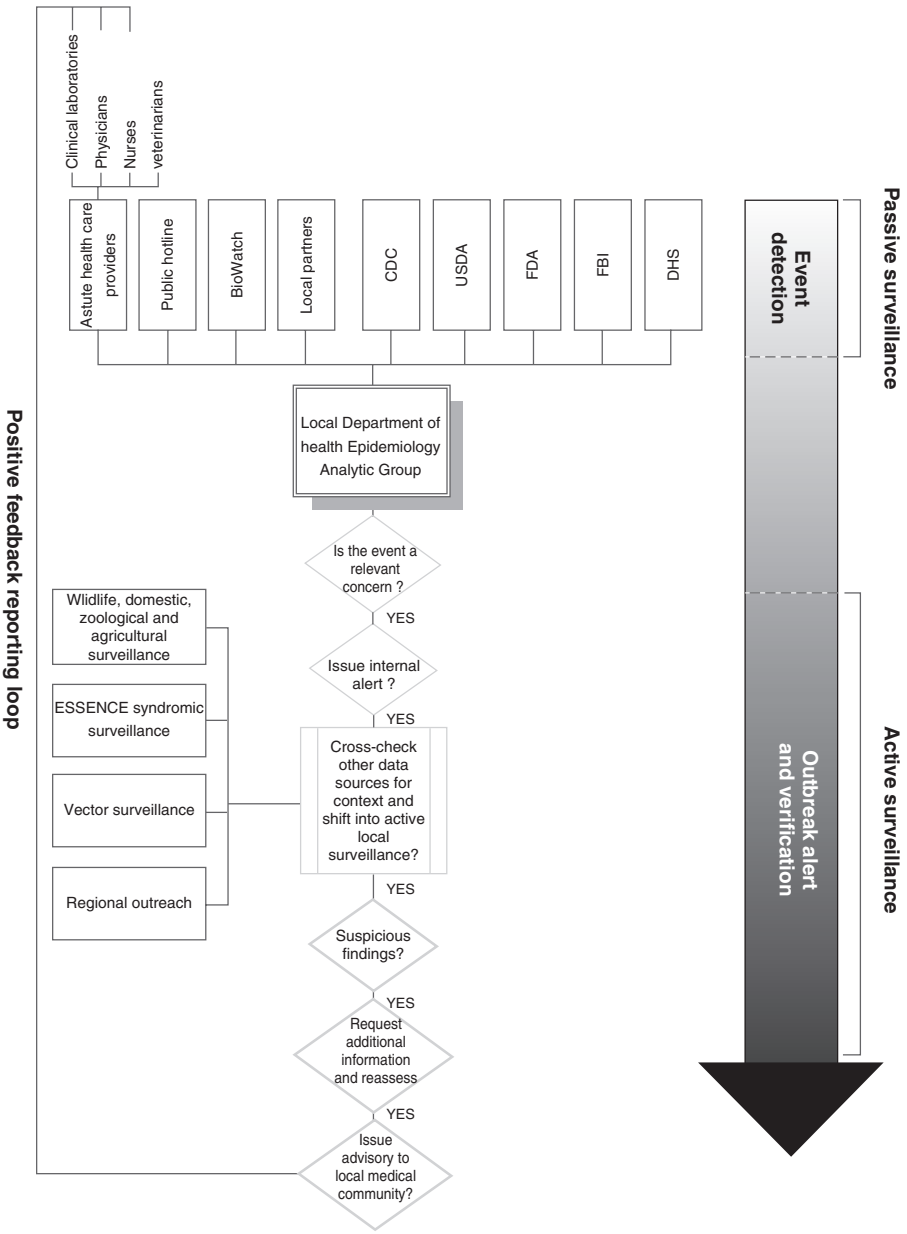



**FIGURE 7** Biosurveillance information processing within the DC DOH.

involves a certain length of time until informed decisions are able to be executed at each step.

Table 9 shows estimates provided by the DC DOH in regards to local sources of information and how relative percentages of information may change with community sensitization. A decision made to sensitize the health care community is used judiciously due to the high risk of desensitization and reporter fatigue. The DC DOH understands

**TABLE 9 Relative Percentages of Source Reporting Within the Category of "Astute Clinician" and Comparison Between Nonsensitized and Sensitized Situations**

| | Not Sensitized—Passive Surveillance (%) | Sensitized—Active Surveillance (%) |
|---|---|---|
| Laboratory worker | 80 | 45 |
| Nurse | 15 | 25 |
| Physician | 4 | 25 |
| Veterinarian | 1 | 5 |

fully that physicians in particular have little time in their daily routines to report issues not perceived to be of immediate importance.

Local public health organizations are typically resource constrained, and therefore have a low tolerance for high daily volumes of nonrelevant biosurveillance information. The challenge of determining information relevance is a critical one to the local public health professional.

## 8 BRIDGING RAW DATA TO ACTIONABLE INFORMATION

There is an important difference between raw data and actionable information. Releasing raw data to a user community is fraught with risk such as inappropriate interpretation and user desensitization. Translating raw data into preliminary information typically requires subject-matter expert input. Without context, it is difficult for end users to interpret the data. Another step is processing the preliminary information by comparing it with other data or information sources for additional context. This may then be followed by first-, second-, or third-order analytics. The final piece of information, or finished information product, may require additional analysis to determine relevance for the individual user. The typical public health analyst, in a resource-constrained environment, will not be as willing to engage in examination of noncontextualized raw data versus a finished assessment. Finished assessments resulting from the abovementioned process take a significant amount of time to produce. Further, the typical public health analyst is generally focused on his/her immediate local health concerns and not necessarily aware, in a timely fashion, of developing regional and international situations that have potential to translocate to his/her area of responsibility. When considering the need for near-real-time detection and tracking of biological events, a balance must be struck whereby a form of preliminary information is passed to the user community *in lieu* of a finished assessment that follows later.

## 9 AN ADVISORY SYSTEM FOR BIOSURVEILLANCE

For several decades, the National Weather Service and the natural disaster community have made effective use of an advisory system to alert users and the general public of impending issues. The advisory system for storms not only informs and cues the meteorological community to closely follow the event in question but also has a translated response implication for the lay public. For example, the average citizen has an inherent

**TABLE 10 The Wilson–Collmann Scale for Biological Event-Related Social Disruption**

| Stage | Condition |
|---|---|
| 0 | Conditions favorable to support the appearance of a biological event |
| 1 | Unifocal biological event |
| 2 | Multifocal biological event |
| 3 | Severe infrastructure strain and depletion of local response capacity |
| 4 | Social collapse |

understanding that a category 1 hurricane is associated with a lower implied need to evacuate the area than a category 5 hurricane [13, 14].

The Wilson—Collmann Scale, a prototype staging system for social disruption due to biological events, has been established and in use by Project Argus since 2004, as summarized in Table 10. This heuristic model enables an analyst to rapidly assess the severity of a biological event based on the level of social disruption generated using a standardized terminology. This information, when placed in context with the suspected pathogen, can assist the analyst in making a decision to issue an advisory to the user community [2].

However, this staging system has not been tested domestically in the United States. Standards for a biosurveillance-informed advisory system have not been developed at the national, state, or local levels for biological events that affect humans, animals, or plants. Reporting requirements beyond legally mandated disease-specific reporting for the biosurveillance environment have not been integrated and standardized across different communities of interest. This then presents a key challenge: how does one define data requirements when no operational requirements have been generated? What should national, state, and local level watchboards post as advisories? What would a warning, watch, and advisory look like from each of these perspectives? How would a warning posted on a national level watchboard be translated in a local watchboard? And of key importance, precisely who at the national, state, and local levels should receive these advisories? This becomes a particularly difficult question when considering the community health care provider is likely to be the first line of response. A nonsensitized health care provider is not as likely to consider exotic diagnoses versus one who has been sensitized to look for a particular disease.

Relevance of the information to the user is difficult to predict. Some users are interested in select agents such as anthrax, others are primarily interested in international public health issues such as polio, and other users are concerned about any disease that may affect a ground deployment. This translates to a high degree of complexity when attempting to design an advisory system. Defining relevance is partly a user-defined process; however, the use of disease risk and transmission models may enable refinement of what advisories are relevant to which US local communities and which biological event may truly present a critical national or homeland security issue.

Advisory systems have value in controlling distribution, in a net-centric manner, to the biosurveillance community. Further, they enable control of network sensitization, where various components of the community can be cued to look for certain indicators of an event of interest. Advisory systems enable operational translation of biosurveillance data into actionable information, which is the key objective.

## 10 DISCUSSION

Biosurveillance as a professional discipline is nascent but rapidly emerging. While the process is largely art versus science, the discipline is certainly approaching a point where robust modeling and statistical rigor may be applied. Similar to medicine, this is a discipline of processing uncertainty, intuition, and hunches. Computer algorithms and sophisticated IT platforms cannot replace such experience gained by trial and error over time by an operational biosurveillance group; however, facilitation of effort is a key objective when dealing with global biosurveillance information. We often liken the emergence of the biosurveillance tradecraft to the history of tornado forecasting, where in the 1950s humans learned how to collect and process information related to an event associated with morbidity and mortality (i.e. tornadoes). Over the decades, enough information was gathered to enable mathematical modeling and eventual expansion of a multidiscipline community of professionals that span the private, academic, and public sectors. We see biosurveillance following this same exciting evolutionary path.

## ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers of this manuscript and Dr Bradley Clark (Trinity Applied Strategies Corporation), Noel Williams, and Dakota Wood (Systems Planning and Analysis, Inc.).

## REFERENCES

1. Association of State and Territorial Health Officials (2006). *Position Statement: Biosurveillance*, March 17. Available from http://www.astho.org/pubs/BiosurveillancePositionStatementFINAL030706.pdf.
2. Wilson, J. M., Polyak, M. G., Blake, J. W., and Collmann, J. (2008). A heuristic indication and warning staging model for detection and assessment of biological events. *J. Am. Med. Inform. Assoc.*, **15**(2), 158–171.
3. Cieri, C., Strassel, S., Gra, D., Martey, N., Rennert, K., and Liberman, M. (2002). Corpora for topic detection and tracking. In *Topic Detection and Tracking—Event-based Information Organization*, J. Allan, Ed. Kluwer Academic Publisher, Norwell, MA, pp. 33–66.
4. Makkonen, J. Investigations on event evolution in tdt. *Proceedings of HLT-NAACL 2003, Human Language Technology Conference of the North American Chapter of the Association for Computational Linguistics Student Workshop 2003*. Edmonton, Alberta, CA.
5. Chien Chin, C., Yao-Tsung, C., Yeali, S., and Meng Chang, C. (2003). Life cycle modeling of news events using aging theory, lecture notes. *Comput. Sci.* **2837**, 47–59.
6. Polyak, M. G., Blake, J. W., Collmann, J., and Wilson, J. M. (2008). Emergence of Severe Acute Respiratory Syndrome (SARS) in the People's Republic of China, 2002–2003: a case study to define requirements for detection and assessment of international biological threats. *J. Am. Med. Inform. Assoc.*, **15**(2), 158–171.
7. Blake, J. W., Polyak, M. G., Gambale, P., Pinzon, J., Tucker, C. J., Collmann, J., and Wilson, J. M. (2008). Venezuelan equine encephalitis: a case study in international biological threat detection and assessment. *J. Am. Med. Inform. Assoc.*, **15**(2), 158–171.
8. Polyak, M. G., Blake, J. W., Hartley, D., and Wilson, J. M. (2006). *Anthrax in Sverdlovsk, U.S.S.R., April–June 1979: A Case Study in Examining Open-Source Media for Indications*

*and Warnings of an Accidental Biological Weapons Release*, Argus Research Operations Center Internal Report, Argus Research Operations Center, Imaging Science and Information Systems Center, Georgetown University Medical Center, Washington, DC.

9. United States General Accounting Office (2003). *Infectious Disease Outbreaks: Bioterrorism Preparedness Efforts Have Improved Public Health Response Capacity, but Gaps Remain*, GAO-03-654T April 9. Available from http://www.gao.gov/new.items/d03654t.pdf.
10. United States General Accounting Office (2003). *Infectious Diseases: Gaps Remain in Surveillance Capabilities of State and Local Agencies*, GAO-03-1176T September 24. Available from http://www.gao.gov/new.items/d031176t.pdf.
11. United States General Accounting Office (2004). *Emerging Infectious Diseases: Review of State and Federal Disease Surveillance Efforts*, GAO-04-877 September 30. Available from http://www.gao.gov/new.items/d04877.pdf.
12. Buehler, J. W., Berkelman, R. L., Hartley, D. M., and Peters, C. J. (2003). Syndromic surveillance and bioterrorism-related epidemics. *Emerg. Infect. Dis.*, **9**(10), 1197–1204.
13. National Hurricane Center, National Weather Service, National Oceanic and Atmospheric Administration *The Saffir-Simpson Hurricane Scale*, Available from: URL: http://www.nhc.noaa.gov/aboutsshs.shtml.
14. National Weather Service, National Oceanic and Atmospheric Administration *Fujita Tornado Damage Scale*, Available from: URL: http://www.spc.noaa.gov/faq/tornado/f-scale.html.

# THE NORTH CAROLINA BIOSURVEILLANCE SYSTEM

ANNA E. WALLER AND AMY I. ISING

*Department of Emergency Medicine, School of Medicine, University of North Carolina, Chapel Hill, North Carolina*

LANA DEYNEKA

*General Communicable Disease Control Branch, North Carolina Division of Public Health, Department of Health and Human Services, Raleigh, North Carolina*

## 1 INTRODUCTION

On October 17, 2007, President George W. Bush issued the Homeland Security Presidential Directive 21 (HSPD 21) [1]. HSPD 21 outlines immediate steps for improving the nation's preparedness for natural and intentional disasters, and includes specific criteria

for effective biosurveillance systems. Biosurveillance systems must be able to "identify specific disease incidence and prevalence in heterogeneous populations and environments and must possess sufficient flexibility to tailor analyses to new syndromes and emerging diseases". In addition, all stakeholders, from public health officials at all levels to data providers and clinicians, must be involved in system design. The North Carolina Disease Event Tracking and Epidemiologic Collection Tool (NC DETECT), is North Carolina's statewide biosurveillance system. Although its roots date back to an electronic emergency department (ED) data collection initiative launched in 1999, NC DETECT embodies those characteristics outlined in HSPD 21.

## 2 BACKGROUND

NC DETECT is an advanced, statewide public health surveillance system made possible through a unique combination of leaders in North Carolina from public health, business, and research working together toward a common goal: to enhance the protection of the NC population. NC DETECT is managed through a collaboration between the North Carolina Division of Public Health (NC DPH) and the University of North Carolina at Chapel Hill Department of Emergency Medicine (UNC DEM).

### 2.1 Data Sources Timeline

The North Carolina Emergency Department Database (NCEDD) project, spearheaded by UNC DEM in 1999, laid the groundwork for electronic ED data collection in North Carolina by developing best practices for collecting and standardizing quality ED data. NC DPH and UNC DEM jointly started developing the hospital arm of the NC DETECT syndromic surveillance system in 2002. In 2004, a partnership between the North Carolina Hospital Association (NCHA) and NC DPH was instrumental in establishing ED data transmissions from the hospitals not yet participating in NC DETECT, including support for a new law making this reporting mandatory as of January 1, 2005 [2]. As of January 7, 2008, there are 109/111 (98%) hospital-based, acute care, 24/7 EDs submitting over 10 000 new visits on a daily basis to NC DETECT, as shown in Figure 1. These data are also transmitted twice daily to the Centers for Disease Control and Prevention's (CDC's) BioSense program.

In addition to ED data, NC DETECT initiated the collection of additional data sources in 2004. Data collection from multiple data sources provides a more comprehensive view of population health and offers redundancy on the occasion one data source has lapses in data transmission. Currently, NC DETECT loads data from roughly 1800 new records for ambulance runs and 285 statewide poison center calls a day. Animal health data from a regional wildlife center and veterinary medicine laboratories are in pilot testing. Future goals include the incorporation of additional animal health data, as well as data from ambulatory and urgent care centers and Veterans Administration (VA) hospitals.

## 3 TECHNOLOGICAL OVERVIEW

NC DETECT is an electronic biosurveillance system that does not require any manual data entry [3]. All data are secondary or dual use; in other words, data are generated as part of the registration, treatment, and/or billing of human and animal patients. Data

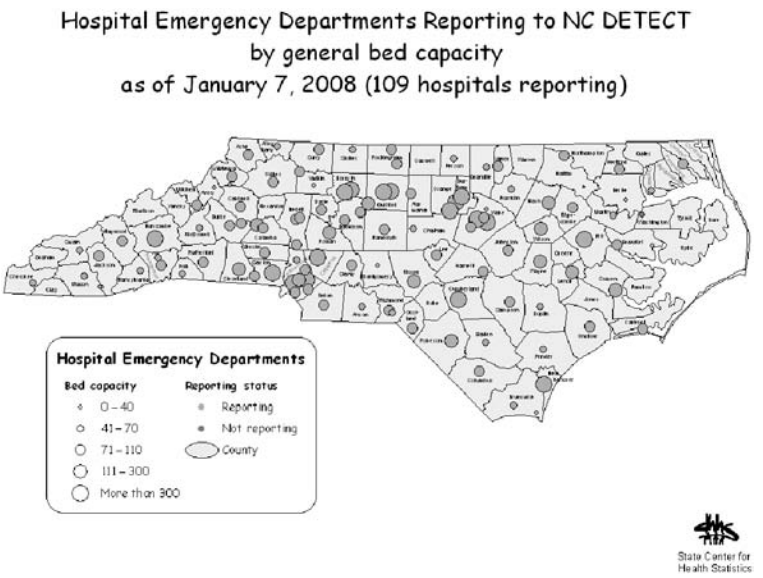



**FIGURE 1** Hospitals reporting ED data to NC DETECT.

are transmitted securely to a centralized server. Before loading into NC DETECT, all data are automatically checked to ensure that all values match established business rules for acceptable quality. Outliers are logged for future follow up and data providers with missing data are notified. As part of the data processing, all data sources are "binned" into one or more syndromes. Public health epidemiologists (PHEs) monitor these syndromes daily, by facility and/or patient's county of residence, to detect unusual events of potential public health significance.

### 3.1 Syndrome Development and Classification

NC DETECT classifies ED visits into zero, one or more "syndromes" based on the presence of certain keyword terms in either the chief complaint or triage note, as well as the documented temperature (if available). Syndrome definitions are designed to capture both potential bioterrorist threats and common community-acquired disease outbreaks.

The keyword terms searched for include both syndrome-specific (e.g. dyspnea, cough, or tachypnea for respiratory syndrome) and constitutional (e.g. fever, malaise, or myalgias) signs and symptoms. Each syndrome definition also searches for common misspellings, abbreviations, truncations, and acronyms for these terms. In order for a record to match a syndrome, it must contain either a single term, which, by itself, is highly suggestive of the syndrome in question (e.g. "flu" for influenza-like illness (ILI)) or the mention of a bioterrorism (BT) related agent. A record will also match a syndrome if it contains the combination of both a syndrome-specific and a constitutional term.

Text-based syndrome case definitions published by the CDC [4] form the basis for the syndrome definitions. The syndromes have been developed and refined through an iterative process by the NC DETECT Syndrome Definition Workgroup and are based on the experience and judgment of the workgroup members with feedback from NC DETECT end users. The workgroup comprises state and local public health officials,

epidemiologists, physicians, and public health informatics researchers. A collaborative research project between the UNC DEM and RTI International is ongoing and has the overarching goal of optimizing the sensitivity and specificity of syndrome definitions for the purposes of early event detection and situational awareness [5]. This work is funded by the CDC's BioSense program.

While the ED data can provide a wealth of information for effective syndrome binning, the chief complaint and triage notes most often contain free form text. The textual data are unstructured and include abbreviations, misspellings, and negation, which require specialized processing. Tools available in the public domain to assist with this processing include the Emergency Medical Text Processor (EMT-P) for chief complaint standardization [6] and NegEx [7] for negation processing, both of which are in use in NC DETECT. While NC DETECT does capture ICD-9-CM final diagnosis codes from all EDs, the codes are most often sent from hospital billing systems that are updated days to weeks after the initial visit [8]. This latency severely limits the utility of this data element for early event detection.

In contrast to the ED data, poison control center data are entered into a nationally standardized electronic system, the National Poison Data System (NDPS), by trained nurses and, therefore, are relatively easily binned into syndromes based on documented clinical effects. EMS data are grouped into seven syndromes based on the standardized pick lists for dispatch complaint and primary symptom. Table 1 lists the syndromes monitored for these three data sources and the bioterrorism agents the syndromes are designed to detect.

### 3.2 Web-Based Application

The NC DETECT Web application provides authorized users with secure, Java-based reports with various customization options. It provides syndrome-based monitoring by patient's county of residence and, for ED data, by hospital. Users can review signals or aberrations using the CDC's EARS CUSUM algorithms [9] for the entire population, as well as stratified by nine age groups. In addition to aggregate views, the application provides users with access to patient-specific line listing reports for the ED, poison center, and EMS data. Authorized users are able to drill down further to retrieve identifiable data as needed for further public health investigation. All NC DETECT Web functionality is developed in a user-centered, iterative process, with user feedback from all stakeholder groups guiding enhancements and new development. This feedback, along with the need for improved situational awareness and the desire to improve communication among users, drove the development of the Annotation Reports and the Custom Event Report.

As explained in HSPD-21, effective disease surveillance alone does not constitute a comprehensive surveillance system. The system must be flexible enough to respond to emerging infections and other public health events not previously anticipated [1]. The NC DETECT Custom Event Report is a separate module that allows for the rapid implementation of new reports designed to monitor known or suspected events that might not be captured by existing syndromes. New custom reports can be added to the system as soon as the search criteria have been finalized and tested, usually 1–2 h. These reports search for suspected cases in the chief complaint and triage notes, as well as ICD-9-CM final diagnosis codes (keeping the latency effect in mind). The queries account for misspellings and abbreviations, and exclude terms that would create false positives; for example, search for *fire* but not *fire ant*. Again, authorized users can retrieve

**TABLE 1 Syndromes Monitored in NC DETECT**

| ED | Poison Center | EMS/Ambulance | Related BT and Chemical Agents (If Applicable) |
|---|---|---|---|
| Botulism-like | N/A | N/A | *BT agents:*<br>Botulism |
| N/A | Cardio | N/A | *Chemical agents:*<br>Cyanide<br>Ricin (ingested) |
| N/A | Fever | Fever | *BT agents:*<br>Smallpox |
| Gastrointestinal-all, gastrointestinal-severe | Gastrointestinal | Gastrointestinal | *BT agents:*<br>Anthrax (gastrointestinal)<br>Food safety threats (e.g. *Salmonella* species, *Escherichia coli* O157:H7, Shigella)<br>Water safety threats<br>Ricin (castor bean oil extract)<br>*Chemical agents:*<br>Vesicants/blister agents: sulfur mustard, lewisite, nitrogen mustard, mustard lewisite, and phosgene-oxime<br>T-2 mycotoxins: Fusarium, Myrotecium, Trichoderma, Verticimonosporium, and Stachybotrys |
| N/A | Hematologic/ hepatic | N/A | *Chemical agents:*<br>Radiation<br>Ricin (ingested) |
| N/A | N/A | Hemorrhagic | N/A |
| Influenza-like Illness | N/A | N/A | N/A |
| Meningo-encephalitis | Neurological | Neurological | *BT agents:*<br>Viral encephalitis<br>*Chemical agents:*<br>Nerve: Sarin (GB), Tabun (GA), Soman (GD), Cyclohexyl Sarin (GF), VX, Novichok agents, organophosphorous compounds (carbamates and pesticides)<br>Cyanides: hydrogen cyanide (HCN), cyanogen chloride<br>- T-2 mycotoxins: Fusarium, Myrotecium, Trichoderma, Verticimonosporium, Stachybotrys |

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| ED | Poison Center | EMS/Ambulance | Related BT and Chemical Agents (If Applicable) |
|---|---|---|---|
| N/A | Nerve agent | N/A | *Chemical agents:*<br>Nerve: Sarin (GB), Tabun (GA), Soman (GD), Cyclohexyl Sarin (GF), VX, Novichok agents, organophosphorous compounds (carbamates and pesticides) |
| N/A | N/A | Poisoning | N/A |
| Fever/Rash | Dermal | Rash | *BT agents:*<br>Anthrax (cutaneous)<br>Plague (bubonic)<br>Smallpox<br>Tularemia (cutaneous)<br>Viral hemorrhagic fevers (e.g. Ebola, Marburg, Old World Lassa, Junin, and Machupo)<br>*Chemical agents:*<br>Vesicants/blister agents (e.g. sulfur mustard, lewisite, nitrogen mustard, mustard lewisite, and phosgene-oxime) |
| N/A | Ocular | N/A | *BT agents:*<br>Botulism<br>*Chemical agents:*<br>Nerve: Sarin (GB), Tabun (GA), Soman (GD), Cyclohexyl Sarin (GF), VX, Novichok agents, organophosphorous compounds (carbamates and pesticides)<br>Cyanides: hydrogen cyanide (HCN), and cyanogen chloride<br>T-2 mycotoxins: Fusarium, Myrotecium, Trichoderma, Verticimonosporium, and Stachybotrys |
| N/A | Renal | N/A | *Chemical agents:*<br>Ricin (ingested) |
| Respiratory | Respiratory | Respiratory | *BT agents:*<br>Anthrax (inhalation)<br>Plague (pneumonic)<br>Tularemia (pneumonic) |

**TABLE 1 (*Continued*)**

| ED | Poison Center | EMS/Ambulance | Related BT and Chemical Agents (If Applicable) |
|---|---|---|---|
| | | | *Chemical agents:*<br>Vesicants/blister agents: sulfur mustard, lewisite, nitrogen mustard, mustard lewisite, and phosgene-oxime<br>Pulmonary/choking agents: phosgene, chlorine, diphosgene, chloropicrin, oxide of nitrogen, sulfur dioxide, etc.<br>Ricin (castor bean oil extract)<br>T-2 mycotoxins: Fusarium, Myrotecium, Trichoderma, Verticimonosporium, and Stachybotrys |

the hospital's original medical record number from the Web-based report for follow up directly with the hospital.

While early event detection systems aim to detect disease outbreaks before traditional means, following up on the many alerts generated by these systems can be time-consuming and a drain on limited resources [10]. NC DETECT offers Annotation Reports to allow users to view the EARS signals for each syndrome, drill down to the patient-specific information, add comments to signals, and view the comments of other users who have access to the same signals. Users also assign an investigation status to the signal: *active investigation, monitoring, no action needed, or investigation complete*. If NC DETECT does not generate a signal for a known or suspected public health situation, users have the option of adding an event with their own parameters to the Annotation Reports for comments and monitoring, as shown in Figure 2. The NC DETECT Annotation Reports have improved communication and information exchange among active NC DETECT users. However, these tools need to be more widely adopted by less active local health departments, regional surveillance teams, and infection control practitioners before statewide situational awareness can reach its potential [11].

### 3.3 Users Roles and Users

As a statewide system, NC DETECT serves users in multiple jurisdictions with varying responsibilities. As a result, the Web-based application provides access to the data based on state mandates governing public health investigation [2]. Users whose job responsibilities include outbreak investigation and response have more data access privileges than users at similar levels in more administrative and/or managerial roles. The NC DETECT role-based security model is based on geography, data source, the right to access aggregate data, line listing data, protected health information (PHI), and annotations. While most of the user roles can be predefined, the system is flexible enough to allow for

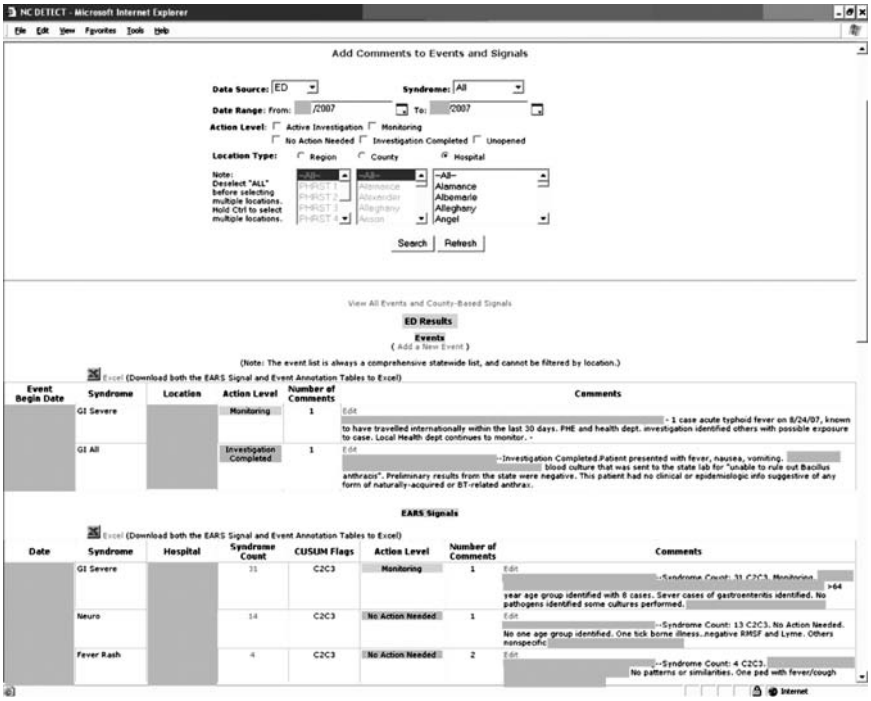



**FIGURE 2** NC DETECT screenshot of Annotation Report.

customized data access; thus, it is possible to meet the needs of all potential NC DETECT users. Access to PHI is strictly controlled. PHI is encrypted in the database and only authorized users have access to it through the SSL-enabled Web portal. The window that displays the PHI closes automatically after 1 min and all access to PHI is logged in detail.

In addition to state level epidemiologists who monitor NC DETECT on a daily basis, the most active user group is the hospital-based PHEs. The PHEs have been funded by NC DPH for over four years as part of state efforts to strengthen public health preparedness and disease surveillance in North Carolina, while fostering communication and relationships between local hospitals and public health departments. Currently staffed in North Carolina's 11 largest hospitals, PHEs serve as in-hospital liaison to local health departments, perform active in-hospital surveillance for community-acquired infections, and conduct biosurveillance using NC DETECT [12].

## 4 NC DETECT OUTCOMES 2005–2008

NC DETECT allows PHEs and infection control specialists to significantly increase the speed of detecting, monitoring, and investigating public health events statewide. The system has proven useful for a variety of public health surveillance needs, including, but not limited to, early event detection, public health situational awareness, case finding, contact tracing, injury surveillance, and environmental exposures.

### 4.1 Early Event Detection

The early event detection capabilities of NC DETECT have contributed to more timely and effective public health intervention in North Carolina, as illustrated in the following examples.

- A Norovirus outbreak was detected in a sorority at UNC Chapel Hill, in 2006. The spread of the disease was prevented by rapid case finding and implementation of control measures.
- Investigation of a possible familial cluster of meningitis in Pitt County, in 2006. The NC DETECT signal helped public health officials to trace the meningitis case, and to provide follow up for the family of five children and one adult through the local health department.
- In early 2007, a public health epidemiologist's investigation of a NC DETECT fever/rash signal in Rowan County revealed a positive diagnosis of meningococcemia (a severe bacterial infection in the blood stream) in a child, prior to reporting by the laboratory or the attending physician. Meningitis prophylaxis was provided to 30 of the patient's close contacts through the Rowan County Health Department.
- The most recent event was a Salmonella London outbreak in a Catawba County Mexican restaurant. From October 29 through November 5, 2007, NC DPH documented 173 cases. NC DETECT was used to monitor this outbreak. The application of age stratification in NC DETECT helped to define the affected population, the majority of which were young adult employees of a nearby plant, as shown in Figure 3.

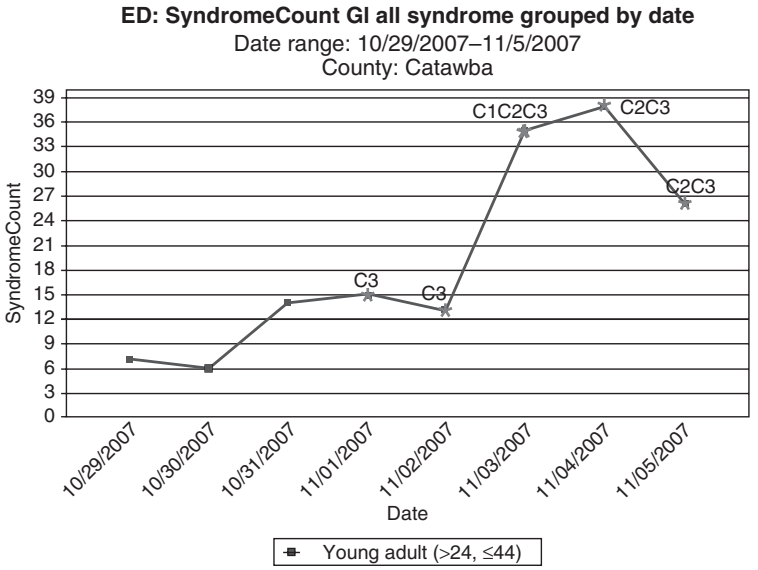



**FIGURE 3** Salmonella outbreak, Catawba County, NC, October–November 2007 evident in NC DETECT GI-All syndrome.

### 4.2 Public Health Situational Awareness

With the NC DETECT system in place, surveillance for new conditions can be established easily and rapidly, as demonstrated with injury and illness surveillance after hurricane Ophelia in NC in 2005. Setting up the specific criteria for surveillance took 2 h, in contrast with similar surveillance after hurricane Isabel in 2003, which required months of labor-intensive data collection, entry, and analysis [13, pp. 26–27]. Querying programs maximize accuracy in analyzing the free text ED data to the greatest extent possible. Detecting unexpected cases and outbreaks earlier in their course than traditional disease-based surveillance has allowed prompt implementation of public health control measures when needed.

***4.2.1 Hurricane Katrina Evacuees.*** At the time of hurricane Katrina, 51 of 111 NC EDs were transmitting data daily to NC DETECT. A new filter was rapidly applied to capture hurricane-associated events. This filter was applied to data transmitted from August 28, 2005, the date of issue of the voluntary evacuation order in the city of New Orleans. Terms used in this filter included: "hurri, storm, flood, Katrina, evacua, New Orleans, refuge, Louisiana, Texas, Alabama, Mississippi, Florida, and fema and not (female)", including variations of misspellings and abbreviations. Surveillance of these data rapidly provided information on the medical needs of hurricane Katrina evacuees in North Carolina. The information from these sources was available to public health officials at the state level on a daily basis, within 24–48 h of the visits. Reasons for evacuee's visits to EDs in North Carolina included medications and prescription refills (15%), specific illnesses and injuries (62%), and mental health issues (7%) [14].

***4.2.2 Apex Chemical Explosion.*** In October 2006, a chemical plant fire forced thousands of people to evacuate from areas of Apex, North Carolina. NC DPH monitored ED data (updated daily) and poison control center data (updated hourly) in NC DETECT to monitor potential human health impact. Near real-time investigation of patients associated with this event was essential, as the list of chemicals stored at the explosion site went unknown for several days. NC DETECT users documented 83 ED visits related to the explosion, including 14 evacuees from an area nursing home and 13 emergency responders. Nearly all patients reported only minor complaints, including gastrointestinal, upper respiratory, and eye and skin irritation, and were discharged home following treatment.

***4.2.3 Peanut Butter Contamination.*** On February 14, 2007, the FDA warned consumers not to eat certain jars of Peter Pan or Great Value peanut butter due to risk of contamination with *Salmonella tennessee* [15]. Surveillance for peanut butter–related ED visits and poison center calls was established within an hour. During the week of February 14, statewide hospital data included 135 ED admissions with peanut butter related gastrointestinal complaints from 39 counties. The poison control center received 370 peanut butter related symptomatic food poisoning calls from 30 counties and adopted a public health message in line with guidance from the NC DPH. In this particular example, the use of the poison center data provided a population-based measure of the reaction to the recall in the general public from persons affected to a degree that did not warrant a visit to a hospital ED.

NC DPH staff documented 16 confirmed cases associated with the *S. tennessee* outbreak in February 2007 in 12 different counties, 7 of which were under 18 years old. Two closely related DNA fingerprint patterns of *S. tennessee* isolates were associated with this outbreak.

***4.2.4 Canned Food Botulism Recall.*** Following reports of four botulism cases in Texas and Indiana associated with commercially canned chili products, the CDC issued a recall in July 2007 [16]. NC DPH increased surveillance for botulism by sharing available information with public and private health care providers through regular communication and also by issuing an alert with the NC Health Alert Network. The NC Department of Agriculture led the product recall activities. Using NC DETECT helped the epidemiologists reviewing North Carolina data by: (i) having immediate access to ED data from 104 hospitals throughout the state, where botulism patients would likely be seen due to the severity of the disease; (ii) having immediate access to all ED patient records matching botulism-like illness, a syndrome continuously monitored with NC DETECT, regardless of this recall; and (iii) focusing on ED visits with records that included words that could associate them with the recall. As an indicator of the "zooming" power of NC DETECT, while 233 patients were picked up by the system between July 16 and July 25 due to the presence of one or more signs or symptoms compatible with the "botulism-like" case definition, only 9 cases during all of July matched a more narrow case definition, restricted to those with records including key words used in this recall. The situation specific "filter" was designed and installed in less than 2 h using the Custom Event Report.

***4.2.5 Heat-Related Illness.*** A report to monitor effects of record heat was added to NC DETECT in early August 2007. Results not only showed an increase of heat-related ED visits as expected but also found that 15–19 year olds and 25–44 year olds had the highest rates of ED visits. As a result, warnings during future heat waves will target these age groups as well as prior target populations, the elderly and those who care for young children [17].

### 4.3 Case Finding and Contact Tracing

With NC DETECT, users with investigative access rights are able to view patient-specific line listing information and to retrieve the hospital's original medical record number. With this information, users are able to conduct follow-ups with much greater ease and reduce the burden on hospital staff.

- In January 2007, users in Guilford County were able to use the arrival date and time information in NC DETECT to locate potential contacts of an ED patient diagnosed with measles more easily and efficiently.
- During a Hepatitis A outbreak investigation in 2006 in Buncombe County, additional Hepatitis A cases were identified and followed up using NC DETECT.
- NC DETECT and another North Carolina-based system called the *investigative monitoring capability* (IMC) were used in a salmonellosis outbreak investigation in New Hanover County (May 2007). Five additional cases were identified using these systems.

**TABLE 2 Carolinas Poison Center Chemical Exposure Signals**

| Exposure | Date | Number of Cases | Site | Co | Syndrome |
|---|---|---|---|---|---|
| Mercury | 10/20/05 | 10 | Residence | Orange | Gastrointestinal |
| Prime 2B | 11/06/05 | 3 | Hospital | Alleghany | Respiratory, dermal |
| Tetrachloroethylene | 04/26/06 | 8 | School | Granville | Respiratory, neuro |
| Apex hazardous exposure | 10/06/06 | 83 | Residence | | Gastrointestinal, respiratory, neuro |
| Pepper spray | 10/10/06 | 11 | School | Wake | Respiratory, dermal |
| Hydrochloric acid | 06/07/07 | 12 | Hotel | Mecklenburg | Respiratory |
| Lead exposure | 06/12/07 | 5 | Residence | Davidson | Gastrointestinal |

### 4.4 Environmental Exposures

Data from poison center calls (Carolinas Poison Center, CPC) allow public health officials to detect and monitor environmental exposures that may otherwise go unreported. For example, a signal investigation during the summer of 2007 revealed a pesticide exposure in Davidson County. The landlord treated the house with an unknown pesticide. The family of 9 (6 adults, 1 of them pregnant, and 3 children) developed gastrointestinal (nausea) and neurological (headache) symptoms, and called CPC for advice. Additional public health investigation revealed that the family lives in a house with bats. The family was provided rabies vaccination and immune globulin prophylaxis through the state program.

Numerous clusters of exposure to chemicals have been identified analyzing signals in the NC DETECT CPC data stream. Some examples are shown in Table 2.

While some of the CPC signal investigations listed in Table 2 did not pose a widespread public health threat, they demonstrate the ability of NC DETECT to identify both environmental and infectious disease clusters and potential bioterrorism events.

***4.4.1 Influenza.*** The NC DETECT ILI definition is used to monitor the influenza season in NC each year, providing data up to two weeks earlier than the traditional, manually tabulated sentinel provider network. The difference in proportion of ILI seen in Figure 4 reflects differences in the case definitions and patient populations rather than a difference in the sensitivity of these surveillance systems.

NC DETECT continues to evolve in response to changing user needs and the increased adoption of timely public health surveillance. While NC DETECT was designed and continues to be used primarily for early event detection and situational awareness, the utility for broader public health surveillance continues to be explored. NC DETECT data have been used to monitor varicella *in lieu* of mandated reporting and have also been used for a variety of injury-related analyses, from the use of all-terrain vehicles to injuries from specific toys to heat-related injuries. Use of the NC DETECT data for chronic diseases continues to expand. Throughout the development of NC DETECT,

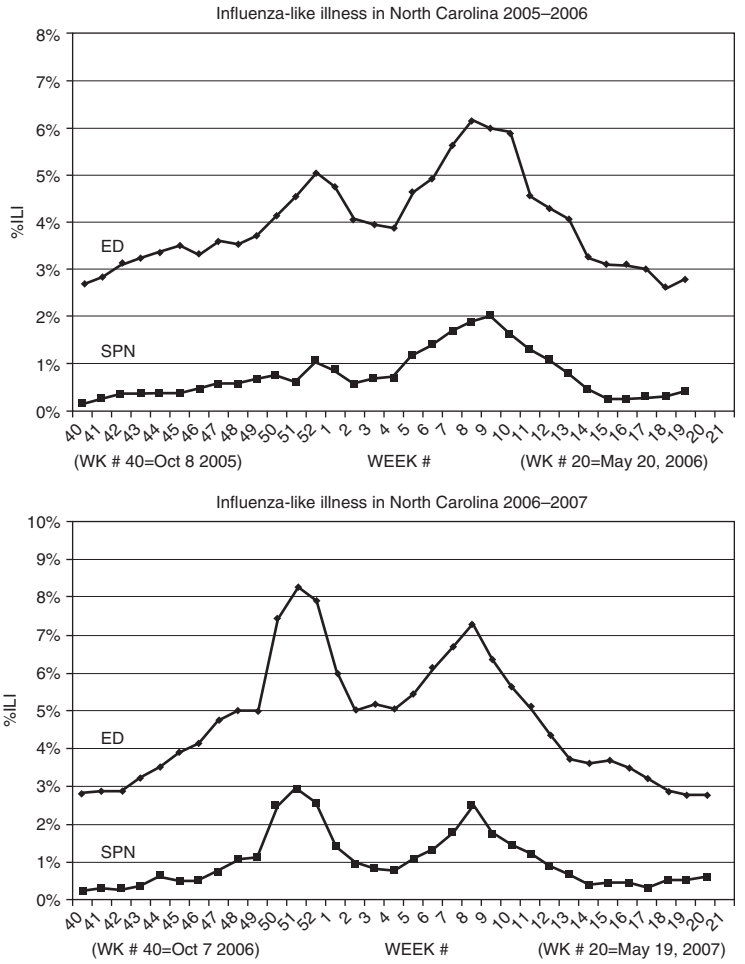



**FIGURE 4** Influenza-like illness in North Carolina, 2005–2007. SPN: 74 volunteer practitioners report weekly their patient workload; using ILI case definition: "fever and cough or sore throat". ED: as of 5/19/2007, 103 hospitals report daily ED visits electronically through the NC DETECT System, using ILI case definition: "ILI cases must include any case with the term "flu" or "influenza" or have at least one fever term and one influenza-related symptom".

leaders from UNC DEM and NC DPH have adhered to the goals of comprehensive, timely, and quality data; strong partnerships; flexibility; and user-centered design.

## 5 LESSONS LEARNED AND CONCLUSIONS

Biosurveillance systems that aim to provide comprehensive population health views need to extend beyond ED chief complaints. The additional ED data elements in NC DETECT, including triage notes, dispositions, and final diagnosis codes, provide opportunities for more efficient case finding, investigation, and follow up. The American Health Information Community (AHIC) Biosurveillance minimum data set aims to establish the ideal

set of data elements for detailed but de-identified surveillance using hospital data, including ED, inpatient, and laboratory data [18]. Leaders involved in the implementation and testing of the AHIC Biosuveillance MDS must be well prepared for the increased data quality vigilance necessary to ensure that this larger data set—that goes far beyond basic demographics and chief complaint—is as accurate and timely as possible for the public health decision-makers relying on it.

### 5.1 Emergency Department Data Collection

Collecting timely, electronic ED data that include clinical data elements, rather than just billing data, is a complicated process. Typically, previous efforts to work with the ED data from a hospital have been limited; therefore, no one really knows what is and is not available or how complete and accurate the data actually are. Bringing a hospital into production with NC DETECT often requires several iterations of test data feeds and programming modifications, primarily because the data must frequently be extracted from multiple hospital information systems. In addition, electronic health records (EHRs) may not store clinical data elements useful for biosurveillance in an easily extractable format, as these data are not normally exchanged between health information systems. EHR vendors must develop systems that store clinical information in discrete data elements so that these data can be used by multiple entities for public health surveillance and research.

Because NC DETECT was designed from the beginning to meet public health data needs beyond bioterrorism surveillance, both administrative and clinical data elements were included from the outset. Although leaders from UNC DEM and NC DPH took an opportunistic approach, accepting the data readily available electronically, the data elements and data sources collected have proven useful beyond original expectations. Within the ED data, triage note is a very valuable data element for a variety of public health surveillance purposes. However, it is not available electronically from all EDs. The data from the poison center calls have provided insight into environmental exposures and community concerns that would not be possible with the ED data alone.

### 5.2 Other Data Sources

The data sources other than ED data in NC DETECT present different challenges. As other organizations collect and store these data and provide only a subset of their information to NC DETECT for biosurveillance, troubleshooting data quality and completeness issues in a timely manner is more difficult. The desire to add novel data sources for biosurveillance continues to grow in North Carolina as it does nationally. Ideally, this process should include an assessment of the data needs of NC DETECT end users and a thorough feasibility assessment. Adding data from less familiar data sources presents challenges of accurate data interpretation. For example, interpreting veterinary laboratory results, including tests for a variety of species, is very different than interpreting human patient lab results, particularly without veterinary medicine expertise on staff.

### 5.3 Data Quality

ED data are notoriously dirty, even by health care data standards. NC DETECT policies require that specific business rules be met before data are available in the production

system. Metadata collected about each data source are extremely helpful in making sense of the data collected in NC DETECT. The metadata allow data quality checks to go beyond the file level (such as, file format, file receipt, and presence of mandatory data elements); each data element is checked for accuracy, timeliness, and appropriate distributions. Examples of typical metadata questions include the following:

- What is the expected percentage of admitted and discharged patients on a given day?
- What is the average daily visit count?

Data checks must be performed using metadata as well as trends. If the data are inaccurate or incomplete from the start, then trends analysis will never be accurate. The metadata also act as the Gold Standard for data quality for several indicators *in lieu* of performing labor-intensive periodic data audits for each data provider. A small data validity audit is in progress for just a few hospitals, which will be comparing the data available in the hospital's electronic ED record for each visit to what is stored in NC DETECT. The goal of this audit is to understand and document the potential data quality issues that arise as dual use data are transmitted and used by disparate systems.

Addressing data quality is an ongoing and never ending effort for NC DETECT. Daily communications occur among UNC DEM, NC DPH, and data providers about data quality issues and effecting improvements to data quality. This issue is complicated by the myriad of stakeholders in the system and the fact that the burden of remedying identified problems often falls back on the data providers. The impact of biosurveillance systems on data providers, both to provide and maintain their data feeds, cannot be underestimated.

### 5.4 Engage Users

The developers of NC DETECT at UNC DEM and NC DPH have been committed to a user-centered, iterative design process that informs how our data are collected, analyzed, and reported. NC DETECT is a biosurveillance system that *requires* a human element. PHEs at the state, regional, and local levels actively use the system everyday for public health surveillance. Because they are familiar and comfortable with the system, they are ready to use it in an emergency situation. Another benefit of involving end users in the design and development of NC DETECT is that they trust the system to provide the information they need. When it does not, they know how and to whom to communicate what changes and improvements are needed.

### 5.5 Security

While North Carolina has mandates for the collection of ED and EMS data for public health use [2], role-based access ensures that users see only the data they need and are authorized to see. The data in NC DETECT belong to NC DPH; all access to the data is through a standardized authorization process and must be approved at the state level. Data use agreements and business associate agreements are used as appropriate and for most access. Aggregate data are more readily shared than visit level data. Balancing privacy/security concerns with the need for public health information is an ongoing challenge.

### 5.6 Conclusions

Timely, flexible public health surveillance tools are crucial for effective preparedness and response. North Carolina has demonstrated that such a system can be built, and used daily, for statewide public health surveillance including biosurveillance. Continuous evaluation of NC DETECT is required to insure a quality, evidence-based system. We continue to strive to meet our goal of a well used and useful system for biosurveillance in North Carolina.

## REFERENCES


1. *Homeland Security Presidential Directive 21,* (2008). http://www.whitehouse.gov/news/releases/2007/10/20071018-10.html.
2. *North Carolina General Statute 130A*, (2008). http://www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_130A.html. Accessed January 17.
3. Henning, K. J. (2004). Overview of syndromic surveillance: what is syndromic surveillance? *MMWR* **53**(suppl), 5–11.
4. Centers for Disease Control and Prevention (2008). (October 23, 2003). *Syndrome Definitions for Diseases Associated with Critical Bioterrorism-associated Agents*, http://www.bt.cdc.gov/surveillance/syndromedef/index.asp. Accessed January 20.
5. Scholer, M. J., Ghneim, G., Wu, S., Westlake, M., Travers, D., Waller, A. E., McCalla, A. and Wetterhall, S. F. (2007). Defining and applying a method for improving the sensitivity and specificity of an emergency department early event detection system. *Proceedings of the 2007 AMIA Annual Symposium*. Chicago, IL, 651–655.
6. Travers, D. A., and Haas, S. W. (2004). Evaluation of Emergency Medical Text Processor, a system for cleaning chief complaint data. *Acad. Emerg. Med.* **11**(11), 1170–1176.
7. Chapman, W. W., Bridewell, W., Hanbury, P., Cooper, G. F., and Bu-chanan, B. G. (2001). A simple algorithm for identifying negated findings and diseases in discharge summaries. *J. Biomed. Inform.* **34**, 301–310.
8. Travers, D. A., Barnett, C., Ising, A., and Waller, A. (2006). Timeliness of emergency department diagnoses for syndromic surveillance. *AMIA Annu. Symp. Proc.* 769–773.
9. Hutwagner, L., Thompson, W., Seeman, G., and Treadwell, T. (2003). Bioterrorism preparedness and response Early Aberration Reporting System. *J. Urban Health* **80**(2 Suppl 1), i89–i96.
10. Heffernan, R., Mostashari, F., Das, D., Karpati, A., Kulldorff, M., and Weiss, D. (2008). Syndromic surveillance in public health practice, New York City. *Emerg. Infect. Dis.* **10**. [serial on the Internet]. 2004 May http://www.cdc.gov/ncidod/EID/vol10no5/03-0646.htm. Accessed January 18.
11. Ising, A., Li, M., Deyneka, L., Barnett, C., Scholer, M., and Waller, A. (2007). Situational Awareness using web-based annotation and custom reporting. *Adv. Dis. Surveill.* **4**, 167.
12. MacFarquhar, J. (2008). Hospital-based public health epidemiology program: a novel approach to public health in NC. *Webinar Symposium Series on Public Health Preparedness, NC Center for Public Health Preparedness*. Chapel Hill, NC. December 2006. http://nccphp.sph.unc.edu/symposium/HospEpiDec-06.pdf, Accessed January 18.
13. Davis, M. V., Temby, J. R. E., MacDonald, P., and Rybka, T. P. (2008). *Evaluation of Improvements in North Carolina Public Health Capacity to Plan, Prepare and Respond to Public Health Emergencies*, North Carolina Center for Public Health Preparedness, The North Carolina Institute for Public Health, September 2004. http://nccphp.sph.unc.edu/hurricane_10_19_04.pdf, Accessed January 18.

14. Barnett, C., Deyneka, L., and Waller, A. E. (2006). Post-Katrina Situational Awareness in North Carolina. *Adv. Dis. Surveill.* **2**, 142.
15. FDA News (2008). *FDA Warns Consumers Not to Eat Certain Jars of Peter Pan Peanut Butter and Great Value Peanut Butter*, Feburary 14, 2007. http://www.fda.gov/bbs/topics/NEWS/2007/NEW01563.html. Accessed January 18.
16. FDA News (2008). *FDA Issues Nationwide Warning to Consumers About Risk of Botulism Poisoning From Hot Dog Chili Sauce Marketed Under a Variety of Brand Names*, July 18, 2007. http://www.fda.gov/bbs/topics/NEWS/2007/NEW01669.html. Accessed January 18.
17. North Carolina Department of Health and Human Services Press Release (2008). *Heat Wave Emergency Department Monitoring Yields Surprising Results*, http://www.ncdhhs.gov/pressrel/8-28-07.htm. Accessed January 18.
18. *Population Health and Clinical Care Connections Workgroup–Archives*, (2008). October 20, 2006. http://www.dhhs.gov/healthit/ahic/population/pop_archive.html#16. Accessed January 18.

## FURTHER READING

Lombardo, J. S., and Buckeridge, D. L., Eds. (2007). *Disease Surveillance: A Public Health Informatics Approach*, Wiley-Interscience, Hoboken, NJ.

http://www.syndromic.org, (2008).

http://www.NCDETECT.org, (2008).

# ESSENCE: A PRACTICAL SYSTEMS FOR BIOSURVEILLANCE

JULIE A. PAVLIN

*Uniformed Services University of the Health Sciences, Bethesda, Maryland*

KENNETH L. COX

*USAF, MC, SFS TRICARE Management Activity (TMA), Office of the Assistant Secretary of Defense (Health Affairs), Falls Church, Virginia*

## 1 BACKGROUND

In 1999, the Department of Defense Global Emerging Infections Surveillance and Response System (DoD-GEIS) piloted a disease surveillance system using data collected

at outpatient visits in the national capital area. This system, the electronic surveillance system for the early notification of community-based epidemics (ESSENCE), collected diagnostic information from International Classification of Diseases, 9th Revision (ICD-9) codes entered after outpatient and emergency room visits at all military treatment facilities (MTFs) in order to detect and track potential infectious disease outbreaks. With advances in knowledge of the utility of newly available data sources, statistical programs for aberration detection, and visualization techniques, the ESSENCE program has expanded to incorporate medical information from all MTFs worldwide and has developed partnerships with universities and government agencies to coordinate population health information for military and civilian public health agencies across the United States.

Publications before the US anthrax mail attacks in 2001 discussed how public health infrastructure had declined over time and decried our nation's lack of readiness for an emergency relating to a lethal disease outbreak [1–3]. Besides the intentional release of anthrax spores in the US mail, natural disease outbreaks, such as hantavirus pulmonary syndrome [4], West Nile virus [5], monkeypox [6], SARS [7], and avian influenza [8], have caused considerable concern for US security. With new ideas proliferating for ways to more rapidly detect and monitor the spread of disease outbreaks, the DoD-GEIS held a symposium in May 2000 to share experiences and foster efficient progress in creating innovative, responsive surveillance systems [9]. Partnerships formed consequent to this meeting have resulted in enhanced methods for disease monitoring that continue to be used and improved in both the military and civilian sectors.

### 1.1 Traditional Surveillance Practices

Traditionally, most infectious disease surveillance systems have relied on laboratory reporting for a list of diseases of public health importance. As in the civilian community, military health providers are required to report any cases of these diseases, whether hospitalized or not, to the public health officials on the military installation as well as the local public health department. Unfortunately, many health care providers are unaware of the notifiable disease list, or whom to contact, or cannot find the time to report; therefore, most reporting is done by laboratory staff after confirmation of a positive test result. However, many diseases are not diagnosed in the laboratory, either because there is no test available or because a specimen is not taken. Reports on completeness and timeliness of active reporting of *hospitalized* notifiable conditions in the military to the respective service's reporting system show rates of 57% in the Army, 30% in the Navy, and 31% in the Air Force for 2003 based on the ICD-9 codes recorded as diagnoses upon discharge of the patient from the hospital [10–12]. In addition, the cases were not reported in a timely fashion, with 15% of Navy, 69% of Army, and 80% of Air Force cases reported within one month.

### 1.2 Other DoD Surveillance Systems

To supplement reportable disease surveillance, the DoD initiated special surveillance programs for high-risk populations or diseases. The Air Force Institute of Operational Health (now known as the US Air Force School of Aerospace Medicine (USAFSAM))

has been operating a military global influenza surveillance program since 1976 [13, 14]. This system now covers all three services as well as local residents in areas where DoD overseas research activities occur and collects respiratory specimens for viral isolation and typing. The Naval Health Research Center operates a febrile respiratory illness surveillance program at all basic training sites [15]. This system collects symptom data on trainees and calculates when rates of respiratory illness exceed the expected rate in order to initiate preventive measures. The Army performs acute respiratory disease (ARD) surveillance at all basic combat training sites [16]. This program monitors the incidence of positive streptococcal cultures in the trainee population and allows the local preventive medicine staff to decide whether to initiate or expand penicillin prophylaxis.

The DoD maintains the Defense Medical Surveillance System (DMSS) [17], which integrates a wide range of health event-related data on all military beneficiaries. The DMSS includes individual demographic information, outpatient/inpatient events, immunization status, and other data for care provided within all permanent MTFs worldwide as well as from the TRICARE purchased care network. As most of these data are received monthly, DMSS has not been useful for near-real-time surveillance purposes, but plays a critical role in retrospective analyses.

The DoD also monitors deployed troops who are routinely in areas with high rates of endemic diseases and at risk for deliberate attacks involving biological agents. Most deployed medical units capture health event data using electronic patient encounter modules. These data, which include ICD-9 codes as assigned by the attending health care provider, and other related information in both structured-note and free-text formats are forwarded at least daily to the Joint Medical Workstation (JMeWS). Analysts monitor trends in various groupings of diseases and nonbattle injuries (DNBI) on at least a weekly basis. During periods of high threat, the frequency of reporting and analysis is on a daily basis, and more focused category definitions related to biological attacks are activated. Additional deployed health event data are available from newer systems including the joint patient tracking application (JPTA) and the US TRANSCOM Regulating and Command and Control Evacuation System ($TRAC^2ES$). Both of these systems support direct clinical care of casualties as they move between different medical treatment facilities, both inside and outside of the military theater of operations.

The Armed Forces Institute of Pathology (AFIP) includes a full medical examiners office, which maintains a DoD mortality registry. AFIP performs full autopsies and extensive investigations on all service members who die while on active duty with special emphasis on identifying sentinel infectious deaths.

The DoD established the Department of Defence serum repository (DoDSR) in 1989 for the purpose of storing serum specimens that remained following mandatory HIV testing within the active and reserve components of the Army and Navy [18–20]. Later, the mission expanded to include the collection and storage of specimens collected before and after operational deployments, for example, Operation IRAQI FREEDOM, and to include Air Force, US Coast Guard, and Federal civilian employee specimens. The DoDSR currently houses more than 40 million specimens and continues to grow by approximately 2.3 million specimens per year. The availability of serial serologic specimens throughout an individual's career, as well as relevant demographic, occupational, and medical information, within the DMSS enables the DoDSR to make significant contributions to clinical and seroepidemiologic investigations.

### 1.3 Need for Improved Surveillance

Despite the previously mentioned surveillance programs for specific illnesses and populations, a real-time, comprehensive system to determine disease status for all military beneficiaries was still needed. With increasing amounts of electronic health data available, to include early diagnostic information, it became feasible to develop ways to visualize and analyze multiple health data streams in novel and potentially useful ways. New surveillance systems such as ESSENCE, initially envisioned for early outbreak detection and later adapted for outbreak investigation aids, situational awareness, temporal and geographic disease tracking, and other augmentations, started to provide the immediate knowledge that public health officials, decision makers, and military leaders required.

## 2 ESSENCE RESEARCH AND DEVELOPMENT

Many academic, public health, commercial, and government institutions have designed what is termed *syndromic surveillance systems* to have more timely knowledge of disease impact in communities. "Syndromic surveillance" typically refers to the use of routinely collected early or prediagnostic health information for timely disease surveillance. It is defined by secondary use of early or prediagnostic data and a focus on prospective disease surveillance and timely outbreak detection. Syndromic systems typically use electronically collected and disseminated data, but can include paper-based, manual methods such as daily reviews of chief complaint logs.

On the basis of the work done by the New York City Department of Health and Mental Hygiene using prescriptions of antidiarrheal medications and number of stool samples submitted for testing to detect gastrointestinal outbreaks [21] and on the basis of the use of coded 911 calls to track influenza outbreaks [22], the DoD-GEIS investigated the use of ICD-9 codes to detect potential infectious disease and bioterrorism outbreaks in the greater Washington, DC area [23]. This project resulted in the creation of the ESSENCE surveillance system.

### 2.1 History of ESSENCE Development

ESSENCE initially relied on the use of ICD-9 codes, grouped into syndromes such as respiratory, gastrointestinal, febrile, and neurological illnesses, to detect abnormal changes in disease incidence rates. At every MTF, the health care provider codes each outpatient and emergency room visit with up to four ICD-9 codes that are recorded electronically. These codes are entered at or near the time of patient visit, but transfer to a central facility could be delayed by 2–3 days or longer. (This situation is changing with the implementation of the Armed Forces Health Longitudinal Technology Application (AHLTA) as the new enterprise health information system. With AHLTA, the data are transmitted in real time, as soon as the provider closes out the record, to a central data repository. The analyzed data are available to military public health officials on a password protected website.) Since its inception in 1999, ESSENCE has expanded from the DC region to all MTFs worldwide and has undergone numerous revisions to improve usefulness, data quality, and algorithm sensitivity and specificity.

Early in the development of the ESSENCE project, DoD-GEIS and the Johns Hopkins University Applied Physics Laboratory (JHU/APL) developed a collaboration to work jointly on a syndromic surveillance system for the Washington, DC region. JHU/APL

had already developed a system in Maryland using nursing home illness cases, medicare billing information, and civilian hospital emergency room chief complaints. With the combination of the two systems, the new ESSENCE II provided a more representative view of the region. Together, the DoD-GEIS and JHU/APL team received a grant from the Defense Advanced Research Projects Agency (DARPA) to further develop a prototype disease surveillance test bed and to evaluate new data sources [24].

Under the DARPA program, ESSENCE II expanded to include over-the-counter (OTC) pharmacy sales, school absenteeism, medication prescriptions, laboratory test orders, and veterinary clinic data in the Washington, DC region. The system also included improved statistical methods to detect both temporal and spatial anomalies and advanced web-based interfaces for the user. ESSENCE II integrated military and civilian data and became the first system to make both available for daily disease surveillance [24].

Development and testing of ESSENCE continued with the ESSENCE III project, funded by the Defense Threat Reduction Agency (DTRA), to evaluate different syndromic surveillance systems in the Albuquerque, NM region. BioNet, a cooperative program between DTRA and the Department of Homeland Security, then selected San Diego as a pilot city to test how to improve detection and event characterization of a biological attack. At the same time, the Joint Services Installation Pilot Project (JSIPP) expanded chemical, biological, and radiological detection and response capabilities at nine military installations and the surrounding communities. As part of JSIPP and BioNet, ESSENCE IV was created to use summary data from military emergency room and outpatient visits, pharmacy prescriptions, procedure codes, and civilian hospital emergency room chief complaints together in an integrated system with advanced on-line analysis capabilities. In addition, depending on the data sources available at each location, sets of daily records of school absenteeism, school nurse visits, ambulance runs, nurse advice calls, and OTC pharmacy sales were also integrated, and their surveillance utility was evaluated. The time series plot in Figure 1 includes a sharp early January increase in case counts representing an outbreak detected by ESSENCE IV.

### 2.2 Lessons Learned

During the initial expansion of ESSENCE, extensive evaluations were conducted through research of data sources and statistical techniques and surveys of users. The results of the evaluations were disseminated to all stakeholders. The major conclusions included the need for validation of data sources for both accuracy and usefulness, utility for public health use beyond bioterrorism detection, simplicity of web-based interaction, portability between different information technology systems, and designated funding for continuation of programs. Table 1 summarizes these findings. Data sources need to be validated before inclusion into any syndromic surveillance system. The validation does not need to be extensive, but should include, at a minimum, comparison between an existing, evaluated surveillance system and other data sources being included in the syndromic surveillance system.

### 2.3 Strengths and Limitations

There are limitations to any surveillance system, and syndromic surveillance systems are no different. It is important to clearly state the goals of a system being developed to decrease false expectations. Syndromic systems like ESSENCE should augment existing

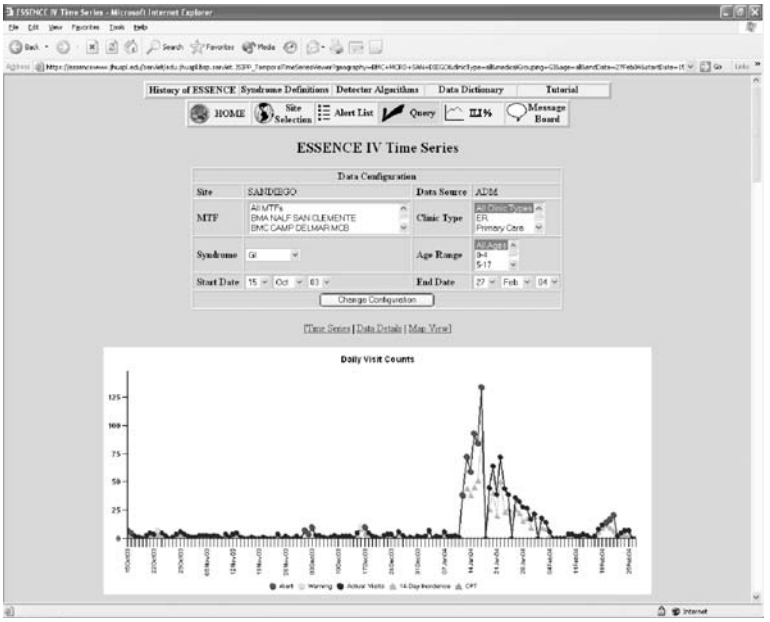



**FIGURE 1** Gastrointestinal outbreak in military personnel depicted in the ESSENCE IV system.

systems by extending the ability to detect and track disease outbreaks in a community. Some of the strengths and limitations found in ESSENCE development and piloting are listed in Table 2.

## 3 IMPLEMENTATION

A surveillance system has value only if people use it. ESSENCE has clearly demonstrated its value as a key tool in the practice of military public health. Still, it is important to establish policy explaining this value and identifying performance expectations.

### 3.1 Recent ESSENCE Enhancements

One of the best ways to gain user acceptance and loyalty is to provide a product that meets the user's needs and minimizes additional work. DoD has redesigned ESSENCE based on user feedback. The most common criticism of earlier versions of ESSENCE was the inability of the local user to access the personal identifying information of individuals contributing to an alert or alarm. This made investigation difficult and time consuming. Consequently, the new ESSENCE allows role-based access at the local level to protected health information [supervisor approved, following Health Insurance Portability and Accountability Act (HIPAA) guidelines]. Since this change, the local military public health practitioner is instantly able to access the name and other personal identifying information. The system will also map outpatient diagnoses against the current tri-service reportable medical events list, allowing local staff to promptly investigate these events. Additionally, automated e-mail and mobile phone alerts of possible disease outbreaks

**TABLE 1 Recommendations for Evaluation of New Disease Surveillance Systems**

Validate data sources
- Ensure that any "gold standard" comparison sources are truly gold standard. It is possible that the standard could be less accurate than the new data source being tested
- The data source should be evaluated across different types of outbreaks. For example, a more severe disease indicator such as ambulance dispatches might be an indicator during influenza season, but may not show any abnormality during a gastrointestinal outbreak
- Before eliminating or including a data source, the elements that make up the syndrome groups should be manipulated to determine the best groupings possible for the population and the database
- Many disease outbreaks are small and of low impact. Data sources that detect these outbreaks are not necessarily unreliable as an indicator of disease rates

Use reliable and user-preferred data sources—most often from interactions with medical care providers
- Emergency room chief complaints and diagnostic information from outpatient visits are the most useful. Ambulance runs provide information slightly earlier, but may miss less severe outbreaks that do not require ambulance transport
- Earlier alerting data such as OTC sales and school absenteeism are good collaborating sources, but cannot be relied upon for confirmation of an outbreak

Evaluate data sources from specific populations for their contribution to the overall surveillance
- Representative populations are best for determining disease rates in large geographic areas, but special subsets of the population can provide critical information if properly utilized

Evaluate timeliness and representativeness
- A new data source should provide population information previously unavailable at low cost and should be timely enough to improve the current surveillance system
- Even if the initial purpose of the system is for bioterrorism detection, ensure the surveillance system can recognize and assist with response to other public health infectious disease outbreaks
- Data sources should also be evaluated for *any* potential public health use, including noninfectious disease related ones. This will make the overall system more cost effective and sustainable

Allow link to identifiers within public health and privacy laws
- Rapid access to identifying information can assist with a public health emergency and in finding and tracking reportable disease events

User interfaces should emphasize simplicity while still allowing advanced users access to manipulate variables
- For example, provide the ability to manipulate ICD-9 codes or text words in syndrome groups and to select algorithms and change their sensitivity

Ensure portability of systems to new locations for ease of expansion
- Information technology support should be obtained in the beginning to ensure ease of transitions later on

Out-year funding or designation of the organization that will provide financial and personnel support after the initial program ends needs to be determined early and continually updated throughout the life of the program
- Without dedicated support, no one will invest the time and commitment a successful system needs

**TABLE 2 Strengths and Limitations of ESSENCE**

| | |
|---|---|
| Strengths | Tracking of community-wide disease outbreaks, both locally and across geographic regions |
| | Quick method to find most up-to-date information on general disease status of a community (situational awareness during threat of outbreak) |
| | Ability to link identifiers if needed for outbreak investigation |
| | Increased ability to find and investigate notifiable diseases |
| | Sharing information with local public health officials |
| Limitations | Inability to detect small outbreaks for some disease syndromes |
| | Lag-time for some data acquisition can result in outbreak detection occurring after optimal time for intervention |
| | False alarms occur and detract from user confidence |
| | Lack of trust that data reflects true health status since acquired early in course of illness |
| | Complex detection algorithms can be difficult to interpret |

are now available. This new version of ESSENCE was fielded on September 28, 2006, by the TRICARE Management Activity Executive Information and Decision Support (EIDS) (now known as the TMA Defense Health Services Systems (DHSS)) office.

### 3.2 Monitoring Requirements

A Health Affairs policy memo published January 17, 2007 identifies ESSENCE as an essential component of military installation protection and a key part of the US national public health surveillance system [25]. The Services must have appropriately trained public health or preventive medicine professionals monitoring ESSENCE at each military installation. These individuals will routinely monitor ESSENCE alerts and associated graphs and data tables for any MTF within their direct jurisdiction as well as other nearby military installations.

The monitoring frequency will be at least once each routine work day, but will increase to include weekends and holidays during periods of increased threat, for example, specific local terrorist threat, World Health Organization/national pandemic influenza alert phase 5 or 6, and so on. There must be active communication between the ESSENCE monitors and the local public health emergency officer [26]. The installation medical professionals responsible for public health must maintain a strong relationship with the local civilian public health office, advising them of potential outbreaks and forwarding reportable medical events information as required by local, county, or state law.

### 3.3 Future ESSENCE Enhancements

In keeping with the lessons learned by DoD and other syndromic surveillance experts across the country, a number of enhancements are planned for the near future. For instance, potential complementary data streams are undergoing evaluation for possible inclusion. These include laboratory orders and results, radiology orders and results, and chief complaints from primary and emergency care settings. The DoD continues to collaborate closely with JHU/APL, the Centers for Disease Control and Prevention's BioSense program, and other national research and development centers in order to identify the best data sources and statistical analytical procedures.

## 4 CONCLUSIONS

In development and use of a surveillance program such as ESSENCE, it is most important to first determine the overriding purpose of such a system. The purpose of a surveillance system determines which attributes are most important. To monitor long-term trends in disease rates or to evaluate the effectiveness of a public health prevention program, accuracy is more important than timeliness. However, to decrease the time needed to detect an outbreak or to monitor its spread, the rapid acquisition and analysis of surveillance data become a priority, as long as it can be done with enough correct information to be useful.

Rapid access to disease surveillance data can provide more than an early indication. Information in this system, such as geographic location of the patients, can assist in a more in-depth outbreak investigation. Once detected, it can be used to monitor the rate and spread of the outbreak, and the effectiveness of control measures. It can also provide situational awareness, letting health officials know the general status of acute disease in a population. And finally, surveillance information can be used by decision makers to determine at-risk populations, decide how to best allocate resources, and provide the public information on how to decrease their risk.

## REFERENCES

1. O'Toole, T. (2001). Emerging illness and bioterrorism: implications for public health. *J. Urban Health* **78**(2), 396–402.
2. Inglesby, T., Grossman, R., and O'Toole, T. (2001). A plague on your city: observations from TOPOFF. *Clin. Infect. Dis.* **32**(3), 435–436.
3. Khan, A. S., and Ashford, D. A. (2001). Ready or not–preparedness for bioterrorism. *N. Engl. J. Med.* **345**(4), 287–289.
4. Centers for Disease Control and Prevention. (1993). Outbreak of hantavirus infection–Southwestern United States. *Morb. Mortal. Wkly. Rep.* **42**, 495–496.
5. Fine, A., and Layton, M. (2001). Lessons from the West Nile viral encephalitis outbreak in New York City, 1999: implications for bioterrorism preparedness. *Clin. Infect. Dis.* **32**(2), 277–282.
6. Reed, K. D., Melski, J. W., Graham, M. B., Regnery, R. L., Sotir, M. J., Wegner, M. V., Kazmierczak, J. J., Stratman, E. J., Li, Fairley, J. A., Swain, G. R., Olson, V. A., Sargent, E. K., Kehl, S. C., Frace, M. A., Kline, R., Foldy, S. L., Davis, J. P., and Damon, I. K. (2004). The detection of monkeypox in humans in the Western Hemisphere. *N. Engl. J. Med.* **350**(4), 342–350.
7. Peiris, J. S., Yuen, K. Y., Osterhaus, A. D., and Stohr, K. (2003). The severe acute respiratory syndrome. *N. Engl. J. Med.* **349**(25), 2431–2441.
8. Fauci, A. S. (2006). Pandemic influenza threat and preparedness. *Emerg. Infect. Dis.* **12**(1), 73–77.
9. Pavlin, J. A., Mostashari, F., Kortepeter, M. G., Hynes, N. A., Chotani, R. A., Mikol, Y. B., Ryan, M. A. K., Neville, J. S., Gantz, D. T., Writer, J. V., Florance, J. E., Culpepper, R. C., Henretig, F. M., and Kelley, P. W. (2003). Innovative surveillance methods for rapid detection of disease outbreaks and bioterrorism: results of an interagency workshop on health indicator surveillance. *Am. J. Public Health* **93**(8), 1230–1235.
10. Army Medical Surveillance Activity (now known as the Armed Forces Health Surveillance Center). (2004). Completeness and timeliness of reporting hospitalized notifiable conditions, active duty servicemembers, US Army medical treatment facilities, 1995–2003. *Med. Surveill. Monthly Rep.* **10**(4), 9–13.

11. Army Medical Surveillance Activity (now known as the Armed Forces Health Surveillance Center). (2004). Completeness and timeliness of reporting hospitalized notifiable conditions, active duty servicemembers, US Naval medical treatment facilities, 1995–2003. *Med. Surveill. Monthly Rep.* **10**(4), 14–17.
12. Army Medical Surveillance Activity (now known as the Armed Forces Health Surveillance Center). (2004). Completeness and timeliness of reporting hospitalized notifiable conditions, active duty servicemembers, US Air Force medical treatment facilities, 1995–2003. *Med. Surveill. Monthly Rep.* **10**(4), 18–21.
13. Williams, R. J., Cox, N. J., Regnery, H. L., Noah, D. L., Khan, A. S., Miller, J. M., Copley, G. B., Ice, J. S., and Wright, J. A. (1997). Meeting the challenge of emerging pathogens: the role of the United States Air Force in global influenza surveillance. *Mil. Med.* **162**(2), 82–86.
14. Canas, L. C., Lohman, K., Pavlin, J. A., Endy, T., Singh, D. L., Pandey, P., Shrestha, M. P., Scott, R. M., Russell, K. L., Watts, D., Hajdamowicz, M., Soriano, I., Douce, R. W., Neville, J., and Gaydos, J. C. (2000). The department of defense laboratory-based global influenza surveillance system. *Mil. Med.* **165**(7, Suppl. 2), 52–56.
15. Gray, G. C., Callahan, J. D., Hawksworth, A. W., Fisher, C. A., and Gaydos, J. C. (1999). Respiratory diseases among US military personnel: countering emerging threats. *Emerg. Infect. Dis.* **5**(3), 379–385.
16. Army SG policy memo DASG-PPM-NC (40), (2001). *Army Acute Respiratory Disease Surveillance Program*, 18 Jul 2001.
17. Department of Defense Directive 6490.2, (2004). *Comprehensive Health Surveillance*, 21 Oct 2004.
18. 10 US Code sec 1074f, 2007.
19. Public Law 105–85sec 765, 18 Nov 1997.
20. Department of Defense Instruction 6490.03, (2006). *Deployment Health*, 11 Aug 2006.
21. Miller, J. R., and Mikol, Y. (1999). Surveillance for diarrheal disease in New York City. *J. Urban Health* **76**, 388–390.
22. Mostashari, F., Fine, A., Das, D., Adams, J., and Layton, M. (2003). Use of ambulance dispatch data as an early warning system for communitywide influenzalike illness, New York City. *J. Urban Health* **80**(2, Suppl. 1), i43–i49.
23. Lewis, M. D., Pavlin, J. A., Mansfield, J. L., O'Brien, S., Boomsma, L. G., Elbert, Y., and Kelley, P. W. (2002). Disease outbreak detection system using syndromic data in the greater Washington, DC area. *Am. J. Prev. Med.* **23**(3), 180–186.
24. Lombardo, J., Burkom, H., Elbert, E., Magruder, S., Lewis, S. H., Loschen, W., Sari, J., Sniegoski, C., Wojcik, R., and Pavlin, J. (2003). A systems overview of the electronic surveillance system for the early notification of community-based epidemics (ESSENCE II). *J. Urban Health* **80**(2, Suppl. 1), i32–i42.
25. Assistant Secretary of Defense for Health Affairs. Policy memorandum (2007). *New Electronic System for the ESSENCE Medical Surveillance System and Monitoring Requirements*, published 17 Jan 2007.
26. Department of Defense Directive 6200.3, (2003). *Emergency Health Powers In Military Installations*, 12 May 2003.

## FURTHER READING

Advances in Disease Surveillance Journal at www.isdsjournal.org, 2006.

Bravata, D. M., McDonald, K. M., Smith, W. M., Rydzak, C., Szeto, H., Buckeridge, D. L., Haberland, C., and Owens, D. K. (2004). Systematic review: surveillance systems for early detection of bioterrorism-related diseases. *Ann. Intern. Med.* **140**, 910–922.

Buehler, J. W., Hopkins, R. S., Overhage, J. M., Sosin, D. M., and Tong, V. (2004). Framework for evaluating public health surveillance systems for early detection of outbreaks. *Morb. Mortal. Wkly. Rep.* **53**(RR05), 1–11.

Centers for Disease Control and Prevention. (2004). Syndromic surveillance: reports from a national conference, 2003. *Morb. Mortal. Wkly. Rep.* **53**(Suppl, 1–268).

Centers for Disease Control and Prevention. (2005). Syndromic surveillance: reports from a national conference, 2004 *Morb. Mortal. Wkly. Rep.* **54**(Suppl, 1–212).

Information on syndromic surveillance and the International Disease Surveillance Society at www.syndromic.org, 2006.

Information on the new military electronic health record at www.ha.osd.mil/ahlta, 2006.

Pavlin, J. A. (2005). Medical surveillance for biological terrorism agents. *Hum. Ecol. Risk Assess.* **11**(3), 525–537.

Pavlin, J. A., and Kelley, P. W. (2005). Department of defense global emerging infections system programs in biodefense. In *Biological Weapons Defense: Infectious Diseases and Counterterrorism*, L. E. Linder, F. J. Lebeda, and G. W. Korch, Eds. Humana Press, Totowa, NJ, pp. 361–385.

Wagner, M. M., Moore, A. W., and Aryel, R. M., Eds (2006). *Handbook of Biosurveillance*. Elsevier Academic Press, Burlington, MA.

# BIODEFENSE PRIORITIES IN LIFE-SCIENCE RESEARCH: CHEMICAL THREAT AGENTS

DAVID A. JETT

*National Institutes of Health/National Institute of Neurological Disorders and Stroke, Bethesda, Maryland*

GENNADY E. PLATOFF JR.

*National Institutes of Health/National Institute of Allergy and Infectious Diseases, Bethesda, Maryland*

## 1 BACKGROUND

The attacks of September and October of 2001 have resulted in heightened awareness of the vulnerability of the United States civilian population to terrorist groups or individuals armed with unconventional weapons. While most of the attention has been given to biological agents, the civilian threat spectrum encompasses radioactive, explosive, and

chemical weapons as well. Chemicals are particularly attractive to terrorists because they are relatively inexpensive and easy to obtain, and have the potential to cause mass casualties when used in a variety of scenarios. Unlike biological and radiological threats, there have actually been several recent chemical attacks that have resulted in mass casualties. For example, sulfur mustard and nerve agents were used against Iraqi Kurdish villages in the late 1980s, and more recently, nerve agents were used by the Japanese cult organization Aum Shinrikyo in two separate attacks against civilians in Japan [1, 2]. Not only does this stress the importance of increasing efforts to prepare for future chemical attacks in the United States, but it also provides the opportunity to analyze these events to learn about potential gaps in our response capabilities.

Chemical threat agents can be categorized on the basis of the target tissues and types of primary acute effects they produce (Table 1) [3]. The traditional chemical warfare agents (CWAs) developed during the first and second World Wars include the organophosphorus

**TABLE 1 Examples of Chemical Warfare Agents and Toxic Industrial Chemicals**

| Type | Common Name (Symbol) | Time to Onset of Initial Symptoms | Acute Effects |
|---|---|---|---|
| Nerve agents | Tabun (GA) | Seconds to minutes | Miosis, anxiety, confusions, excess secretions, muscle fasciculations, bronchoconstriction, paralysis, cardiorespiratory depression, convulsions and seizures, coma, and death |
| | Sarin (GB) | Seconds to minutes | |
| | Soman (GD) | Seconds to minutes | |
| | Cyclosarin (GF) | Seconds to minutes | |
| | VX | Minutes | |
| Vesicants or blister agents | Sulfur mustard (H and HD) | 4–6 h | Tearing, burning eyes, rhinorrhea, sneezing, cough, erythema, corneal damage, dyspnea, pulmonary edema, and vesication |
| | Sulfur mustard-T mixture (HT) | 4–6 h | |
| | Nitrogen mustard (HN-1, 2 or 3) | 4–6 h | |
| | Lewisite and other arsenicals (L) | Immediate | |
| Pulmonary (choking agents) | Phosgene (CG) | Immediate irritant effects; pulmonary edema 4–48 h postexposure | Cough, dyspnea, pulmonary edema, and respiratory failure |
| | Chlorine (Cl) | Immediate irritant effects; pulmonary edema in 2–4 h | |
| | Diphosgene (DP) | Similar to CG | |
| Blood agents (cellular poisons) | Hydrogen cyanide (AC) (vapor and liquid) | <1 min (persistence <1 h) | Convulsions, hemolysis, coma, respiratory and renal failure, bradycardia, and cardiac arrest |
| | Cyanogen chloride (CK) (vapor) | <1 min (nonpersistent) | |

(OP) nerve agents such as sarin and VX, and the mustard vesicating agents. As a consequence of previous state-sponsored CWA programs, several stockpiles remain around the world. A terrorist group could illegally obtain or manufacture traditional CWAs and use them as weapons of terror. The United States also produces and uses over 80,000 chemicals, many of which are highly toxic and lethal at relatively low doses. Chemical agents in this broad category include the toxic industrial chemicals (TICs) manufactured and stored in large volume at industrial facilities, and transported across the nation for various uses. The threat from CWAs is mitigated by restricted access, difficulty in synthesis of purified agent, and international treaties against their use. But the TICs are not regulated as strictly, and many chemicals are readily available or stored in large enough amounts to pose a serious threat to human health if released by accident, natural disaster, or by a deliberate act of sabotage to manufacturing plants, storage sites, or transport vehicles. According to a 2003 report published by the General Accounting Office [4], the US Environmental Protection Agency (EPA) has identified 123 chemical plants in the United States where a terrorist attack or accident could potentially expose more than 1 million people to a cloud of toxic gas. Unfortunately, there are also examples of industrial accidents with chemicals, such as the deadly incident in Bhopal, India, where methyl isocyanate was released from an industrial storage tank in 1984 killing 5,000 people and injuring thousands more, some with long-term health effects [5], and the more recent fatal accidents involving chlorine gas releases during transportation in the United States [6]. Chemical plants are also vulnerable to natural disasters such as the recent hurricanes Katrina and Rita [7]. Many are not built to withstand high wind and water, which may be significant because of recent trends in extreme weather.

The US military has developed countermeasures to protect the war fighter from a chemical attack on the battlefield, but many of these are not well suited for civilian chemical terrorism scenarios. Protective clothing, gas masks, and prophylactic drugs used by the military can be effective with advanced preparation, but a chemical attack against civilians or accident is likely to come without warning. Requirements for an effective response to a civilian chemical attack or large-scale accident or natural disaster include (i) postexposure treatments that are effective within an often short therapeutic time window, (ii) drugs and devices that can be used by medical personnel at the scene of the event or in a prehospital setting to treat many victims, (iii) drugs and devices that are appropriate for a diverse population including pediatric and elderly victims, and individuals with preexisting medical conditions, and (iv) rapid and effective diagnostic technologies to determine the chemical agent and pathophysiology. Some available treatments for chemicals that affect cellular respiration (e.g. cyanide) or the nervous system (e.g. nerve agents) have dangerous side effects and a short therapeutic window. Postexposure treatments for chemicals that affect the respiratory system, skin, and eyes are largely limited to supportive therapy and alleviation of symptoms. To address potential gaps in our medical emergency preparedness, and at the request of the US Department of Health and Human Services (DHHS), the National Institutes of Health (NIH) developed the "NIH Strategic Plan and Research Agenda for Medical Countermeasures Against Chemical Threats" for the development of improved medical countermeasures that could be used in the case of chemical terrorist attack or accident [3]. The plan focuses on therapeutics and diagnostics for chemicals that affect the nervous system; respiratory tract; skin, eyes, and mucous membranes; and cellular respiration. Much of the information

in this article has been obtained and paraphrased in some cases from the NIH Strategic Plan, which was authored in part by the authors of this article.

The implementation of the NIH Strategic Plan was established through the Countermeasures Against Chemical Threats (CounterACT) Research Program in fiscal year 2006 to develop new and improved diagnostic technologies and therapies for conditions caused by chemicals that could be used in a terrorist attack or released by accident http://www.ninds.nih.gov/funding/research/counterterrorism/index.htm. The program includes a network of academic, private, and federal laboratories funded through large research centers of excellence, individual research projects, small business grants, and targeted contracts. The network conducts basic, translational, and clinical research aimed at the discovery and/or identification of better therapeutic and diagnostic medical countermeasures against chemical threat agents, and the movement of promising products through the regulatory process. Research areas supported within this program include the development and validation of *in vitro* and animal models for efficacy screening of compounds, efficacy screening of compounds using these models, advanced efficacy and preclinical studies with appropriate animal models including nonhuman primates using current Good Laboratory Practices (cGLPs), and clinical studies, including clinical trials with new drugs.

## 2 OVERVIEW OF THREATS AND SOLUTIONS

### 2.1 Chemicals Affecting the Nervous System

Several chemical agents of highest priority target the nervous system, including some highly toxic insecticides and rodenticides, and the OP nerve agents that have been used as chemical weapons. The OP nerve agents belong to a chemically diverse group of organic compounds, which have in common at least one carbon atom bound to a phosphorous atom. They are sometimes referred to as *nerve gases* because of the high volatility of some of the specific agents, but in fact they are clear colorless liquids at room temperature. The OP nerve agents were synthesized during World War II by the Nazis to be used as CWAs against the allied forces. They are closely related to the OP pesticides that were also being developed during that time. Traditional OP nerve agents fall into two groups, the G-series and the V-series, based on their chemical and physical properties. The G-series nerve agents include GA (tabun), GB (sarin), GD (soman), and others. These are volatile liquids at room temperature that can be deadly when inhaled as a vapor or from percutaneous exposure to the vapor. V-series agents (VX and others) have a consistency similar to oil and have low volatility. V-series agents can remain on clothing and other surfaces for a long time and pose more of a risk from dermal exposure or by ingestion. Agents in the V-series are approximately 10- to 100-fold more toxic than those in the G-series.

OP nerve agents inhibit the catalytic function of acetylcholinesterase (AChE) (EC 3.1.1.7; AChE) by phosphorylating the esteratic site of the enzyme [8]. This removes the capacity of the enzyme to catalyze its endogenous substrate acetylcholine (ACh). As a consequence, the hydrolysis of ACh is prevented, leading to accumulation of ACh in the synaptic cleft, and overstimulation and subsequent desensitization of ACh receptors in brain, glands, and skeletal and smooth muscles. These effects cause disruption of nerve function that leads rapidly to a progression from miosis, excessive secretions, and muscle fasciculation to epileptic seizures, muscle paralysis, cardiorespiratory depression, and death due to respiratory failure. The OP nerve agents are more toxic than the related

OP pesticides still in use today. They are lethal at minute doses. For example, the median lethal dose (LD50) of VX for a 70 kg person is only 10 mg.

Acute poisonings with OP nerve agents and pesticides are treated with atropine sulfate to inhibit central muscarinic effects, and pralidoxime (2-PAM) chloride to reactivate the inhibited AChE. Atropine blocks muscarinic cholinergic receptors in the parasympathetic nervous system to reduce excessive secretions and smooth muscle contraction. It does not have a significant therapeutic effect for central nervous system (CNS) toxicity or does not appear to work well at cholinergic synapses on skeletal muscle. Atropine works well as an antidote to OPs, but it can have significant side effects if dosing is not carefully monitored. Other cholinergic drugs and drugs that interact with other neurotransmitter systems are under development, which may be more selective and have fewer side effects.

The oxime 2-PAM chloride appears to be most effective at nicotinic cholinergic synapses on skeletal muscle [8]. It removes OP nerve agents and pesticides from the OP-AChE complex by virtue of its highly nucleophilic oxime moiety. Both OP pesticides and nerve agents undergo a deacylation process called *aging* during which the bond strength between the OP and AChE significantly increases, and after which oximes are ineffective. Once aging has occurred, the AChE is irreversibly inactivated and enzyme activity can only be restored by *de novo* resynthesis. Aging times vary according to the nerve agent, and ranges from very fast with soman (2 min) to much slower with sarin (3–4 h) and longer for others. Research on improved AChE reactivators is focused on increasing activity within the CNS, and increasing the therapeutic window, especially for fast-aging nerve agents. This includes developing novel compounds as well as investigating alternative oximes used in other countries such as trimedoxime and HI-6. Atropine and 2-PAM chloride are packaged together for civilian use in the Strategic National Stockpile's CHEMPACK program, and in spring-powered auto-injectors used by the US military. Other treatment strategies for OP nerve agents include sequestration or inactivation of the agent using endogenous or modified proteins to bind free nerve agent stoichiometrically or the introduction of enzymes with high catalytic activity to remove the nerve agent from circulation before it reaches the target site. An enzyme similar to AChE, butyrylcholinesterase (BChE), is under development by the military as a prophylactic agent. It remains uncertain if this could be given safely and effectively in humans, and if it could be used to treat civilians after exposure to nerve agents has already occurred.

Exposure to sufficient doses of OP nerve agents cause epileptic seizures. Prolonged seizure activity after nerve agent exposure has been shown in animals to cause neuropathologic lesions in the CNS that are associated with long-term impairment of cognitive function and other behaviors [9–12]. It is believed that the long-term effects of nerve agent-induced seizures involve stimulation of the glutamatergic system causing eventual excitotoxicity, calcium accumulation, increased catabolic activity, and cell death [13]. Research in the area of antiglutamatergic drugs and prevention of excitotoxcity is being pursued since in many cases first responders may not be able to administer any treatment until this latter excitotoxic phase. Alone, the atropine and 2-PAM treatment regimen is not effective against OP-induced seizures once they are established, but these antidotes are crucial to the effectiveness of anticonvulsants, and the dose of atropine influences the effectiveness of anticonvulsants [14]. The benzodiazepine diazepam is an anticonvulsant used for treatment of exposure to OP nerve agents, and is included in 10 mg doses in the antidote treatment regimen used by the US military convulsant antidote, nerve agent (CANA). It is also included in the civilian CHEMPACK stockpile. Administering

diazepam is an effective treatment for the seizures associated with nerve agent exposure, but it has limited bioavailability when administered intramuscularly, and there is a loss in efficacy after prolonged seizure activity. As with most drugs that suppress CNS activity, the potential for over-sedation and respiratory depression exists with diazepam, especially in cases where patients may already be suffering from paralysis or hypoxia from the nerve agent. This last point regarding OP-induced paralysis is also important when considering the diagnosis of seizure activity and appropriate treatments. The muscular effects of OP nerve agents may mask or mimic signs of seizure activity. A field deployable electroencephalograph (EEG) suitable for use by first responder medical personnel could be used to detect potential nonconvulsive seizures during a chemical event.

## 2.2 Chemical Affecting the Pulmonary Tract

Many TICs produced and transported in high volume in the United States can severely disrupt normal pulmonary function and lead to respiratory failure if individuals are exposed to high enough levels. The volatility of many TICs and CWAs is of particular concern because of the ease at which many people can be exposed by inhalation. Of the several hundred chemicals identified by the US EPA as TICs, sulfuric acid, ammonia, chlorine, nitric acid, and ammonium nitrate are among the most abundant. Ammonia and alkali agents like sodium hydroxide, as well as acids used in industries such as hydrochloric and sulfuric acid, are highly corrosive to the upper airways. Sulfur mustard, a highly corrosive CWA, targets the upper airways and can cause acute inflammation, painful ulcerations, increased secretions, and difficulties in breathing and swallowing. Secondary bacterial infections may result from and further exacerbate the initial injury. Damage to the upper airways can lead to respiratory failure and death. Exposure can also lead to long-term health problems. For example, chronic respiratory problems such as scarring and narrowing of the trachea have been observed in Iranians exposed to sulfur mustard during the Iran–Iraq War of the 1980s [15].

Other toxic chemicals used in industry may reach the lower respiratory tract and cause life-threatening injuries such as pulmonary edema. These include ammonia, chlorine, phosgene, and perfluoroisobutylene. Pulmonary edema is the leakage of fluid into the lungs, which prevents oxygen delivery to the blood, ultimately preventing oxygen from reaching the brain, kidneys, and other organs. Symptoms may be immediate or delayed, for example, chlorine causes immediate airway irritation and pain, whereas phosgene exposure may not be evident for 24–48 h (Table 1) [3]. People who survive a single, acute exposure to respiratory airway toxins generally show little or no long-term health problems, although some may eventually develop asthma or chronic bronchitis. Individuals at greatest risk are those with preexisting cardiopulmonary disease. Chlorine is a greenish-yellow volatile gas with pungent order and is 2.5 times heavier than air as a gas. It produces severe pain and irritation almost immediately within the conjunctiva and mucous membranes in the nasal passages and upper airway. Coughing and choking is very common early after exposure. Chlorine was first used during World War I by the Germans in Ypres, Belgium, and caused more than 15,000 British and French casualties with 5,000 deaths. Phosgene is a colorless gas that has an odor described as in new-mown hay. It is 3.5 times heavier than air as a vapor and more stable than chlorine when used with explosives. It is also 10 times more toxic than chlorine and far less irritating than chlorine when initially inhaled, which results in an insidious delayed action promoting continued inhalation and more prolonged exposure. Other agents used in warfare such as

sulfur mustard and nerve agents also have severe deleterious effects on the pulmonary tract, and these are discussed in detail in other sections of this article.

Specific drugs to prevent chemically induced damage to the respiratory airways are not available. Analgesic medications, oxygen, humidification, and ventilator support currently constitute the current standard of care for most chemical exposures affecting the pulmonary tract. Hemorrhaging, signifying substantial damage to the lining of the airways and lungs, can occur with exposure to highly corrosive chemicals and may require additional medical interventions. Treatment of injuries to the lower respiratory tract is also supportive and usually includes administration of oxygen, the use of mechanical ventilation to include positive airway pressure, and bronchodilators to treat bronchospasms. Drugs that reduce the inflammatory response, promote healing of tissues, and prevent the onset of pulmonary edema or secondary inflammation may be used following severe injury to prevent chronic scarring and airway narrowing. Current diagnostic capabilities are limited. Exposure to chlorine, phosgene, or any of the major alkali agents is determined based on clinical signs and symptoms. If newer, more specific therapies are to be developed for chemical agents, then diagnosis of exposure to specific agents may be important, as will screening tests to identify individuals exposed to low levels of chemicals.

The need for prehospital treatments for exposure to pulmonary agents is evident because most of the current treatments can only be administered in a controlled hospital setting, and many hospitals are ill suited for a situation involving mass casualties among civilians. Inexpensive positive-pressure devices that can be used easily in a mass casualty situation and drugs to prevent inflammation and pulmonary edema are needed. Several drugs that have been approved by the US Food and Drug Administration (FDA) for other indications hold promise for treating chemically-induced pulmonary edema. These include $\beta$ 2-agonists, dopamine, insulin, allopurinol, and nonsteroidal anti-inflammatory drugs (NSAIDs) such as ibuprofen. Ibuprofen is particularly appealing because it has an established safety record and can be easily administered as an initial intervention. Studies have shown that ibuprofen improves survival and reduces lung fluid levels in mice exposed to phosgene [16]. Inhaled and systemic forms of $\beta$ 2-agonists used in the treatment of asthma, and other commonly used medications may also be fruitful avenues of future research on new treatments for chlorine and phosgene exposure. Some of these potential drugs target the inflammatory response or the specific site(s) of injury. Others modulate the activity of ion channels that control fluid transport across lung membranes or target surfactant, a substance that lines the air sacs in the lungs and prevents them from collapsing.

It is clear for chemical agents that affect the pulmonary tract that basic mechanistic research is needed to discover new targets for therapeutic development; however, research is also needed to test the effectiveness of the many drugs already approved by the FDA for other diseases and disorders with similar pathologies. The anti-inflammatory drugs probably hold the greatest potential at present as a first step for treating mass chemical exposures. Research will require the identification and validation of appropriate *in vitro* systems and animal models for preclinical testing of drugs to treat chemically induced injury to the upper and lower respiratory tract. Since it is clear that some of the chemicals may cause long-term chronic health effects, studies are needed to fully characterize these effects for the purpose of developing effective medical interventions. Finally, some chemicals generate metabolic byproducts that could be used for diagnosis, but detection of these byproducts may not be possible until many hours after initial exposure. Diagnostic

tools and biological markers associated with acute lung injury are needed to help guide medical interventions in both the pre- and in-hospital settings.

### 2.3 Metabolic and Cellular Poisons

Metabolic poisons can be inhaled or ingested. Many of the TICs of concern affect cellular respiration. These include chemicals such as phosphine, arsine, and the infamous and highly toxic cyanide compounds. Exposure to high concentrations of hydrogen cyanide (HCN) gas can cause death within minutes. This narrow therapeutic window presents a formidable challenge for treatment, but emphasizes the need for immediate medical intervention. Inhalation of lower concentrations of cyanide vapor or cyanide salt ingestion may result in a slower development of symptoms. Metabolic poisons, such as hydrogen cyanide and cyanogen chloride, inhibit cellular respiration, whereby oxygen is extracted from the blood at the cellular level and sugar molecules are transformed into energy. All systems of the body are ultimately affected but the cardiovascular system and the CNS are most strongly affected due to their high demands for oxygen and energy and limited ability to use alternative pathways for energy production. Exposure to metabolic poisons can quickly cause seizures, respiratory failure, cardiac arrest, and death (Table 1). Long-term effects are poorly understood and may include gradual neurodegeneration [17].

No pretreatment for cyanide poisoning is available and it may not be practical. Since 1933, a cyanide antidote kit has been marketed for use in the United States, but as a kit, it has never received formal regulatory approval by the FDA. The cyanide antidote kit includes crushable ampoules of amyl nitrite for inhalation, and sodium nitrite and sodium thiosulfate, which are administered intravenously. The nitrites bind with hemoglobin in the blood to produce methemoglobin molecules. The methemoglobin then binds with cyanide to produce a much less toxic cyanomethemoglobin, which is eventually eliminated from the body. Sodium thiosulfate, often referred to as a *sulfur donor drug*, converts cyanide into nontoxic thiocyanate, which is then excreted by the kidneys. The cyanide antidote kit can be very effective, but it carries the risk of toxic side effects. High levels of methemoglobin can be lethal. Dosing is especially challenging for pediatric casualties because of this toxicity [18]. Individuals with preexisting glucose 6-phosphate deficiency have a risk of red cell hemolysis if given sodium thiosulfate [19]. Individuals with renal deficiency, or anemia, could also suffer toxicity from the treatment. The ability to predictably quantify the amount of amyl nitrite that would be absorbed through inhalation may also be difficult.

In 2007, the FDA approved Cyanokit (hydroxocobalamin for injection) for treatment of cyanide poisoning. It has not yet been determined how effective this new countermeasure would be in a mass casualty situation since it needs to be administered intravenously. Administration of 10% hyperbaric oxygen is a major component in the treatment of cyanide poisoning, typically used even before the administration of any cyanide antidotes. However, the value of hyperbaric oxygen has not been determined, especially with products that form methemoglobin.

Government and private sector organizations have developed research agendas on next generation cyanide antidotes and new approaches. For example, cobinamide, one of the precursor compounds in the biosynthesis pathway of hydroxocobalamin, is a promising drug that warrants further investigation [20]. Cyanohydrin-forming compounds (e.g. $\alpha$-ketoglutarate and pyruvate) and vasodilatory drugs that act similar to nitrite compounds are potential new cyanide antidotes, as are drugs that act at the cellular level,

such as synthetic S crystallized rhodanese (an enzyme that promotes the conversion of cyanide to nontoxic thiocyanate). Sulfur-containing medications may also have potential benefits in the treatment of cyanide poisoning, especially those that remain in circulation for longer periods of time than sodium thiosulfate. The identification of FDA-approved drugs containing sulfur may have a therapeutic value in the treatment of cyanide poisoning. Drugs that form methemoglobin may have an advantage, but there are significant health risks associated with high levels of methemoglobin.

Within the NIH Strategic Plan, both short- and long-term strategies are being pursued in order to develop countermeasures against metabolic poisons [3]. Short-term goals include the improved understanding of the mechanisms of injury from cyanide-containing compounds, and identification of potential targets for medical intervention. The determination of optimal and novel routes of drug administration of promising compounds, to include administration through inhalation is a goal being pursued. The identification of screening tests and biological markers consistent with the identification of hydrogen cyanide and/or cyanide metabolite(s) and the level of exposure to such agents are under investigation. Also of concern is the identification and validation of appropriate *in vitro* systems and animal models for preclinical testing of drugs that could be useful in cyanide poisoning. The validation for the use of oxygen therapy in the initial treatment of cyanide poisoning, alone or in combination with other medical countermeasures along with the understanding of the differences in cyanide intoxication between different age ranges, and establishment of a treatment plan for susceptible populations are also short-term goals being pursued.

Long-term goals include the conduct of safety and efficacy studies with promising drugs, and the identification of effective routes of administration that would lead to timely intervention. The identification of major mechanisms and pathways by which sulfur donors, methemoglobin formers, and cobalt compounds counter cyanide toxicity in different systems of the body is an area of ongoing research. The expansion of the current NIH research infrastructure to enable preclinical and clinical studies on compounds with promising anticyanide activity is also a goal. NIH research is pursuing the development of rapid diagnostic tests and assays to identify specific biological markers consistent with cyanide exposure. The identification of any long-term or chronic health effects resulting from exposure to hydrogen cyanide, the cyanide-containing salts, and/or cyanogen chloride is an important long-range goal. Also, NIH is establishing databases of clinical, epidemiological, and laboratory information that will contribute to the understanding of the acute and chronic health effects of high- and low-level exposures to cyanide-containing compounds. Lastly, the review of current therapeutic interventions with oxygen and the assessment of the value of other proposed alternatives, such as the use of hyperbaric oxygen in treatment are being pursued.

### 2.4 Chemicals Affecting the Skin, Eyes, and Mucous Membranes

Vesicating (blister) agents, such as sulfur mustard, nitrogen mustard, lewisite, and caustic industrial chemicals, can cause severe blistering and burns to the eyes, mucous membranes, skin, and upper airways, as well as chronic eye inflammation and blindness. The eyes are the organs most sensitive to these chemicals. Vesicants may also affect other parts of the body, including the respiratory tract, immune system, and bone marrow. Sulfur mustard can cause tissue damage within minutes of exposure. Physical injury from other vesicants agents may not be evident for several hours and may result in delayed

recognition of exposure (Table 1). Many vesicating agents including sulfur mustard are oily liquids and considered "persistent" chemicals, that is, they do not evaporate quickly and remain active for an extended time. Clothing, skin, and hair may remain contaminated with sulfur mustard for hours, presenting a challenge to health care providers. The military and first responders rely heavily on individual physical protection (e.g. protective masks and suits) to prevent exposure to vesicants. No medical pretreatment drugs are yet available.

Although mustard agents were used in World War I, there is still no antidote for this vesicant. This is of great concern in view of the history of use and present day arsenals. Additionally, despite over 80 years of research, there is still no clear understanding of the biochemical mechanism of action. Despite the fact that the chemistry of mustard interaction with cellular components is well defined in the literature [21], the correlation with actual injury has not been made and is still under investigation. Current treatment of vesicant injuries is largely symptomatic and supportive. Eye injuries require the use of special eye drops, antibiotics, and other drugs to prevent secondary infection and steroids to limit the inflammatory response and speed the healing process. Skin wounds, especially when severe with blister formation, require specific medical attention to reduce pain, prevent infection, and reduce inflammation. Debridement (removal) of a layer of the injured skin may be necessary to speed the secondary healing process. British-Anti-Lewisite (BAL, dimercaprol) is a specific antidote for the chemical agent Lewisite and is also used for the treatment of heavy metal poisoning. BAL skin and eye ointments were developed for the military and these may decrease the severity of skin and eye lesions when quickly applied. BAL may be useful in the topical treatment of other injuries from vesicants besides Lewisite. However, because of reported toxicities associated with BAL, this compound has not been considered to be a useful prophylactic drug. Other therapeutic compounds are needed that can prevent/reduce the redness and deep tissue damage (blisters) in a short period. Also needed are improved skin protectants, reactive skin protectants that can neutralize the agent, new skin and eye therapies, and improved healing techniques.

Diagnosis of vesicant injury is based on clinical signs and symptoms and the detection of specific agents in the environment. There are no FDA-approved clinical laboratory tests for sulfur mustard in blood or tissue. However, compounds such as thiodiglycol (TDG) are produced in the body after exposure to sulfur mustard and can be detected in blood, urine, and tissue. These compounds can be analyzed in a research setting and require the use of complex laboratory equipment such as gas chromatographic mass spectrophotometers.

Short-term goals being pursued by the NIH include the comparison of medical countermeasures used by the Department of Defense (DoD) for the treatment of vesicating injuries for their use in civilian populations during mass casualty situations. Also, the evaluation and monitoring of promising ophthalmic drugs developed in the DoD program is being assessed for applicability for civilian populations and first responders. Further investigation with FDA-approved skin protectants against chemical agents for potential use in civilian populations is underway. The identification and validation of appropriate *in vitro* systems and animal models for preclinical drug testing is being pursued. This is to address both caustic agents and vesicants.

Long-term goals include the development of novel therapeutic strategies, including reactive therapeutic compounds, to prevent blister formation and inflammatory effects in skin and eyes. The goals also include the evaluation of the effectiveness of new

immunotherapeutic compounds and their applicability in the treatment of acid/alkali and mustard injuries. The identification of the specific mechanisms of action of specific chemical agents and their sites of injury to the skin, eyes, and mucous membranes, down to the molecular level is being pursued, as well as the investigation of the healing mechanisms following chemical injury. Part of this research is to identify novel ways of accelerating the recovery process following injury. Long-range strategic goals also will consider the mechanisms of action of vesicants on tissues, organs, and the hematopoetic system for the development of therapeutic interventions. This will be critical for the evaluation of novel therapeutic strategies for acid and alkali injuries. Additionally, the identification of biological markers consistent with types of chemical agents and the level of exposure to such agents are being investigated. The evaluation of "reactive" or "catalytic" skin protectants for use in civilian populations, such as first responders who must operate in a contaminated environment, is a long-range strategy. The evaluation of decontamination approaches for patients with open wound injuries and the identification of novel opportunities for medical intervention is a planned research effort. These efforts will potentially assist in the development of practical therapies that can be easily and safely administered to decontaminate the skin during mass causality situations.

## 3 SUMMARY AND CONCLUSIONS

It is impossible to predict when or where the next deliberate or accidental release of chemical weapons or TICs will occur. Unpredictable circumstances require a two-pronged approach. Firstly, a solution that reduces the threat or the unpredictability of the threat, which is beyond the scope of this article. Secondly, a solution that prepares one to mitigate the deleterious effects of the event once it has occurred. Part of the overall strategy employed by the US government to enhance emergency preparedness involves improving our medical response capabilities in order to reduce casualties and the strain on the health care system after an emergency event. Chemical agents that can be regarded as posing a threat to civilians at the mass casualty level include traditional CWAs such as nerve agents and sulfur mustard, and TICs such as chlorine and cyanide. These could be either used in attacks against civilians or released in large quantity after an industrial accident or natural disaster. These toxic chemicals cause a wide variety of health effects, both acute injuries and lethality at relatively low doses, and long-term, sometimes, delayed chronic illnesses.

Currently, many medical interventions that reduce mortality and morbidity after exposure to chemical threat agents are available. Antidotes, diagnostic tools, and drugs to treat symptoms are available for all of the highest priority chemical threats to civilians. However, research has identified several new opportunities to develop even better medical intervention strategies that will enhance medical response capabilities. These include better therapies that treat the most severe symptoms such as safer, faster-acting anticonvulsants to treat exposure to nerve agents, antidotes based on basic knowledge of the specific agents such as those that target the metabolic pathway of cyanide, and broad spectrum drugs that target common physiological mechanisms of injury such as anti-inflammatory drugs that could be used to treat victims exposed to many different kinds of chemicals.

The NIH in collaboration with the DoD has developed a research and development program to enhance the Strategic National Stockpile and better prepare health care professionals for an emergency event involving the release of toxic chemicals. The goal

of this program is to identify existing FDA-approved drugs, new drugs, and better diagnostic tools that could be rapidly deployed and used during a mass casualty event. The CounterACT and other programs at DHHS charged with this important goal are essential to national security and will require strong support to meet the challenges ahead. It will require a commitment that is consistent with the cost and time required for drug discovery and development, and should support research at the basic, translational and clinical levels.

## REFERENCES


1. Kortepeter, M. G., Cieslak, T. J., and Eitzen, E. M. (2001). Bioterrorism. *J. Environ. Health* **63**, 21–24.
2. Morita, H., Yanagisawa, N., Nakajima, T. (1995). et al Sarin poisoning in Matsumoto, Japan. *Lancet* **346**, 290–293.
3. NIAID (2007). *NIH Strategic Plan and Research Agenda for Medical Countermeasures Against Chemical Threats: U.S. Department of Health and Human Sefvices*, National Institutes of Health, Bethesda, MD, 24.
4. Office USGA (2003). *Homeland Security. Voluntary Initiatives are under way at chemical facilities, but the extent of security preparedness is unknown*, Washington, DC, p. 42.
5. Broughton, E. (2005). The Bhopal disaster and its aftermath: a review. *Environ. Health* **4**, 6.
6. Joseph, G. (2004). Chlorine transfer hose failure. *J. Hazard Mater*. **115**, 119–125.
7. Broderick, K. E., Potluri, P., Zhuang, S., Scheffler, I. E., Sharma, V. S., Pilz, R. B., and Boss, G. R. Cyanide detoxification by the cobalamin precursor cobinamide. *Exp Biol Med (Maywood)*. 2006. **231**(5), 641–649.
8. Taylor, P. (1990). Anticholinesterase agents. In *Goodman and Gilman's The Pharmacological Basis of Therapeutics*, 8th ed, A. G. Gilman, T. W. Rall, A. S. Nies, P. Taylor, Eds. Pergamon Press, New York, 131–149.
9. Kadar, T., Shapira, S., Cohen, G., Sahar, R., Alkalay, D., and Raveh, L. (1995). Sarin-induced neuropathology in rats. *Hum. Exp. Toxicol.* **14**(3), 252–259.
10. McDonough, J. H. Jr., Dochterman, L. W., Smith, C. D., and Shih, T. M. (1995). Protection against nerve agent-induced neuropathology, but not cardiac pathology, is associated with the anticonvulsant action of drug treatment. *Neurotoxicology* **16**, 123–132.
11. McDonough, J. H. Jr., and Shih, T. M. (1997). Neuropharmacological mechanisms of nerve agent-induced seizure and neuropathology. *Neurosci. Biobehav. Rev.* **21**, 559–579.
12. Shih, T. M., Duniho, S. M., and McDonough, J. H. (2003). Control of nerve agent-induced seizures is critical for neuroprotection and survival. *Toxicol. Appl. Pharmacol*. **188**, 69–80.
13. Solberg, Y., and Belkin, M. (1997). The role of excitotoxicity in organophosphorous nerve agents central poisoning. *Trends Pharmacol. Sci*. **18**, 183–185.
14. Shih, T. M., Rowland, T. C., and McDonough, J. H. (2007). Anticonvulsants for nerve agent-induced seizures: the influence of the therapeutic dose of atropine. *J. Pharmacol. Exp. Ther.* **320**(1), 154–161.
15. Ghanei, M., and Harandi, A. A. (2007). Long term consequences from exposure to sulfur mustard: a review. *Inhal. Toxicol*. **19**, 451–456.
16. Sciuto, A. M., and Hurt, H. H. (2004). Therapeutic treatments of phosgene-induced lung injury. *Inhal. Toxicol*. **16**, 565–580.
17. Gracia, R., and Shepherd, G. (2004). Cyanide poisoning and its treatment. *Pharmacotherapy* **24**, 1358–1365.

18. Geller, R. J., Barthold, C., Saiers, J. A., and Hall, A. H. (2006). Pediatric cyanide poisoning: causes, manifestations, management, and unmet needs. *Pediatrics* **118**, 2146–2158.
19. Baskin, S. I., Horowitz, A. M., and Nealley, E. W. (1992). The antidotal action of sodium nitrite and sodium thiosulfate against cyanide poisoning. *J. Clin. Pharmacol.* **32**, 368–375.
20. Lippin, T. M., McQuiston, T. H., Bradley-Bull, K., Burns-Johnson, T., Cook, L., Gill, M. L., Howard, D., Seymour, T. A., Stephens, D., and Williams, B. K. (2006). Chemical plants remain vulnerable to terrorists: a call to action. *Environ Health Perspect*, **114**(9), 1307–1311.
21. Hurst, C. G., and Smith, W. J. (2000). *Chemical Warfare Agents: Toxicity at Low Levels*, CRC Press, Boca Raton, p. 253.

# DEVELOPMENT OF RADIATION COUNTERMEASURES

TERRY C. PELLMAR

*Armed Forces Radiobiology Research Institute, Uniformed Services University of the Health Sciences, Bethesda, Maryland*

## 1 INTRODUCTION

With the increasing concerns about the possibilities of misuse of nuclear or radiological materials comes the requirement for appropriate medical treatment of the biological consequences of exposure to ionizing radiation. Radiation injury results from exposure to sources both external and internal to the body. Penetrating radiation, such as high-energy $\gamma$ rays or neutrons, presents the greatest hazard of external radiation injury. Internal exposures result from the internalization of radionuclides through inhalation, ingestion, or absorption through the skin or wounds. After detonation of a nuclear device, internal exposure is a relatively minor component of the injury. For this reason, efforts to develop countermeasures have focused on the acute radiation syndrome (ARS) resulting from penetrating radiation. With radiological acts of terrorism, scenarios do exist where internal contamination is the primary threat. This article will review the injury that results from radiation exposure and explore some of the efforts in the development of radiation countermeasures. With a long history of research and the recently renewed energy in this area, many agents have already been evaluated and new options continually arise. This review cannot be comprehensive; instead, it presents examples of countermeasures under investigation to convey the past and future status of the field.

## 2 RADIATION INJURY

### 2.1 Acute Radiation Syndrome

ARS is the spectrum of syndromes named for the organ system that is most likely to cause lethality after whole-body exposure to radiation [1, 2]. Doses of radiation less than 1 Gy elicit few acute symptoms. Within the first day, some people might experience mild prodromal symptoms such as nausea and a slight decrease in circulating lymphocytes, but long-term survival is probable [1, 3]. As the radiation dose increases over 2 Gy, prodromal symptoms become more severe with an earlier onset. After a transient recovery (or latent phase), the hematopoietic syndrome becomes evident as neutrophil and platelet counts drop after a few weeks. Neutropenia increases susceptibility to infection, and loss of platelets leads to bleeding, which can lead to death. With increasing radiation doses, the integrity of the gut wall is also impaired, allowing the translocation of gut bacteria, which can lead to sepsis. Both hematopoietic and gastrointestinal (GI) consequences are more severe with increasing doses. With exposures between 8 and 12 Gy, the GI syndrome predominates with severe loss of intestinal crypts and extensive breakdown of the mucosal barrier. Death results from the GI effects, usually within a couple of weeks. At doses greater than 12 Gy, death can result relatively quickly from cardiovascular and nervous system effects. Without treatment, the LD50 for ARS is about 3.5 Gy [4]. Several factors can modify this LD50 value. The effects of radiation are mitigated by poorly penetrating radiation, partial-body exposures, low dose rates, and good supportive care; they are exacerbated by extremes of age, coexisting trauma or infection, poor nutritional status, and neutron radiation. A concurrent traumatic injury also significantly increases the likelihood of lethality from radiation exposure.

### 2.2 Internal Contamination

The biological consequences of internalized radionuclides depend on their absorption, distribution, metabolism, and excretion pathways [5, 6]. Particular organs may be targeted by the agent, but if the distribution is broad and the radioactivity is high, ARS can also result. Radioactive materials can be internalized through inhalation, ingestion, or transdermal absorption. Inhalation is the most likely route of exposure. Larger particles, deposited in the upper bronchi, can be cleared relatively quickly. However, smaller particles (5–10 μm) can penetrate deeply into the lungs, reaching the alveoli. Soluble forms of the radionuclides are absorbed into the blood stream or the lymphatic system. Insoluble forms may stay in the lung causing radiation and chemical damage to the surrounding tissue. Contaminated food and water, as well as aerosolized particles that enter the nasal and oral cavities, provide routes for ingestion of radioactive materials. As with inhalation, the absorption from the GI tract depends on the solubility. Soluble particles are distributed through the circulation but nonsoluble particles remain in the gut. Although these particles will eventually be excreted, the transit time provides opportunities for radiation exposure of GI tissue. Intact skin presents a physical barrier through which few radionuclides can penetrate. (Tritiated water, which can permeate skin, is the primary exception to this.) Wounds and burns, however, provide more direct access to the circulation. Again, solubility as well as other factors (e.g. tissue reactivity and particle size) affects the absorption from a wound. Once internalized, radionuclides distribute in the same way as their nonradioactive counterparts. Depending on the element, it may be evenly distributed through the body (e.g. tritium or cesium) or concentrated

in particular organs (e.g. iodine to thyroid, uranium to bone and kidney). Elimination of absorbed radionuclides occurs primarily through the urine or secretion via the bile into the intestine.

### 2.3 Current Status of Medical Countermeasures

Although no drugs have yet been specifically approved for treatment of ARS, the medical approach to radiological accidents and our knowledge of the response to clinically used whole-body radiation have provided insights into regimens that are likely to be effective. For internal contamination, three countermeasures have been approved: potassium iodide (KI) to block the uptake of I131, Prussian blue to enhance the excretion of cesium, and Ca- and Zn-DTPA (diethylenetriaminepentaacetic acid) to chelate the transuranic elements. A number of reviews and manuals provide guidance for medical management of radiation injury [3–5, 7–9]. In contrast to accidents, where the few victims receive intensive clinical care from a medical staff knowledgeable about radiation injury [3], mass casualties pose serious logistical challenges. Breakdowns in transportation, communication, and access to medical care [10–12] are possible. Thousands of patients with poorly defined radiation exposures will converge on the hospitals. Extensive medical support (e.g. antibiotics and platelet transfusions) may not be available. A licensed drug for ARS that is safe and efficacious even in the absence of ancillary care is essential. Nonmedical personnel should be able to administer the agent on a schedule that is logistically achievable. An ideal drug will be inexpensive and stable without any special storage requirements to allow long-term storage even if refrigeration is unavailable. These ideals are yet to be attained.

The cytokine granulocyte colony-stimulating factor (G-CSF) (Neupogen) is currently the pharmaceutical most likely to be recommended for hematopoietic reconstitution following radiation injury [3, 7, 13–15]. Neupogen and the pegylated form of G-CSF (Neulasta) are Food and Drug Administration (FDA) approved for treatment of severe neutropenia that occurs with chemotherapy for cancer. Neupogen received investigational new drug (IND) status for treatment of radiation injury and can now be used if an emergency waiver is authorized [16]. Neupogen must be stored under refrigeration and must be injected subcutaneously for several days (up to 2 weeks) starting as soon as possible after radiation exposure. The recommended dosage of Neulasta is a single subcutaneous injection [3]. Both Neupogen and Neulasta can cause moderate bone pain. Symptomatic treatment with antibiotics, antifungals, blood transfusions, intravenous fluids and electrolytes [3, 4, 7], and platelet transfusions [17] are generally necessary, as well.

Accidents have taught us that, in addition to hematopoietic effects, GI damage is usually present after radiation injury as well. With partial-body exposures, GI effects may actually be the more critical component of ARS because shielding of marrow-producing bones spares critical stem cells and promotes recovery of neutrophils and other cells. Kepivance (palifermin), a modified keratinocyte growth factor (KGF), recently has been approved by FDA to reduce the incidence of mucositis after radiation therapy followed by stem cell rescue. For this indication, palifermin is administered as a daily injection for several days. As with Neupogen, the route of administration poses logistical issues for mass casualties.

In the event of a radiological/nuclear terrorist attack, first responders, remediation workers, and given advanced warning, the resident population, would benefit from a radioprotectant to prevent the effects of ionizing radiation. A radioprotectant given to

healthy individuals needs to be long-lasting, easily self-administered, and with very low toxicity. Currently, nothing of the kind is available. Amifostine has been shown to be an effective radioprotectant in animals, and it is approved as a preventive measure for xerostomia with clinical radiation, but its side effects of hypotension and nausea limit its usefulness [18].

Current treatment of internal contamination aims to dilute, block, or remove the radionuclides [5]. Nonpharmaceutical approaches can be used to minimize absorption. This includes pulmonary or gastric lavage, emetics, or enemas. Excretion of tritium can be enhanced by increasing oral fluids. In the event of release of radioactive material from a nuclear reactor, KI will be used to prevent radioiodine from accumulating in the thyroid [19]. To be effective, KI must be administered within a few hours of exposure. Radioactive iodine has the most serious effects on the thyroid of children and young adults. Adults above 40 years show little benefit from treatment [20, 21]. Prussian blue, ferric hexacyanoferrate, when administered orally, enhances fecal excretion of cesium and thallium by means of ion exchange. It was used effectively in the accidental dispersal of cesium-137 in Goiania, Brazil [22–24].

Clearly, there is a need for development of new pharmaceuticals for treatment of radiation injury. As our understanding of the mechanisms of radiation injury increases, new drugs can be targeted toward specific mechanisms.

## 3 APPROACHES TO INTERNAL CONTAMINATION

The effects of internalized radionuclides depend on the amount absorbed and the distribution in the body. As a result, the effects are agent specific. Countermeasures for internal contamination focus on expediting the removal from the body (decorporation) or protecting their primary site of activity. Decorporation is generally less effective if the radionuclide has already distributed to target tissues. Because of this, early treatment is usually more efficacious. Although there are FDA-approved treatments (Prussian blue, DTPA, and KI) and therapeutic approaches (e.g. lavage, emetics), gaps exist regarding treatment for internalized nuclides. Yet, research into the development of new decorporation and blocking agents has been very limited over the past couple of decades.

### 3.1 Blocking Agents

KI is the prototype for a countermeasure that blocks the site of activity. The primary site of toxicity of iodine-131 is the thyroid gland, increasing the risk of thyroid cancer [19, 21]. Nonradioactive KI displaces the radioactive element, thereby protecting the thyroid gland. Similarly, calcium gluconate can be used to prevent strontium binding at the bone surface by competing with calcium ions at binding sites [25, 26]. Through this mechanism it has some efficacy as a treatment for internal contamination from inhalation of radioactive strontium.

### 3.2 Decorporation Agents

DTPA chelates many heavy metals to form a water soluble compound that is excreted through the kidneys. The disadvantages of this approved therapeutic approach is the requirement for intravenous injection and the toxicity associated with prolonged

exposure to the chelator, which can cause trace metal deficiencies. Aerosol formulation of Ca-DTPA for use in a nebulizer is also available. This approach may be effective when used soon after inhalation exposure if lung function is normal. Oral delivery DTPA would be logistically easier to use in a mass casualty setting [27].

Prussian blue given orally enhances the elimination of cesium that is ingested or released through the bile into the GI tract. Through this mechanism, it reduces the biological half life of the element. In patients treated in Goiania, the half life was reduced from 80 days in untreated adults to 26 days with Prussian blue treatment [28].

Blocking absorption through the GI track is an effective strategy for Sr ingestion. Alginates have traditionally been used to treat internal contamination with radioactive strontium [29, 30]. Alginates are substances obtained from brown sea algae and sodium alginate binds tightly with strontium, significantly reducing absorption in the GI tract. The high viscosity of the alginates makes them difficult to ingest and limits their usefulness. Attempts to incorporate alginates into bread has had limited success [30]. Ingested strontium absorption can also be significantly reduced by aluminum phosphate gel and by barium sulfate, when used soon after exposure [5]. Sodium bicarbonate ($NaHCO_3$) can increase the excretion of uranium by alkylating the urine, creating a nontoxic uranium complex, which is promptly excreted.

More recent efforts are exploring new chelating agents such as catecholicpolyaminopolycarboxylate ligands 9501 and 7601 for thorium [31] and hydroxypyridinonate (HOPO) ligands such as 3,4,3-LIHOPO for plutonium and other actinides [32–34] and the biphosphonate, ethane-1-hydroxy-1,1-biphosphonate (EHBP) for uranium [35]. The HOPO ligands have the advantage of having oral efficacy [32, 35].

## 4 ARS CASCADE: TARGETS FOR COUNTERMEASURES

Ionizing radiation deposits much of its energy in biological tissue through the generation of free radicals in the aqueous environment. These very reactive free radicals damage the lipids, proteins, and DNA, which are integral to the function of cells. As a consequence of this damage, intra- and intercellular signaling can be impaired. An inflammatory cascade of events is initiated (Table 1). The cell cycle signals, as well as other cellular activities, are disrupted. Death of mitotic cells causes the loss of progenitor cells in bone marrow and in the crypts of the GI tract, resulting in neutropenia, thrombocytopenia, anemia, and loss of gut integrity. With increased susceptibility to infection, bleeding, and loss of fluid and electrolytes, death occurs. Countermeasures are being developed to address each step of this cascade (see Table 2).

### 4.1 Free Radical Damage

Through deposition of its energy in the aqueous environment of biological tissue, $\gamma$ radiation generates free radicals that mediate the injurious effects. Higher LET (linear energy transfer) radiation such as $\alpha$ radiation is more likely to cause direct damage to the biological tissues rather than the free radicals that cause indirect damage. Free radicals are damaging to the macromolecules of biological tissues. Free radicals produce DNA strand breaks and altered bases, which if not repaired impact cell activity. Lipid peroxidation of polyunsaturated fatty acids disrupts the lipid bilayers that comprise the

**TABLE 1 The Cascade of Radiation Injury and Targets for Countermeasures**

| | | | | |
|---|---|---|---|---|
| **Radiation Exposure** | | | | |
| Damage: | Free radical generation | Damaged macromolecules affect signaling pathways | Cell death, failure to proliferate, progenitor cell depletion | Organ failure, bacterial translocation, sepsis, and death |
| Goal: | Prevent lipid peroxidation, DNA damage, protein oxidation | Prevent apoptosis, restore proper cell signaling | Stimulate proliferation of surviving progenitor cells | Prevent infection and lethality |

cell membranes. Protein thiols are particularly sensitive to free radicals; their oxidation can affect many cell functions.

Because free radicals are a normal part of oxidative metabolism, the body has evolved antioxidant mechanisms to mitigate the damaging aspects of free radical generation. Superoxide dismutase (SOD) modifies superoxide ($O_2^-$) to produce hydrogen peroxide and water. Removal of the peroxide is also important since it can interact with metals to create the extremely reactive hydroxyl radicals ($OH^\bullet$). Catalase converts hydrogen peroxide into water and oxygen. Glutathione (GSH) peroxidase expends peroxide in the oxidation of a GSH to glutathione disulfide (GSSG).

Interventions at this level of the cascade of injury are usually either free radical scavengers or enzymatic mimics.

***4.1.1 Free Radical Scavengers.*** The earliest radiation countermeasures focused on the free radical scavenging ability of aminothiols [18, 36–38]. Unfortunately, although cysteine, the first aminothiol radioprotectant, was efficacious, it caused nausea and vomiting that precluded its use [39]. In the 1960s, Walter Reed Army Institute of Research conducted an intense search for an effective radioprotectant. Among the most promising compounds produced was WR2721, also known as *amifostine*. Amifostine has been approved as a preventive measure for xerostomia with clinical radiation. As with cysteine, however, the associated hypotension and nausea have limited its usefulness in healthy individuals at risk of radiation injury [18]. In addition, amifostine has a short duration of effectiveness, requiring injection within 30 min of exposure. More recent studies have explored different formulations and dosing of amifostine that might improve its usefulness. Reducing the administered concentration reduced the toxicity while sustaining some efficacy but still only within a very short time window [40]. Use of a slow release formulation (implanted pellets) broadened the time window, up to a couple of hours in the mouse, but toxicity was still a problem [40]. Reformulation of amifostine with nanoparticles that allowed oral administration showed some measure of success [41]. Although

**TABLE 2 Selected Drugs in Development for Acute Radiation Syndrome**

| Drug | Endpoint(s) | Comments |
|---|---|---|
| | **Antioxidants** | |
| Amifostine | FDA approved for mucositis | Significant toxicity |
| Alpha tocopherol | Survival in mice | |
| Tempol | Survival in mice | IND for radiation-induced alopecia; systemic toxicity |
| Eukarion-189 | Survival in mice | |
| Seleniomethionine | Survival in mice | Selenium synergizes with other radioprotectants |
| | **Altered cell signaling** | |
| Genistein | Survival in mice | Oral efficacy |
| Statins | Protection of lungs | |
| Prostagladins | Survival in mice | Significant toxicity |
| | **Progenitor cell depletion/immunomodulators** | |
| G-CSF | Survival in mice and NHPs | IND for radiation injury; multiple daily injections |
| | FDA approved as antineutropenic | |
| Pegylated G-CSF | Survival in mice and NHPs | Weekly injections |
| | FDA approved as antineutropenic | |
| KGF | FDA approved for mucositis | |
| IL-1 | Survival in mice | Significant toxicity |
| 5-AED | Survival in mice and NHPs | IND for radiation injury |
| Beta glucans | Survival in mice | |
| OK-432 | Survival in mice | |

not quite as effective as the injected amifostine, treatment with the oral nanoparticles 1 h prior to lethal radiation exposure conferred significant improvement in the 30-day survival of mice [41]. Additional assessment and optimization is necessary before this approach can be implemented.

Naturally occurring antioxidants have attracted attention because of the expectation of low toxicity [see 37, 42 for reviews]. Among the most promising agents to date are the vitamin E analogs. $\alpha$-Tocopherol, for example, reduces lethality in rodents when administered prophylactically or therapeutically [43–45]. A single subcutaneous injection of 400 IU given 24 h prior to lethal irradiation shifted the 50% lethal dose from 8.96 to 11.14 Gy (a dose reduction factor, [DRF] of 1.23) [46]. The radioprotective action of $\alpha$-tocopherol has long been attributed to its antioxidant activity [47], protecting membranes from radiation damage [48] by inhibiting lipid peroxidation [49]. In addition, $\alpha$-tocopherol and its analogs decrease free radical- and radiation-induced DNA damage [37, 50, 51]. Non-antioxidant mechanisms [52, 53] such as inhibition of protein kinase C [54] also have been proposed for the efficacy of $\alpha$-tocopherol as a radioprotectant.

***4.1.2 Antioxidant Enzymes.*** SOD, catalase, and GSH peroxidase are effective natural defense mechanisms for free radical injury following radiation exposure. As proteins, however, they are not readily administered as drugs. Several laboratories have been exploring approaches to use these enzymes through novel delivery systems [55–58]. For example, proof of principle for gene therapy was generated in an *in vitro* study where retroviral SOD gene transfer decreased DNA fragmentation and increased clonogenic survival [58] in irradiated murine hematopoietic progenitor cells. In a mouse model, liposomes were used to deliver the SOD gene to the esophagus or to the lungs. This treatment increased survival after thoracic irradiation [55, 56].

Another alternative is the development of small compounds that mimic the antioxidant enzyme activity [59–63]. One example of this approach is the development of nitroxides such as Tempol. These nitroxides are small molecules that act as an SOD [64]. When mice were injected intraperitoneally, 5–10 min prior to irradiation, the LD50/30 shifted from 7.84 to 9.97 Gy, corresponding to a DRF of 1.27 [65]. However, hypotension and epileptic activity were associated with the administration of Tempol [66, 67]. Several other nitroxides have been tested and Tempol-H (the reduced, hydroxylamine form of Tempol) was found to provide similar radioprotection with fewer hemodynamic side effects [61]. Recently a new SOD-catalase mimetic Eukarion-189 (EUK-189) was tested for its effects against radiation damage in the rat. Intraperitoneal injection of EUK-189, 1–2 h after lung irradiation reduced the formation of micronuclei in lung fibroblasts, reflecting reduced DNA damage [63]. Additional studies will be necessary to assess its potential as a countermeasure for ARS.

Selenium, a nutritional requirement in trace amounts, is present at each of four active sites of GSH peroxidase [68] and is necessary for the enzyme's activity. Selenomethionine injected intraperitoneally, any time between 24 h and 15 min prior to a lethal radiation exposure improved the 30-day survival [69]. Selenium appears to synergize with vitamin E. Together they are more effective than either alone in promoting survival from lethal radiation exposure [37]. The combination of injected sodium selenite and vitamin E for 10 days prior to radiation normalized the levels of blood GSH, GSH peroxidase, SOD, and plasma lipid peroxides after exposure [70]. The actual mechanism by which selenium might confer a radioprotective effect is not yet known; possibilities under consideration are direct induction of GSH and a mimetic effect of the enzyme [37].

## 4.2 Altered Cell Signaling

As a consequence of radiation exposure and the resulting damage, a variety of intracellular and extracellular signaling pathways [71–74] are activated. Signals that trigger apoptosis, cell cycle arrest, and cell repair provide opportunities for the cell to either recover from the damage or die. Therapeutics are being developed to prevent apoptosis and thereby, promote survival of progenitor cells. Targets for this strategy can be the upregulation of nuclear factor kappa-B (NF$\kappa$B), which usually acts to enhance cell survival. Alternatively, drugs may be designed to block the proapoptotic pathways, such as those involving p53 or p73. Another approach for countermeasure development is to trigger cell cycle arrest to allow time for cell repair and to promote survival of progenitor and stem cells. In addition, radiation causes functional changes in growth factor receptors, such as members of the ErbB family and tumor necrosis factor $\alpha$ (TNF$\alpha$) and transforming growth factor $\beta$ (TGF$\beta$) receptors, which affect proliferation, growth, and apoptosis [71]. These receptors can serve as targets for new drugs.

Radiation also initiates an inflammatory response with the release of proinflammatory cytokines (induced, in part, by NF$\kappa$B) and other messengers. Countermeasures can intervene in the stimulated inflammatory responses. Included in this approach are modulators of heat shock protein, iNOS (inducible nitric oxide synthase), prostaglandins, and thrombin [72, 74, 75].

***4.2.1 Stimulation of Antiapoptotic Pathways.*** Several drugs are currently in development that are designed to block apoptosis. These include agents with direct activity on the apoptotic signaling pathways and drugs that activate the pathways through receptor mechanism (e.g. toll-like receptors, TLRs).

ON01210 is a dual kinase inhibitor of Chk2 and c-Abl that reduces radiation-induced p73 expression and apoptosis *in vitro* [76]. When injected prior to irradiation, it has been shown to enhance the survival of mice [77]. Activation of toll-like receptor 5 (TLR5) releases NF$\kappa$B and stimulates the innate immune system [78–80]. Acting through TRL5, CBLB502, a derivative of the flagellin secreted by *Salmonella typhimurium*, can promote survival from a lethal radiation dose in nonhuman primates when injected prior to exposure [81, 82]. Through interaction with TLR9, CpG-ODN (cytosine-phosphate-guanosine oligodeoxynuclides) mimics bacterial DNA to stimulate the innate immune system and activate NF$\kappa$B [83, 84]. Preradiation treatment of mice with CpG-ODN improved 30-day survival [85].

***4.2.2 Other Pathways.*** Genistein is a soy-derived isoflavone that inhibits protein tyrosine kinase acting through the ErbB-2 pathway [86]. Genistein, injected subcutaneously 24 h prior to radiation, enhanced the 30-day survival of mice with a DRF of 1.16 [87]. No toxicity was observed, even with doses more than 10 times the radioprotective dose. Studies in mice demonstrate that oral administration is also effective in promoting survival when given for 4–7 consecutive days prior to radiation exposure [88, 89]. The survival benefit conferred by Genistein was related to the protection of the hematopoietic progenitor cells in the bone marrow and accelerated recovery of circulating neutrophils and platelets [90].

Endothelial thrombomodulin (TM) plays an important modulatory role in endothelial microvasculature. Through interaction with Protein C, it has anti-inflammatory properties; by binding thrombin, it suppresses coagulation [72, 91]. Clinical and animal studies show that ionizing radiation reduces intestinal endothelial TM down to 10–15% of unirradiated tissue levels [92, 93]. The decrease correlates with the severity of structural and functional tissue injury [93, 94]. Statins, used clinically to lower cholesterol, appear to have some promise in modulating this pathway and mitigating the effects of radiation. In endothelial cells *in vitro*, statins upregulate TM [91, 95], protect against radiation-induced cell death [96], and reduce levels of proinflammatory cytokines induced by radiation [97]. *In vivo*, they protect the intestines [98] and lungs [99] from the effects of radiation after localized exposure. The TM-Protein C pathway and the possible role of statins as radiation countermeasures require additional attention.

The prostaglandin, 16,16-dimethyl prostaglandin E2 (dmPGE2), has shown significant survival benefit in the mouse. DRFs between 1.25 and 1.72 have been reported [100–103] after preradiation administration in various strains of mice. The effects were even more dramatic when dmPGE2 was used in combination with other agents such as WR2721 [101]. Although effective, the toxicity of the drug may preclude its use. Toxic side effects include diarrhea, reduced locomotor activity, and sedation [100, 102, 104].

### 4.3 Progenitor Cell Depletion

Disruption of cell signaling pathways leads to organ failure from cell death, failure of cells to proliferate, and progenitor cell depletion. In the bone marrow, the hematopoietic progenitor cells are very vulnerable to damage from ionizing radiation and the mature cells are much less so. As a result, the cells are maintained in the circulation until the mature cells complete their normal life span (8–10 days). As these cells die, fewer cells are available to replace them and the overall population drops. It can be several weeks before the cells reach their minimum level. The rate and severity of the cell loss is radiation dose dependent. The loss of neutrophils increases susceptibility to infection. Platelet loss results in deficits in coagulation and concomitant hemorrhage.

In the gut, the progenitor cells of the intestinal villi, crypt cells, also are sensitive to radiation. As the crypt cells die, mature cells are not available to repopulate the villi. In addition, there is injury to the microvasculature of the mucosa and submucosa. These events occur within 5–10 days of irradiation, depending on the radiation dose. At the lower ranges of GI syndrome, damage to the functional properties of the epithelial cells can occur, which can lead to a loss of fluids and electrolytes.

Countermeasures at this level of the cascade of radiation injury are usually designed to stimulate the proliferation and differentiation of surviving progenitor cells.

#### *4.3.1 Cytokines: G-CSF and GM-CSF.*

A number of studies have demonstrated the efficacy of G-CSF and granulocyte-macrophage colony-stimulating factor (GM-CSF) in animal models. They are approved for use for neutropenia associated with cancer chemotherapy and have been used off-label for several radiation accident victims [14]. In rodents, [105–107] the cytokines have been shown to increase survival after an otherwise lethal radiation exposure and to speed the recovery from myelosuppression.

These observations have been extended to radiation injury in nonhuman primates and canines. In lethally irradiated dogs [108–110] recombinant G-CSF, started within a few hours of radiation exposure and injected daily for about 3 weeks, reduced the duration of neutropenia and had a significant survival benefit compared to supportive care alone, with a DRF of approximately 1.5 [7]. The efficacy of G-CSF was lost if initial administration was delayed by a week [109]. Nash [111] found that, in the dog, GM-CSF was much less effective than G-CSF both in preventing lethality and promoting hematopoietic recovery.

As in the canine model, recombinant human granulocyte colony-stimulating factor (rhG-CSF) was found to significantly reduce the duration of neutropenia [112] in another model. Nonhuman primates (NHPs) were exposed to 7-Gy $\gamma$ radiation, and received rhG-CSF subcutaneously daily, beginning 1 day after radiation for 23 days. All irradiated animals received clinical support (including antibiotics, blood transfusions, and fluids). Although the cytokines (GM-CSF and G-CSF) significantly shortened the period of neutropenia, whole blood or platelet transfusions were required to prevent lethality. Addition of thrombopoietin (TPO) to the treatment protocol eliminated this requirement [113, 114]. In contrast to prior studies in the dog, a study in the NHP demonstrated efficacy of GM-CSF that was not lost if treatment was delayed for 7 days [115].

Although G-CSF and GM-CSF are tolerated fairly well by patients, they do have occasional severe side effects that mandate supervision by a physician [116]. The requirement for multiple injections has been addressed by a reformulation into a pegylated form that can be injected on a weekly basis instead of daily [3].

As noted above, the combined use of G-CSF and TPO has been proposed to enhance platelet recovery [117]. Current investigations are exploring additional combinations of cytokines designed to stimulate recovery of multiple hematopoietic lineages (granulocyte-macrophage, erythrocytic, thrombocytic, etc. ) [117].

***4.3.2 Other Cytokines.*** Interleukin 1 (IL-1) is a stimulator of normal hematopoiesis, acting both directly on the primitive stem cells and indirectly through release of other factors. IL-1 has been shown to be effective against radiation injury in the mouse primarily when administered before radiation exposure [118–127] and to some extent when administered early after exposure as well [122]. Because of its pyrogenic and inflammatory properties [118], clinical applications for radioprotection are limited. In an effort to produce a molecule that maintains the functional domains but lacks the toxicity of IL-1, a synthetic nonapeptide was developed that mimics immunostimulation in vivo without the inflammatory effects [128]. Preliminary studies in a mouse demonstrate potential efficacy as a radioprotectant in mice exposed to 8.5 Gy irradiation [129].

KGF has recently been approved for treatment of mucositis after radiation therapy. Since it promotes the regeneration of crypt cells in GI mucosa, it has been proposed as a possible therapy for the GI syndrome after whole-body irradiation. Preliminary assessments on the survival of the irradiated mouse show promise [130–132].

***4.3.3 Other Immunomodulators.*** 5-Androstenediol (5-AED) is a naturally occurring, nonandrogenic adrenocortical steroid. It has been shown to promote survival in both mice and nonhuman primates [133–137]. In mice, the 50% lethal dose of $\gamma$-radiation was shifted from approximately 9.5 to 12 Gy, corresponding to a DRF of 1.26 [133]. In nonirradiated mice, 5-AED increased the numbers of circulating neutrophils and platelets; histologically, bone marrow showed marked myelopoiesis [133, 138]. Administration of 5-AED resulted in increased numbers of NK (natural killer) cells and their activation [133]. In addition, the steroid promoted resistance to infection when radiation was combined with a bacterial [133] or viral [136] challenge. With administration 24 h prior to sublethal irradiation of mice, 5-AED mitigated the expected neutropenia and thrombocytopenia; the AED-induced changes in blood elements in irradiated animals persist for at least several weeks [138]. In an *in vitro* model, 5-AED enhances clonogenic survival of irradiated human hematopoietic progenitor cells through NF$\kappa$B-dependent pathways [139]. The efficacy of 5-AED on radiation injury has been confirmed in nonhuman primates. 5-AED reduced the magnitude and duration of neutropenia, thrombocytopenia, and anemia when given once a day for 5 days starting within several hours of radiation exposure [137]. In addition, preliminary data demonstrate that 5-AED provides survival benefit in nonhuman primate. Since 5-AED is a small, stable molecule that, to date, has no demonstrated toxicity, it may provide a viable alternative to G-CSF as a treatment for the hematopoietic syndrome.

Beta glucans are polysaccharides that act as nonspecific immune system stimulants. Particulate glucan-P and soluble glucan-F have shown significant capabilities of survival enhancement after lethal radiation in the mouse [140–142]. The most pronounced effects were observed when glucan was administered 1 day before irradiation. The enhanced survival in glucan-treated mice in part appeared to be mediated by an enhanced resistance to the enteric pathogens that cause infection following radiation-induced hematopoietic and immune depression. Both glucan-P and glucan-F appear to function specifically by enhancing hemopoietic recovery, enhancing the recovery of peripheral blood white

cell and platelet numbers and increasing endogenous pluripotent hemopoietic stem cell numbers in sublethally irradiated mice. Glucan-P consistently offered slightly better protection than glucan-F at all radiation doses. More recently, Betafectin PGG-glucan (poly-[1-6]–D-glucopyranosyl-[1-3]–D-glucopyranose glucan), a beta-(1,3)glucan with broad-spectrum anti-infective activities, was tested on hematopoietic recovery in the irradiated mouse and cyclophosphamide-treated cynomolgus monkeys. PGG-glucan accelerated hematopoietic recovery and reduced the duration of the neutropenia in both models [143]. PGG-glucan was also found to mobilize peripheral blood progenitor cells (PBPC) that would promote reseeding of ablated bone marrow [144].

OK-432 is an immunomodulator derived from a killed streptoccocus preparation. It has been tested in clinical trials as an anticancer agent [e.g. 145]. Data from animal models suggest that it may provide survival benefits when used either alone or in combination with other agents after radiation exposure. Several studies demonstrated an increase in the number of animals surviving a lethal radiation dose [146–151]. With a single treatment given to a mouse immediately after radiation, the 50% lethal dose shifted from 7.55 Gy to 8.45 Gy. The efficacy was significantly improved when multiple injections of OK-423 were given, every other day through day 11. Under these conditions, the LD50 was 9.56, a DRF of 1.26. A delay in the onset of treatment course for 72 h was less effective but still significantly increased survival [150]. OK-432 in combination with other agents such as G-CSF [149] and antibiotics [151] improved the efficacy.

### 4.4 Organ Failure and Infection

Even with the use of efficacious radiation countermeasures that intervene at various steps in the cascade of injury, additional interventions are likely to be necessary. G-CSF for example does not reverse the thrombocytopenia, necessitating platelet transfusions. Because of the neutropenia and reduced integrity of the gut, sepsis is likely and antimicrobials are inevitably needed. These treatment regimens are briefly addressed here.

***4.4.1 Supportive Care.*** The availability of supportive care, even without any other countermeasures, can provide significant therapeutic efficacy. MacVittie [152] assessed the value of supportive care in irradiated dogs over a wide dose range. Antibiotics with fluids, nutrition, and platelet transfusions provide a DRF of 1.3 in irradiated canines [152]. The radiation dose that caused 50% lethality increased from 2.59 Gy to 3.37 Gy with supportive care alone. Studies demonstrate a similar shift in the LD50 in nonhuman primates with supportive care [113, 115, 153, 154] compared to historical controls [155, 156].

Antibiotics by themselves can provide significant improvements in outcome following radiation exposure, since control of infection during the severe postradiation neutropenia is a limiting factor for survival [157]. The most effective antimicrobial therapy is directed toward both gram-negative and gram-positive bacteria, sparing indigenous intestinal anaerobic bacteria. In irradiated mice, the radiation exposure significantly reduces both aerobic and anaerobic bacteria in the gut within the first few days of exposure; but the aerobic bacteria rebound in about a week while the anaerobes stay depressed [158]. Translocation of these pathogenic organisms through the gut poses the risk of fatal bacteremia. An antibiotic strongly effective on both anaerobes and aerobes (e.g. metronidazole) increased mortality in irradiated mice [159] while quinolones promoted survival after lethal radiation, in part due to their ability to preserve the anaerobic gut flora [158, 160].

***4.4.2 Cellular Therapies.*** Bone marrow transplants and stem cell transplants can save lives in patients with malignant hematological conditions. Allogenic transplants have been performed in the treatment of a number of radiation accident victims [3, 161–165]. Despite transient engraftment with the transplanted cells, almost all patients showed autologous hematopoietic reconstitution. The benefits of cellular therapies have been difficult to validate; most do not survive. It is uncertain whether the transplants have had any impact on survival. The accident victims who showed hematopoietic recovery, died from failure of other organs [14, 166, 167]. In the 1999 accident in Tokaimura, Japan [14], two of the three victims received allogenic stem cell transplants. Although both began to show proliferation of the donor cells, this was only transient; their own cells eventually took hold. The impact on survival time is hard to assess. Advances in the technology may eventually allow production of adequate supplies of hematopoietic progenitor cells that can be easily administered without immunological complications. These approaches will need to be administered in combination with therapeutic approaches to enhance recovery of other organs.

## 5 ADDITIONAL TREATMENT CONSIDERATIONS

### 5.1 Radiation Quality and Dose Rate

Many disaster scenarios could involve high levels of neutrons mixed with $\gamma$ radiation. Unfortunately, far less is known about the effects of neutrons on hematopoiesis and immune function than about the effects of $\gamma$ radiation. Moreover, there are very few studies of pharmacological countermeasure efficacy in the context of neutron irradiation. Comparable clinical support (fluids, antibiotics, and platelets or whole blood) is more effective with gamma exposure (DRF = 1.3) compared to a mixed neutron/gamma field (DRF = 1.21) in dogs [152]. The radioprotectant effects of aminothiols [168–170], synthetic trehalose dicorynomycolate [171–174], and prostaglandins [175] have been examined in mice exposed to neutrons. A small number of studies have examined the effects of cytokines on animals recovering from acute whole-body neutron irradiation [115, 176, 177].

The dose rate of radiation exposure also can have a significant effect on the biomedical consequences, which would impact medical treatment. For the same total radiation dose, exposure at a lower dose rate has a sparing effect. Prolonging the dose rate significantly increases the LD50. At an exposure of 7 Gy/min the LD50 in mice was 7.88 Gy. At about 0.7 Gy/min, this increased to 8.5 Gy. With further reduction of the dose rate to 0.025 Gy/min, the LD50 increased to almost 11 Gy [see 178]. Although the effects of very low dose rates have been assessed particularly on the hematological response to radiation [e.g. 179], the biomedical consequences associated with dose rates that might be expected in a heavy fallout field (1–6 Gy/day) have not been well characterized.

### 5.2 Partial-Body Exposures

An exposure in an uncontrolled environment is likely to be nonhomogeneous because of the physical environment and partial-body shielding that would occur. Any shielding of bone marrow increases the probability of sparing progenitor and stem cells that can

repopulate the hematopoietic system and improve survival and recovery. The nadir of neutropenia correlated with the volume of irradiated bone marrow [180]. Recovery depends on the reseeding of the damaged bone marrow with cells from the protected marrow [181–184]. A myeloablative dose of 11.7 Gy to the upper body of the dog, which damages about 70% of the bone marrow, causes an increase in proliferation and differentiation of granulocyte/macrophage colony forming cells (GM-CFC) in the protected marrow. The reseeding becomes evident by day 7 with the appearance of progenitor cells in the ablated bone marrow [180, 183, 184]. The hematopoietic recovery continues for about 3 weeks but then levels off until a secondary increase begins about 4 months after the radiation exposure. It takes about a year for the marrow to fully repopulate in this dog model [180, 183, 184]. When only the lower body is exposed, ablating 30% of the bone marrow, the time course is the same [180]. Currently, research is exploring approaches to enhance the repopulation of the bone marrow by mobilizing cells from the spared marrow [13, 182, 185].

Because of the repopulation of progenitor cells from spared marrow, radiation doses that would be lethal if given as a total body exposure can be survived, even without treatment, with partial-body exposures. Hematopoietic reconstitution has been observed in accident victims with partial-body radiation exposure of up to 10–12 Gy [14]. Ultimate survival, however, may depend on the extent of damage to other organs.

### 5.3 Combined Injury

In the event of a nuclear or radiological incident, concurrent exposures of radiation with traumatic injuries, infectious disease, or toxins are likely. These combined injuries can dramatically exacerbate the lethality of radiation.

Traumatic injuries increase the mortality associated with the ARS [186–188]. In a mouse model, for example, a wound that by itself caused minimal lethality shifted the 50% lethal radiation dose from 9.60 Gy to 7.6 Gy, and had a dose modification factor (DMF) of 1.26. Similarly a minimally lethal burn had a DMF of 1.17 [188]. Radiation doses that by themselves were fully survivable become fatal when combined with a traumatic injury. The mechanism of synergism is not known but an increase in the susceptibility to infection and enhanced translocation of gut bacteria are thought to contribute to lethality [189, 190]. Radiation delays recovery from wounds [191]. Although closing a wound may reduce some of the synergistic effects [192], treatment (excision and closure) of a thermal burn may not provide the same benefit [193]. Because of these interactions, current recommendations are to perform any surgical procedures as soon as possible after radiation exposure; waiting can increase lethality [194–196].

Similarly, combined exposures to radiation and an infectious agent can be lethal even if neither insult by itself causes significant lethality. Since radiation impairs the immune system, susceptibility to infection increases. Animal studies demonstrate that after radiation exposure, fewer microbes are required to establish an infection and the clinical manifestations are more severe [133, 197–200]. For example, exposing sublethally irradiated mice to *Klebsiella pneumoniae* that caused 5% mortality without radiation elicited 100% mortality [133, 199]. The higher the radiation dose, the fewer microbes that were needed to induce lethality. Susceptibility to infection and mortality from *K. pneumoniae* increased within 1 day of exposure to $\gamma$ radiation and remains high for at least 2 weeks.

## 6 FUTURE RESEARCH DIRECTIONS

With the increasing concerns about radiological and nuclear terrorism, the requirement for adequate medical countermeasures has become a national research priority. Although few drugs are currently approved for treatment of radiation injury, many are in the pipeline. New efforts are beginning to focus on drugs directed at particular pathways in the cascade of radiation injury. As more is discovered about the apoptotic pathways and cell cycle checkpoints, new agents will be defined that can modulate these processes. With countermeasures directed toward specific targets, it may be possible to limit the toxicological side effects of more broadly effective agents. New delivery systems, such as slow release capsules or transdermal patches, may simplify the logistics of administration.

Current efforts are generally focused on single compounds. Using drug combinations may be an effective approach to limiting toxicity by reducing the dosage of each component of a cocktail. Because ARS is a spectrum of syndromes afflicting multiple organ systems, it is likely that multiple drugs will be needed to allow survival at the higher radiation doses. For example, combinations for both the hematopoietic syndrome and the GI syndrome are likely to be required. As prospects of survival at increasingly high radiation doses improve, the late effects of radiation such as fibrosis of the lung and kidney will need to be addressed. While some efforts in this area are ongoing, they have not been emphasized.

The current focus for radiation countermeasures has been on treating radiation injury alone. In future efforts, it will be important to consider many other factors that can modulate the radiation response and possibly affect the efficacy of the treatments. For most of the countermeasures under development, it is unknown if their efficacy will be affected by combined injury, neutron exposures, dose rates associated with heavy fallout fields, or partial-body exposures.

While much work remains to be done, the recent advances in the field demonstrate great promise for development of effective countermeasures for radiation injury.

## REFERENCES

1. Anno, G. H., Baum, S. J., Withers, H. R., and Young, R. W. (1989). Symptomatology of acute radiation effects in humans after exposure to doses of 0.5-30Gy. *Health Phys.* **56**, 821–838.
2. Coleman, C. N., Blakely, W. F., Fike, J. R., MacVittie, T. J., Metting, N. E., Mitchell, J. B., Moulder, J. E., Preston, R. J., Seed, T. M., Stone, H. B., Tofilon, P. J., and Wong, R. S. L. (2003). Molecular and cellular biology of moderate dose (1-10 Gy) radiation and potential mechanisms of radiation protection: Report of a Workshop at Bethesda, Maryland, December 17-18, 2001. *Radiat. Res.* **159**, 812–834.
3. Waselenko, J. K., MacVittie, T. J., Blakely, W. F., Pesik, N., Wiley, A. L., Dickerson, W. E., Tsu, H., Confer, D. L., Coleman, C. N., Seed, T., Lowry, P., Armitage, J. O., and Dainiak, N. (2004). Medical management of the acute radiation syndrome: recommendations of the Strategic National Stockpile Radiation Working Group. *Ann. Intern. Med.* **140**, 1037–1051.
4. Armed Forces Radiobiology Research Institute. (2003) *Medical Management of Radiological Casualties*, www.afrri.usuhs.mil.
5. NCRP. (1985) *Management of Internally Deposited Radionuclides*. Report no. 65, National Council on Radiation Protection and Measurements, Bethesda.

6. Cervany, T. J. (1989). Treatment of internal radionuclide contamination. In *Medical Consequences of Nuclear Warfare: Textbook of Military Medicine*, R. I., Walker, and T., Jan Cervany, Eds. Office of the Surgeon General, Falls Church, Virginia, pp. 55–65.
7. Daniak, N., Waselenko, J. K., Armitage, J. O., MacVittie, T. J., and Farese, A. M. (2003). The hematologist and radiation casualties. *Hematology (Am. Soc. Hematol. Educ. Program)* 473–496.
8. Mettler, F. A. Jr, and Voelz, G. L. (2002). Major radiation exposure—what to expect and how to respond. *N. Engl. J. Med.* **346**(20), 1554–1561.
9. Koenig, K. L., Goans, R. E., Hatchett, R. J., Mettler, F. A. Jr, Schumacher, T. A., Noji, E. K., and Jarrett, D. G. (2005). Medical treatment of radiological casualties: current concepts. *Ann. Emerg. Med.* **45**(6), 643–652.
10. British Medical Association's Board of Science and Education. (1983). *The Medical Effects of Nuclear War*. John Wiley & Sons, New York.
11. Flynn, D. F., and Goans, R. E. (2006). Nuclear terrorism: triage and medical management of radiation and combined-injury casualties. *Surg. Clin. North Am.* **86**(3), 601–636.
12. Holdstock, D., and Waterston, L. (2000). Nuclear weapons, a continuing threat to health. *Lancet* **355**(9214), 1544–1547.
13. Baranov, A. E., Selidovkin, G. D., Butturini, A., and Gale, R. P. (1994). Hematopoietic recovery after 10-Gy acute total body radiation. *Blood* **83**(2), 596–599.
14. Maekawa, K. (2002). Overview of medical care for highly exposed victims in the Tokaimura accident. In *The Medical Basis for Radiation-Accident Preparedness: The Clinical Care of Victims*, R. C., Ricks, M. E., Berger, and F. M., O'Hara, Eds. Parthenon, New York, pp. 313–318.
15. Mettler, F. A. Jr, and Guskova, A. K. (2001). Treatment of acute radiation syndrome. In *Medical Management of Radiation Accidents*, I. A., Gusev, A. K., Guskova, and F. A., Mettler, Eds. CRC Press, Washington, DC, pp. 53–68.
16. Ansari, A. (2004). Dirty bomb pills, shots, weeds and spells. *Health Phys. News* **32**, 1–4.
17. MacVittie, T. J., and Farese, A. M. (2002). Cytokine-based treatment for acute radiation-induced myelosuppression: preclinical and clinical perspective. In *The Medical Basis for Radiation-Accident Preparedness; The Clinical Care of Victims*. R. C., Ricks, M. E., Berger, and F. M., O'Hara Jr, Eds. Parthenon Publishing, Boca Raton, pp. 53–72.
18. Weiss, J. F. (1997). Pharmacologic approaches to protection against radiation-induced lethality and other damage. *Environ. Health Perspect.* **105**(Suppl. 6), 1473–1478.
19. NCRP. (1977). *Protection of the thyroid gland in the event of releases of radioiodine*. Report no. 55. National Council on Radiation Protection and Measurements, Washington, DC.
20. US Food and Drug Administration, Center for Drug Evaluation and Research. (2001). *Guidance: Potassium Iodide as a Thyroid Blocking Agent in Radiation Emergencies*. Available at: http://www.fda.gov/cder/guidance/4825fnl.pdf, Accessed January 5 2007.
21. National Research Council. (2004). *Distribution and Administration of Potassium Iodide in the Event of a Nuclear Incident*. National Academies Press, Washington, DC.
22. Farina, R., Brandao-Mello, C. E., and Oliveira, A. R. (1991). Medical aspects of 137-Cs decorporation: the Goiania radiological accident. *Health Phys.* **60**(1), 63–66.
23. US Food and Drug Administration. (2004). *FDA Approves Drugs to Treat Internal Contamination from Radioactive Elements*. http://www.fda.gov/bbs/topics/news/2004/NEW01103.html, Accessed January 5 2007.
24. International Atomic Energy Agency. (1998). *Dosimetric and Medical Aspects of the Radiological Accident in Goiania in 1987*. Publication TECDOC 1009. International Atomic Energy Agency, Vienna.

25. Jagtap, V. S., Sonawane, V. R., Pahuja, D. N., Rajan, M. G., Rajashekharrao, B., and Samuel, A. M. (2003). An effective and better strategy for reducing body burden of radiostrontium. *J. Radiol. Prot.* **23**(3), 317–326.
26. Sonawane, V. R., Jagtap, V. S., Pahuja, D. N., Rajan, M. G., and Samuel, A. M. (2004). Difficulty in dislodging in vivo fixed radiostrontium. *Health Phys.* **87**(1), 46–50.
27. Pellmar, T. C., and Rockwell, S. (2005). The radiological/nuclear threat countermeasures working group. priority list of research areas for radiological nuclear threat countermeasures. *Radiat. Res.* **163**(1), 115–123.
28. US Food and Drug Administration. (2003). *Radiogardase™ Insoluble Prussian blue capsules*. http://www.fda.gov/cder/foi/label/2003/021626lbl.pdf, accessed Jan 5, 2007.
29. Hollriegl, V., Rohmuss, M., Oeh, U., and Roth, P. (2004). Strontium biokinetics in humans: influence of alginate on the uptake of ingested strontium. *Health Phys.* **86**(2), 193–196.
30. Gong, Y. F., Huang, Z. J., Qiang, M. Y., Lan, F. X., Bai, G. A., Mao, Y. X., Ma, X. P., and Zhang, F. G. (1991). Suppression of radioactive strontium absorption by sodium alginate in animals and human subjects. *Biomed. Environ. Sci.* **4**(3), 273–282.
31. Chen, H., Luo, M., Sun, M., Hu, Y., Wang, Y., Jin, M., and Cheng, W. (2005). Decorporating efficacy of catecholaminocarboxylate chelating agents for thorium-234 and protective effects on associated radiation injury. *Int. J. Radiat. Biol.* **81**(4), 309–318.
32. Durbin, P. W., Kullgren, B., Xu, J., Raymond, K. N., Henge-Napoli, M. H., Bailly, T., and Burgada, R. (2003). Octadentate hydroxypyridinonate (HOPO) ligands for plutonium (i.v.): pharmacokinetics and oral efficacy. *Radiat. Prot. Dosimetry.* **105**(1-4), 503–508.
33. Guilmette, R. A., Hakimi, R., Durbin, P. W., Xu, J., and Raymond, K. N. (2003). Competitive binding of Pu and Am with bone mineral and novel chelating agents. *Radiat. Prot. Dosimetry.* **105**(1-4), 527–534.
34. Fukuda, S. (2005). Chelating agents used for plutonium and uranium removal in radiation emergency medicine. *Curr. Med. Chem.* **12**(23), 2765–2770.
35. Martinez, A. B., Cabrini, R. L., and Ubios, A. M. (2000). Orally administered ethane-1-hydroxy-1,1-biphosphonate reduces the lethal effect of oral uranium poisoning. *Health Phys.* **78**(6), 668–671.
36. Maisin, J. R. (1998). Bacq, Alexander Award lecture–chemical radioprotection: past, present, and future prospects. *Int. J. Radiat. Biol.* **73**(4), 443–450.
37. Weiss, J. F., and Landauer, M. R. (2003). Protection against ionizing radiation by antioxidant nutrients and phytochemicals. *Toxicology.* **189**(1-2), 1–20.
38. Murray, D. (1998). Aminothiols. In *Radioprotectors Chemical, Biological and Clinical Perspectives*, E. A., Bump, and K., Malaker, Eds. CRC Press, Boca Raton, pp. 53–110.
39. Patt, H. M., Tyree, E. B., Straube, R. L., and Smith, D. E. (1949). Cysteine protection against x-irradiation. *Science.* **110**, 213–214.
40. Srinivasan, V., Pendergrass, J. A., Kumar, K. S., Landauer, M. R., and Seed, T. M. (2002). Radioprotection, pharmacokinetic and behavioral studies in mouse implanted with biodegradable drug (amifostine) pellets. *Int. J. Radiat. Biol.* **78**(6), 535–543.
41. Pamujula, S., Kishore, V., Rider, B., Fermin, C. D., Graves, R. A., Agrawal, K. C., and Mandal, T. K. (2005). Radioprotection in mice following oral delivery of amifostine nanoparticles. *Int. J. Radiat. Biol.* **81**(3), 251–257.
42. Maurya, D. K., Devasagayam, T. P., and Nair, C. K. (2006). Some novel approaches for radioprotection and the beneficial effect of natural products Indian. *J. Exp. Biol.* **44**(2), 93–114.
43. Bichay, T. J., and Roy, R. M. (1986). Modification of survival and hematopoiesis in mice by tocopherol injection following irradiation. *Strahlenther. Onkol.* **162**(6), 391–399.
44. Kumar, K. S., Srinivasan, V., Toles, R., Jobe, L., and Seed, T. M. (2002). Nutritional approaches to radioprotection: vitamin E. *Mil. Med.* **167**(2 Suppl), 57–59.

45. Srinivasan, V., and Weiss, J. F. (1992). Radioprotection by vitamin E: injectable vitamin E administered alone or with WR- 3689 enhances survival of irradiated mice. *Int. J. Radiat. Oncol. Biol. Phys.* **23**(4), 841–845.

46. Seed, T., Kumar, S., Whitnall, M., Srinivasan, V., Singh, V., Elliott, T., Landauer, M., Miller, A., Chang, C. M., Inal, C., Deen, J., Gehlhaus, M., Jackson, W. III, Hilyard, E., Pendergrass, J., Toles, R., Villa, V., Miner, V., Stewart, M., Benjack, J., Danilenko, D., and Farrell, C. (2002). New strategies for the prevention of radiation injury: possible implications for countering radiation hazards of long-term space travel. *J. Radiat. Res. (Tokyo)* **43**(Suppl), S239–S244.

47. Burton, G. W., Joyce, A., and Ingold, K. U. (1982). First proof that vitamin E is major lipid-soluble, chain-breaking antioxidant in human blood plasma. *Lancet* **2**(8293), 327.

48. Mishra, K. P. (2004). Cell membrane oxidative damage induced by gamma-radiation and apoptotic sensitivity. *J. Environ. Pathol. Toxicol. Oncol.* **23**(1), 61–66.

49. Noguchi, N., and Niki, E. (1999). Chemistry of active oxygen species and antioxidants. In *Antioxidant Status, Diet, Nutrition, and Health*, A. M., Papas, Ed. CRC Press, Boca Raton, pp. 3–20.

50. Nair, C. K., Salvi, V., Kagiya, T. V., and Rajagopalan, R. (2004). Relevance of radioprotectors in radiotherapy: studies with tocopherol monoglucoside. *J. Environ. Pathol. Toxicol. Oncol.* **23**(2), 153–160.

51. Sweetman, S. F., Strain, J. J., and Mckelvey-Martin, V. J. (1997). Effect of antioxidant vitamin supplementation on DNA damage and repair in human lymphoblastoid cells. *Nutr. Cancer* **27**(2), 122–130.

52. Azzi, A., Breyer, I., Feher, M., Ricciarelli, R., Stocker, A., Zimmer, S., and Zingg, J.-M. (2001). Nonantioxidant functions of $\alpha$ tocopherol in smooth muscle cells. *J. Nutr.* **131**, 378s–381s.

53. Traber, M., and Packer, L. (1995). Vitamin E: beyond antioxidant function. *Am. J. Clin. Nutr.* **62**, 1501S–1509S.

54. Freedman, J. E., Farhat, J. H., Loscalzo, J., and Keany, J. F. Jr. (1996). $\alpha$-tocopherol inhibits aggregation of human platelets by a protein kinase C-dependent mechanism. *Circulation* **94**, 2434–2440.

55. Carpenter, M., Epperly, M. W., Agarwal, A., Nie, S., Hricisak, L., Niu, Y., and Greenberger, J. S. (2005). Inhalation delivery of manganese superoxide dismutase-plasmid/liposomes protects the murine lung from irradiation damage. *Gene Ther.* **12**(8), 685–693.

56. Epperly, M. W., Defilippi, S., Sikora, C., Gretton, J., and Greenberger, J. S. (2002). Radioprotection of lung and esophagus by overexpression of the human manganese superoxide dismutase transgene. *Mil. Med.* **167**(2 Suppl), 71–73.

57. Niu, Y., Shen, H., Epperly, M., Zhang, X., Nie, S., Cao, S., and Greenberger, J. S. (2005). Protection of esophageal multi-lineage progenitors of squamous epithelium (stem cells) from ionizing irradiation by manganese superoxide dismutase-plasmid/liposome (MnSOD-PL) gene therapy. *In Vivo.* **19**(6), 965–974.

58. Southgate, T. D., Sheard, V., Milsom, M. D., Ward, T. H., Mairs, R. J., Boyd, M., and Fairbairn, L. J. (2006). Radioprotective gene therapy through retroviral expression of manganese superoxide dismutase. *J. Gene Med.* **8**(5), 557–565.

59. Hahn, S. M., Sullivan, F. J., DeLuca, A. M., Krishna, C. M., Wersto, N., Venzon, D., Russso, A., and Mitchell, J. B. (1997). Evaluation of Tempol radioprotection in a murine tumor model. *Free Radic. Biol. Med.* **22**(7), 1211–1216.

60. Hahn, S. M., DeLuca, A. M., Coffin, D., Krishna, C. M., and Mitchell, J. B. (1998). In vivo radioprotection and effects on blood pressure of the stable free radical nitroxides. *Int. J. Radiat. Oncol. Biol. Phys.* **42**(4), 839–842.

61. Hahn, S. M., Krishna, C. M., DeLuca, A. M., Coffin, D., and Mitchell, J. B. (2000). Evaluation of the hydroxylamine Tempol-H as an in vivo radioprotector. *Free Radic. Biol. Med.* **28**(6), 953–958.
62. Kumar, K. S., Vaishnav, Y. N., and Weiss, J. F. (1988). Radioprotection by antioxidant enzymes and enzyme mimetics. *Pharmacol. Ther.* **39**(1-3), 301–309.
63. Langan, A. R., Khan, M. A., Yeung, I. W., Van Dyk, J., and Hill, R. P. (2006). Partial volume rat lung irradiation: the protective/mitigating effects of Eukarion-189, a superoxide dismutase-catalase mimetic. *Radiother. Oncol.* **79**(2), 231–238.
64. Mitchell, J. B., Samuni, A., Krishna, M. C., DeGraff, W. G., Ahn, M. S., Samuni, U., and Russo, A. (1990). Biologically active metal-independent superoxide dismutase mimics. *Biochemistry* **29**(11), 2802–2807.
65. Hahn, S. M., Tochner, Z., Krishna, C. M., Glass, J., Wilson, L., Samuni, A., Sprague, M., Venzon, D., Glatstein, E., Mitchell, J. B., and Russo, A. (1992). Tempol, a stable free radical, is a novel murine radiation protector. *Cancer Res.* **52**(7), 1750–1753.
66. Hahn, S. M., Lepinski, D. L., DeLuca, A. M., Mitchell, J. B., and Pellmar, T. C. (1995). Neurophysiological consequences of nitroxide antioxidants. *Can. J. Physiol. Pharmacol.* **73**(3), 399–403.
67. Hahn, S. M., Sullivan, F. J., DeLuca, A. M., Bacher, J. D., Liebmann, J., Krishna, M. C., Coffin, D., and Mitchell, J. B. (1999). Hemodynamic effect of the nitroxide superoxide dismutase mimics. *Free Radic. Biol. Med.* **27**(5-6), 529–535.
68. Halliwell, B., and Gutteridge, J. (1985). *Free Radicals in Biology and Medicine*, Oxford University Press, New York.
69. Weiss, J. F., Srinivasan, V., Kumar, K. S., and Landauer, M. R. (1992). Radioprotection by metals: selenium. *Adv. Space Res.* **12**, 223–231.
70. Noaman, E., Zahran, A. M., Kamal, A. M., and Omran, M. F. (2002). Vitamin E and selenium administration as a modulator of antioxidant defense system: biochemical assessment and modification. *Biol. Trace Elem. Res.* **86**(1), 55–64.
71. Dent, P., Yacoub, A., Contessa, J., Caron, R., Amorino, G., Valerie, K., Hagan, M. P., Grant, S., and Schmidt-Ullrich, R. (2003). Stress and radiation-induced activation of multiple intracellular signaling pathways. *Radiat. Res.* **159**(3), 283–300.
72. Hauer-Jensen, M., Fink, L. M., and Wang, J. (2004). Radiation injury and the protein C pathway. *Crit. Care Med.* **32**(5 Suppl), S325–S330.
73. Liu, S. S., Chan, K. Y., Leung, R. C., Law, H. K., Leung, T. W., and Ngan, H. Y. (2006). Enhancement of the radiosensitivity of cervical cancer cells by overexpressing p73alpha. *Mol. Cancer Ther.* **5**(5), 1209–1215.
74. McBride, W. H., Chiang, C. S., Olson, J. L., Wang, C. C., Hong, J. H., Pajonk, F., Dougherty, G. J., Iwamoto, K. S., Pervan, M., and Liao, Y. P. (2004). A sense of danger from radiation. *Radiat. Res.* **162**(1), 1–19.
75. Linard, C., Marquette, C., Mathieu, J., Pennequin, A., Clarencon, D., and Mathe, D. (2004). Acute induction of inflammatory cytokine expression after gamma-irradiation in the rat: effect of an NF-kappaB inhibitor. *Int. J. Radiat. Oncol. Biol. Phys.* **58**(2), 427–434.
76. Perkins, M. W., Cosenza, S. C., Ramana Reddy, M. V., Premkumar Reddy, E., Bell, S., Alfieri, A., and Kumar, S. (2006). Evaluation of radiation induced apoptotic pathway of the novel radioprotectant ON1210 by RNA interference (Abstract). *Annual Meeting of the Radiation Research Society* Philadelphia, PA, Nov 5–8, 2006.
77. Alfieri, A. A., Liu, L., Sharma, A., Gorla, G., Bell, S., Ramana, R. M., Cosenza, S., Reddy, P. E., and Guha, C. (2004). Radiation damage protection by the benzyl styryl sulfone analog, Ex-Rad. *Int. J. Radiat. Oncol. Biol. Phys.* **60**(Supplement 1), S367–S368.

78. Hayashi, F., Smith, K. D., Ozinsky, A., Hawn, T. R., Yi, E. C., Goodlett, D. R., Eng, J. K., Akira, S., Underhill, D. M., and Aderem, A. (2001). The innate immune response to bacterial flagellin is mediated by Toll-like receptor 5. *Nature* **410**(6832), 1099–1103.
79. Means, T. K., Hayashi, F., Smith, K. D., Aderem, A., and Luster, A. D. (2003). The Toll-like receptor 5 stimulus bacterial flagellin induces maturation and chemokine production in human dendritic cells. *J. Immunol.* **170**(10), 5165–5175.
80. Yu, Y., Nagai, S., Wu, H., Neish, A. S., Koyasu, S., and Gewirtz, A. T. (2006). TLR5-mediated phosphoinositide 3-kinase activation negatively regulates flagellin-induced proinflammatory gene expression. *J. Immunol.* **176**(10), 6194–6201.
81. Cleveland BioLabs Inc. (2006). *Protectan CBLB502*. http://wwwcbiolabscom/candidates/protectans.
82. Krivokrysenko, V. (2006). Single injection of novel radioprotector CBLB502 significantly increases survival of lethally irradiated non-human primates (poster). *9th Annual Force Health Protection Conference Albuquerque*, New Mexico, August 6–11, 2006.
83. Klinman, D. M. (2004). Use of CpG oligodeoxynucleotides as immunoprotective agents. *Expert Opin. Biol. Ther.* **4**(6), 937–946.
84. Takeshita, F., Ishii, K. J., Ueda, A., Ishigatsubo, Y., and Klinman, D. M. (2000). Positive and negative regulatory elements contribute to CpG oligonucleotide-mediated regulation of human IL-6 gene expression. *Eur. J. Immunol.* **30**(1), 108–116.
85. Srinivasan, V., Villa, V., Jackson, W. E. III, Klinman, D. M., and Whitnall, M. H.. Radiation protection by cytosine-phosphate-guanine (CpG) motif containing oligodeoxynucleotides (CpG ODN) in mice exposed to cobalt-60 gamma radiation (abstract). *2006 Annual Meeting of the Radiation Research Society* Philadelphia, PA, Nov 5–8, 2006.
86. Valachovicova, T., Slivova, V., and Sliva, D. (2004). Cellular and physiological effects of soy flavonoids. *Mini Rev. Med. Chem.* **4**(8), 881–887.
87. Landauer, M. R., Srinivasan, V., and Seed, T. M. (2003). Genistein treatment protects mice from ionizing radiation injury. *J. Appl. Toxicol.* **23**(6), 379–385.
88. Zhou, Y., and Mi, M. T. (2005). Genistein stimulates hematopoiesis and increases survival in irradiated mice. *J. Radiat. Res. (Tokyo)* **46**(4), 425–433.
89. Davis, T. A., Clarke, T. K., Mog, S. R., and Landauer, M. R. (2007). Subcutaneous administration of genistein prior to lethal irradiation supports multilineage, hematopoietic progenitor cell recovery and survival. *Int. J. Radiat. Biol.* **83**(3), 141–151.
90. Landauer, M. R., Clarke, T. K., Mog, S. R., and Davis, T. A. (2006). Radiation protection by subcutaneous administration of genistein: enhancement of hematopoietic recovery and survival in lethally irradiated mice. *Chem.-Biol. Interact.* **161**, 212.
91. Shi, J., Wang, J., Zheng, H., Ling, W., Joseph, J., Li, D., Mehta, J. L., Ponnappan, U., Lin, P., Fink, L. M., and Hauer-Jensen, M. (2003). Statins increase thrombomodulin expression and function in human endothelial cells by a nitric oxide-dependent mechanism and counteract tumor necrosis factor alpha-induced thrombomodulin downregulation. *Blood Coagul. Fibrinolysis* **14**(6), 575–585.
92. Richter, K. K., Fink, L. M., Hughes, B. M., Sung, C.-C., and Hauer-Jensen, M. (1997). Is the loss of endothelial thrombomodulin involved in the mechanism of chronicity in late radiation enteropathy? *Radiother. Oncol.* **44**(1), 65–71.
93. Wang, J., Zheng, H., Ou, X., Fink, L. M., and Hauer-Jensen, M. (2002). Deficiency of microvascular thrombomodulin and upregulation of protease-activated receptor 1 in irradiated rat intestine: possible link between endothelial dysfunction and chronic radiation fibrosis. *Am. J. Pathol.* **160**, 2063–2072.
94. Wang, J., Zheng, H., Ou, X., Albertson, C. M., Fink, L. M., Herbert, J.-M., and Hauer-Jensen, M. (2004). Hirudin ameliorates intestinal radiation toxicity in the rat: support for thrombin

inhibition as strategy to minimize side effects after radiation therapy and as countermeasure against radiation exposure. *J. Thromb. Haemost.* **2**(11), 2027–2035.

95. Masamura, K., Oida, K., Kanehara, H., Suzuki, J., Horie, S., Ishii, H., and Miyamori, I. (2003). Pitavastatin-induced thrombomodulin expression by endothelial cells acts via inhibition of small G proteins of the rho family. *Arterioscler. Thromb. Vasc. Biol.* **23**, 512–513.
96. Nubel, T., Damrot, J., Roos, W. P., Kaina, B., and Fritz, G. (2006). Lovastatin protects human endothelial cells from killing by ionizing radiation without impairing induction and repair of DNA double-strand breaks. *Clin. Cancer Res.* **12**(3 Pt 1), 933–939.
97. Gaugler, M. H., Vereycken-Holler, V., Squiban, C., Vandamme, M., Vozenin-Brotons, M. C., and Benderitter, M. (2005). Pravastatin limits endothelial activation after irradiation and decreases the resulting inflammatory and thrombotic responses. *Radiat. Res.* **163**(5), 479–487.
98. Wang, J., Qiu, X., Zheng, H., Joseph, J., Ponnappan, U., Mehta, J. L., Fink, L. M., and Hauer-Jensen, M. (2004). Effect of statins on endothelial thrombomodulin in vitro and the intestinal radiation response in vivo (Abstracts). *Radiat. Res. Soc.* **51**, 37.
99. Williams, J. P., Hernady, E., Johnston, C. J., Reed, C. M., Fenton, B., Okunieff, P., and Finkelstein, J. N. (2004). Effect of administration of lovastatin on the development of late pulmonary effects after whole-lung irradiation in a murine model. *Radiat. Res.* **161**(5), 560–567.
100. Berk, L. B., Patrene, K. D., and Boggs, S. S. (1990). 16,16-Dimethyl prostaglandin E2 and/or syngeneic bone marrow transplantation increase mouse survival after supra-lethal total body irradiation. *Int. J. Radiat. Oncol. Biol. Phys.* **18**(6), 1387–1392.
101. Hanson, W. R. (1987). Radiation protection of murine intestine by WR-2721, 16,16-dimethyl prostaglandin E2, and the combination of both agents. *Radiat. Res.* **111**(2), 361–373.
102. Walden, T. L., Patchen, M., and Snyder, S. L. (1987). Jr 16,16-Dimethyl prostaglandin E2 increases survival in mice following irradiation. *Radiat. Res.* **109**(3), 440–448.
103. Walden, T. L. Jr, and Farzaneh, N. K. (1995). Radioprotection by 16,16 dimethyl prostaglandin E2 is equally effective in male and female mice. *J. Radiat. Res. (Tokyo)* **36**(1), 1–7.
104. Landauer, M. R., Davis, H. D., Kumar, K. S., and Weiss, J. F. (1992). Behavioral toxicity of selected radioprotectors. *Adv. Space Res.* **12**(2-3), 273–283.
105. Neta, R. (1998). Modulation of the radiation response by cytokines. In E. A., Bump, and K., Malaker, Eds. *Radioprotectors Chemical, Biological and Clinical Perspectives*, CRC Press, Boca Raton, pp. 237–252.
106. Waddick, K. G., Song, C. W., Souza, L., and Uckun, F. M. (1991). Comparative analysis of the in vivo radioprotective effects of recombinant granulocyte colony-stimulating factor (G-CSF), recombinant granulocyte-macrophage CSF, and their combination. *Blood* **77**(11), 2364–2371.
107. Patchen, M. L., MacVittie, T. J., Solberg, B. D., and Souza, L. M. (1990). Therapeutic administration of recombinant human granulocyte colony-stimulating factor accelerates hemopoietic regeneration and enhances survival in a murine model of radiation-induced myelosuppression. *Int. J. Cell Cloning* **8**(2), 107–122.
108. MacVittie, T. J., Monroy, R. L., Patchen, M. L., and Souza, L. M. (1990). Therapeutic use of recombinant human G-CSF (rhG-CSF) in a canine model of sublethal and lethal whole-body irradiation. *Int. J. Radiat. Biol.* **57**(4), 723–736.
109. Schuening, F. G., Storb, R., Goehle, S., Graham, T. C., Appelbaum, F. R., Hackman, R., and Souza, L. M. (1989). Effect of recombinant human granulocyte colony-stimulating factor on hematopoiesis of normal dogs and on hematopoietic recovery after otherwise lethal total body irradiation. *Blood* **74**(4), 1308–1313.
110. Schuening, F. G., Appelbaum, F. R., Deeg, H. J., Sullivan-Pepe, M., Graham, T. C., Hackman, R., Zsebo, K. M., and Storb, R. (1993). Effects of recombinant canine stem cell factor, a c-kit

ligand, and recombinant granulocyte colony-stimulating factor on hematopoietic recovery after otherwise lethal total body irradiation. *Blood* **81**(1), 20–26.

111. Nash, R. A., Schuening, F. G., Seidel, K., Appelbaum, F. R., Boone, T., Deeg, H. J., Graham, T. C., Hackman, R., Sullivan-Pepe, M., and Storb, R. (1994). Effect of recombinant canine granulocyte-macrophage colony-stimulating factor on hematopoietic recovery after otherwise lethal total body irradiation. *Blood* **83**(7), 1963–1970.
112. MacVittie, T. J., Farese, A. M., Herodin, F., Grab, L. B., Baum, C. M., and McKearn, J. P. (1996). Combination therapy for radiation-induced bone marrow aplasia in nonhuman primates using synthokine SC-55494 and recombinant human granulocyte colony-stimulating factor. *Blood* **87**(10), 4129–4135.
113. Neelis, K. J., Dubbelman, Y. D., Qingliang, L., Thomas, G. R., Eaton, D. L., and Wagemaker, G. (1997). Simultaneous administration of TPO and G-CSF after cytoreductive treatment of rhesus monkeys prevents thrombocytopenia, accelerates platelet and red cell reconstitution, alleviates neutropenia, and promotes the recovery of immature bone marrow cells. *Exp. Hematol.* **25**(10), 1084–1093.
114. Neelis, K. J., Hartong, S. C., Egeland, T., Thomas, G. R., Eaton, D. L., and Wagemaker, G. (1997). The efficacy of single-dose administration of thrombopoietin with coadministration of either granulocyte/macrophage or granulocyte colony-stimulating factor in myelosuppressed rhesus monkeys. *Blood* **90**(7), 2565–2573.
115. Farese, A. M., Williams, D. E., Seiler, F. R., and MacVittie, T. J. (1993). Combination protocols of cytokine therapy with interleukin-3 and granulocyte-macrophage colony-stimulating factor in a primate model of radiation-induced marrow aplasia. *Blood* **82**(10), 3012–3018.
116. Vial, T., and Descotes, J. (1995). Clinical toxicity of cytokines used as haemopoietic growth factors. *Drug Saf.* **13**(6), 371–406.
117. Herodin, F., and Drouet, M. (2005). Cytokine-based treatment of accidentally irradiated victims and new approaches. *Exp. Hematol.* **33**(10), 1071–1080.
118. Dinarello, C. A., and Neta, R. (1989). An overview on interleukin-1 as a therapeutic agent. *Biotherapy* **1**(4), 245–254.
119. Manori, I., Kushilevsky, A., and Weinstein, Y. (1986). Analysis of interleukin-1 mediated radioprotection. *Clin. Exp. Immunol.* **63**(3), 526–532.
120. Neta, R. (1988). Cytokines in radioprotection and therapy of radiation injury. *Biotherapy* **1**(1), 41–45.
121. Neta, R. (1988). Role of cytokines in radioprotection. *Pharmacol. Ther.* **39**(1-3), 261–266.
122. Neta, R., and Oppenheim, J. J. (1988). Cytokines in therapy of radiation injury. *Blood* **72**(3), 1093–1095.
123. Neta, R., Douches, S., and Oppenheim, J. J. (1986). Interleukin-1 is a radioprotector. *J. Immunol.* **136**(7), 2483–2485.
124. Neta, R., Sztein, M. B., Oppenheim, J. J., Gillis, S., and Douches, S. D. (1987). The in vivo effects of interleukin-1. I. Bone marrow cells are induced to cycle after administration of interleukin-1. *J. Immunol.* **139**(6), 1861–1866.
125. Neta, R., Vogel, S. N., Sipe, J. D., Wong, G. G., and Nordan, R. P. (1988). Comparison of in vivo effects of human recombinant IL-1 and human recombinant IL-6 in mice. *Lymphokine Res.* **7**(4), 403–412.
126. Neta, R., Monroy, R., and MacVittie, T. J. (1989). Utility of interleukin-1 in therapy of radiation injury as studied in small and large animal models. *Biotherapy* **1**(4), 301–311.
127. Wu, S. G., Tuboi, A., and Miyamoto, T. (1989). Radioprotection of C3H mice by recombinant human interleukin-1a. *Int. J. Radiat. Biol.* **56**(4), 485–492.
128. Boraschi, D., Nencioni, L., Villa, L., Censini, S., Bossu, P., Ghiara, P., Presentini, R., Perin, F., Frasca, D., Doria, G., Forni, G., Musso, T., Giovarelli, M., Ghezzi, P., Bertini, R.,

Besedovsky, H. O., Rey, A. D., Sipe, J. D., Antoni, G., Silvestri, S., and Tagliabue, A. (1988). In vivo stimulation and restoration of the immune response by the noninflammatory fragment 163–171 of human interleukin 1h. *J. Exp. Med.* **168**(2), 675–686.

129. Bajpai, K., Singh, V. K., Sharan, R., Yadav, V. S., Haq, W., Mathur, K. B., and Agarwal, S. S. (1998). Immunomodulating activity of analogs of noninflammatory fragment 163–171 of human interleukin-1h. *Immunopharmacology* **38**(3), 237–245.
130. Potten, C. S., O'Shea, J. A., Farrell, C. L., Rex, K., and Booth, C. (2001). The effects of repeated doses of keratinocyte growth factor on cell proliferation in the cellular hierarchy of the crypts of the murine small intestine. *Cell Growth Differ.* **12**(5), 265–275.
131. Farrell, C. L., Bready, J. V., Rex, K. L., Chen, J. N., DiPalma, C. R., Whitcomb, K. L., Yin, S., Hill, D. C., Wiemann, B., Starnes, C. O., Havill, A. M., Lu, Z. N., Aukerman, S. L., Pierce, G. F., Thomason, A., Potten, C. S., Ulich, T. R., and Lacey, D. L. (1998). Keratinocyte growth factor protects mice from chemotherapy and radiation-induced gastrointestinal injury and mortality. *Cancer Res.* **58**(5), 933–939.
132. Khan, W. B., Shui, C., Ning, S., and Knox, S. J. (1997). Enhancement of murine intestinal stem cell survival after irradiation by keratinocyte growth factor. *Radiat. Res.* **148**(3), 248–253.
133. Whitnall, M. H., Elliott, T. B., Harding, R. A., Inal, C. E., Landauer, M. R., Wilhelmsen, C. L., McKinney, L., Miner, V. L., Jackson, W. E. III, Loria, R. M., Ledney, G. D., and Seed, T. M. (2000). Androstenediol stimulates myelopoiesis and enhances resistance to infection in gamma-irradiated mice. *Int. J. Immunopharmacol.* **22**(1), 1–14.
134. Whitnall, M. H., Wilhelmsen, C. L., McKinney, L., Miner, V., Seed, T. M., and Jackson, W. E. III. (2002). Radioprotective efficacy and acute toxicity of 5-androstenediol after subcutaneous or oral administration in mice. *Immunopharmacol. Immunotoxicol.* **24**(4), 595–626.
135. Whitnall, M. H., Villa, V., Seed, T. M., Benjack, J., Miner, V., Lewbart, M. L., Dowding, C. A., and Jackson, W. E. III. (2005). Molecular specificity of 5-androstenediol as a systemic radioprotectant in mice. *Immunopharmacol. Immunotoxicol.* **27**(1), 15–32.
136. Loria, R. M., Conrad, D. H., Huff, T., Carter, H., and Ben-Nathan, D. (2000). Androstenetriol and androstenediol protection against lethal radiation and restoration of immunity after radiation injury. *Ann. N. Y. Acad. Sci.* **917**, 860–867.
137. Stickney, D. R., Dowding, C., Garsd, A., Ahlem, C., Whitnall, M., McKeon, M., Reading, C., and Frincke, J. M. (2006). 5-Androstenediol stimulates multilineage hematopoiesis in rhesus monkeys with radiation-induced myelosuppression. *Int. Immunopharmacol.* **6**(11), 1706–1713.
138. Whitnall, M. H., Inal, C. E., Jackson, W. E., Miner, V. L., Villa, V., and Seed, T. M. (2001). III In vivo radioprotection by 5-androstenediol: Stimulation of the innate immune system. *Radiat. Res.* **156**(3), 283–293.
139. Xiao, M., Inal, C. E., Parekh, V. I., Siddiqi, W. S., Whitnall, M. H. (2006). 5-Androstenediol Promotes Survival of Irradiated Human Hematopoietic Progenitors: Role of Nuclear Factor kappa B (NFkB) in CD34+ cells (Abstracts). *Annual Meeting of the Radiation Research Society* Philadelphia, PA, Nov 5–8, 2006.
140. Patchen, M. L., MacVittie, T. J., and Brook, I. (1986). Glucan-induced hemopoietic and immune stimulation: therapeutic effects in sublethally and lethally irradiated mice. *Methods Find. Exp. Clin. Pharmacol.* **8**(3), 151–155.
141. Patchen, M. L., and MacVittie, T. J. (1982). Use of glucan to enhance hemopoietic recovery after exposure to cobalt-60 irradiation. *Adv. Exp. Med. Biol.* **155**, 267–272.
142. Patchen, M. L., and MacVittie, T. J. (1986). Comparative effects of soluble and particulate glucans on survival in irradiated mice. *J. Biol. Response Mod.* **5**(1), 45–60.
143. Patchen, M. L., Vaudrain, T., Correira, H., Martin, T., and Reese, D. (1998). In vitro and in vivo hematopoietic activities of Betafectin PGG-glucan. *Exp. Hematol.* **26**(13), 1247–1254.

144. Patchen, M. L., Liang, J., Vaudrain, T., Martin, T., Melican, D., Zhong, S., Stewart, M., and Quesenberry, P. J. (1998). Mobilization of peripheral blood progenitor cells by Betafectin PGG-Glucan alone and in combination with granulocyte colony-stimulating factor. *Stem Cells.* **16**(3), 208–217.

145. Katano, M., and Morisaki, T. (1998). The past, the present and future of the OK-432 therapy for patients with malignant effusions. *Anticancer Res.* **18**(5D), 3917–3925.

146. Joshima, H., Ohara, H., and Aoki, Y. (1992). The effect of OK-432 upon erythropoietic recovery in sub-lethally irradiated mice: a preliminary report. *J. Radiat. Res. (Tokyo)* **33**(4), 290–300.

147. Kimura, H., Ikebuchi, M., Nyaruba, M. M., Sugamoto, K., Aoyama, T., and Sugahara, T. (1994). Effects of combination of immunomodulators and an adrenochrome derivative on survival of irradiated mice. *Int. J. Radiat. Oncol. Biol. Phys.* **29**(3), 627–630.

148. Nose, M., Aoki, Y., Kawase, Y., Suzuki, G., Akashi, M., and Akanuma, A. (1994). In vitro effects of OK-432 on irradiated mouse bone marrow cells. *Int. J. Radiat. Oncol. Biol. Phys.* **29**(3), 631–634.

149. Nose, M., Uzawa, A., Ogyu, T., and Suzuki, G. (2001). OK-432 reduces mortality and bacterial translocation in irradiated and granulocyte-colony stimulating factor (G-CSF)-treated mice. *J. Radiat. Res. (Tokyo)* **42**(2), 191–200.

150. Kurishita, A., Katoh, H., Uehara, Y., Uchida, A., Mizutani, Y., Ono, T., Hirose, S., and Okada, S. (1991). Post-irradiation treatment with OK432 can prevent radiation-induced bone marrow death. *Int. J. Radiat. Biol.* **59**(3), 711–716.

151. Kurishita, A., Ono, T., and Uchida, A. (1993). Prevention of radiation-induced bacteraemia by post-treatment with OK-432 and aztreonam. *Int. J. Radiat. Biol.* **63**(3), 413–417.

152. MacVittie, T. J., Monroy, R., Vigneulle, R. M., Zeman, G. H., and Jackson, W. E. (1991). The relative biological effectiveness of mixed fission-neutron-gamma radiation on the hematopoietic syndrome in the canine: effect of therapy on survival. *Radiat. Res.* **128**(1 Suppl), S29–S36.

153. Farese, A. M., Hunt, P., Grab, L. B., and MacVittie, T. J. (1996). Combined administration of recombinant human megakaryocyte growth and development factor and granulocyte colony-stimulating factor enhances multilineage hematopoietic reconstitution in nonhuman primates after radiation-induced marrow aplasia. *J. Clin. Invest.* **97**(9), 2145–2151.

154. Farese, A. M., Casey, D. B., Smith, W. G., Vigneulle, R. M., McKearn, J. P., and MacVittie, T. J. (2001). Leridistim, a chimeric dual G-CSF and IL-3 receptor agonist, enhances multilineage hematopoietic recovery in a nonhuman primate model of radiation-induced myelosuppression: effect of schedule, dose, and route of administration. *Stem Cells.* **19**(6), 522–533.

155. Schlumberger, H. G., and Vasquez, J. J. (1954). Pathology of total body irradiation in the monkey. *Am. J. Pathol.* **30**, 1013–1047.

156. Broerse, J. J., van Bekkum, D. W., Hollander, C. F., and Davids, J. A. (1978). Mortality of monkeys after exposure to fission neutrons and the effect of autologous bone marrow transplantation. *Int. J. Radiat. Biol. Relat. Stud. Phys. Chem. Med.* **34**(3), 253–264.

157. Perman, V., Cronkite, E. P., Bond, V. P., and Sorensen, D. K. (1962). The regenerative ability of hemopoietic tissue following lethal x-irradiation in dogs. *Blood* **19**, 724–737.

158. Brook, I., Elliott, T. B., Ledney, G. D., and Knudson, G. B. (2002). Management of postirradiation sepsis. *Mil. Med.* **167**(2 Suppl), 105–106.

159. Brook, I., and Ledney, G. D. (1994). Effect of antimicrobial therapy on the gastrointestinal bacterial flora, infection, and mortality in mice exposed to different doses of irradiation. *J. Antimicrob. Chemother.* **33**(1), 63–72.

160. Brook, I., and Ledney, G. D. (1994). Quinolone therapy in the prevention of endogenous and exogenous infection after irradiation. *J. Antimicrob. Chemother.* **33**(4), 777–784.

161. Georges, G. E., and Storb, R. F. (2002). Experimental and clinical experience with hematopoietic stem cell transplants. In *The Medical Basis for Radiation-Accident Preparedness: The Clinical Care of Victims*, R. C., Ricks, M. E., Berger, and F. M., O'Hara Jr, Eds. Parthenon Publishing, Boca Raton, pp. 73–93.

162. Herodin, F., Mayol, J. F., Mourcin, F., and Drouet, M. (2005). Which place for stem cell therapy in the treatment of acute radiation syndrome? Folia Histochem. *Cytobiologie* **43**(4), 223–227.

163. Resnick, I. B., and Slavin, S. (2005). Lessons from bone marrow transplantation for a victim of a radiological accident with acute radiation syndrome. *BJR Suppl.* **27**, 21–25.

164. Uozaki, H., Fukayama, M., Nakagawa, K., Ishikawa, T., Misawa, S., Doi, M., and Maekawa, K. (2005). The pathology of multi-organ involvement: two autopsy cases from the Tokai-mura criticality accident. *BJR Suppl.* **27**, 13–16.

165. Changlin, Y., and Genyao, Y. (2005). Multi-organ failure in a radiation accident: the Chinese experience of 1990. *BJR Suppl.* **27**, 47–54.

166. Densow, D., Kindler, H., Baranov, A. E., Tibken, B., Hofer, E. P., and Fliedner, T. M. (1997). Criteria for the selection of radiation accident victims for stem cell transplantation. In *Radiation Injury and the Chernobyl Catastrophe*, N., Dainiak, W. J., Schull, L., Karkanitsa, and O. A., Aleinikova, Eds. Alpha Med Press, Miamisburg, OH.

167. Baranov, A., Gale, R. P., Guskova, A., Piatkin, E., Selidovkin, G., and Muravyova, L. (1989). Bone marrow transplantation after the Chernobyl nuclear accident. *N. Engl. J. Med.* **321**(4), 205–212.

168. Steel, L. K., Walden, T. L. J., Hughes, H. N., and Jackson, W. E. III. (1988). Protection of mice against mixed fission neutron gamma (n: gamma = 1:1) irradiation by WR-2721, 16,16-dimethyl PGE2, and the combination of both agents. *Radiat. Res.* **115**(3), 605–608.

169. Ledney, G. D., Elliott, T. B., Landauer, M. R., Vigneulle, R. M., Henderson, P. L., Harding, R. A., and Tom, S. P. Jr. (1994). Survival of irradiated mice treated with WR-151327, synthetic trehalose dicorynomycolate, or ofloxacin. *Adv. Space Res.* **14**(10), 583–586.

170. Balcer-Kubiczek, E. K., Harrison, G. H., Hill, C. K., and Blakely, W. F. (1993). Effects of WR-1065 and WR-151326 on survival and neoplastic transformation in C3H/10T1/2 cells exposed to TRIGA or JANUS fission neutrons. *Int. J. Radiat. Biol.* **63**(1), 37–46.

171. McChesney, D. G., Ledney, G. D., and Madonna, G. S. (1990). Trehalose dimycolate enhances survival of fission neutron-irradiated mice and Klebsiella pneumoniae-challenged irradiated mice. *Radiat. Res.* **121**(1), 71–75.

172. Madonna, G. S., Ledney, G. D., Moore, M. M., Elliott, T. B., and Brook, I. (1991). Treatment of mice with sepsis following irradiation and trauma with antibiotics and synthetic trehalose dicorynomycolate (S-TDCM). *J. Trauma.* **31**(3), 316–325.

173. Brook, I., Ledney, G. D., Madonna, G. S., DeBell, R. M., and Walker, R. I. (1992). Therapies for radiation injuries: research perspectives. *Mil. Med.* **157**(3), 130–136.

174. Brook, I., Tom, S. P., and Ledney, G. D. (1993). Quinolone and glycopeptide therapy for infection in mouse following exposure to mixed-field neutron-gamma-photon radiation. *Int. J. Radiat. Biol.* **64**(6), 771–777.

175. Hanson, W. R., and Grdina, D. J. (1991). Misoprostol, a PGE1 analog, protects mice from fission-neutron injury. *Radiat. Res.* **128**(1 Suppl), S12–S17.

176. Farese, A. M., Myers, L. A., and MacVittie, T. J. (1994). Therapeutic efficacy of recombinant human leukemia inhibitory factor in a primate model of radiation-induced marrow aplasia. *Blood* **84**(11), 3675–3678.

177. Herodin, F., Mestries, J. C., Janodet, D., Martin, S., Mathieu, J., Gascon, M. P., Pernin, M. O., and Ythier, A. (1992). Recombinant glycosylated human interleukin-6 accelerates peripheral blood platelet count recovery in radiation-induced bone marrow depression in baboons. *Blood* **80**(3), 688–695.

178. Casarett, A. P. (1968). *Radiation Biology*, Prentice Hall Inc., Englewood Cliffs.

179. Seed, T. M., Fritz, T. E., Tolle, D. V., and Jackson, W. E. III. (2002). Hematopoietic responses under protracted exposures to low daily dose gamma irradiation. *Adv. Space Res.* **30**(4), 945–955.

180. Baltschukat, K., Fliedner, T. M., and Nothdurft, W. (1989). Hematological effects in dogs after irradiation of the lower part of the body with a single myeloablative dose. *Radiother. Oncol.* **14**(3), 239–246.

181. Fliedner, T. M., Graessle, D., Paulsen, C., and Reimers, K. (2002). Structure and function of bone marrow hemopoiesis: mechanisms of response to ionizing radiation exposure. *Cancer Biother. Radiopharm.* **17**(4), 405–426.

182. Nothdurft, W., and Kreja, L. (1998). Hemopoietic progenitor cells in the blood as indicators of the functional status of the bone marrow after total-body and partial-body irradiation: experiences from studies in dogs. *Stem Cells* **16**(Suppl 1), 97–111.

183. Nothdurft, W., Calvo, W., Klinnert, V., Steinbach, K. H., Werner, C., and Fliedner, T. M. (1986). Acute and long-term alterations in the granulocyte/macrophage progenitor cell (GM-CFC) compartment of dogs after partial-body irradiation: irradiation of the upper body with a single myeloablative dose. *Int. J. Radiat. Oncol. Biol. Phys.* **12**(6), 949–957.

184. Nothdurft, W., Baltschukat, K., and Fliedner, T. M. (1989). Hematological effects in dogs after sequential irradiation of the upper and lower part of the body with single myeloablative doses. *Radiother. Oncol.* **14**(3), 247–259.

185. Grande, T., and Bueren, J. A. (2006). The mobilization of hematopoietic progenitors to peripheral blood is predictive of the hematopoietic syndrome after total or partial body irradiation of mice. *Int. J. Radiat. Oncol. Biol. Phys.* **64**(2), 612–618.

186. Alpen, E. L., and Sheline, G. E. (1954). The combined effects of thermal burns and whole-body X irradiation on survival time and mortality. *Ann. Surg.* **140**(1), 113–118.

187. Brooks, J. W., Evans, E. I., Ham, W. T., and Reid, J. D. (1952). The influence of external body radiation on mortality from thermal burns. *Ann. Surg.* **136**(3), 533–545.

188. Pellmar, T. C., Ledney, G. L.. (2005). Combined injury: radiation in combination with trauma, infectious disease, or chemical exposures. *Published in the Proceedings of the NATO Human Factors and Medicine (HFM) Panel Research Task Group (RTG) 099 Meeting, "Radiation Bioeffects and Countermeasures"*, Bethesda, June 21–23, 2005.

189. Mishima, S., Yukioka, T., Matsuda, H., and Shimazaki, S. (1997). Mild hypotension and body burns synergistically increase bacterial translocation in rats consistent with a "two-hit phenomenon". *J. Burn Care Rehabil.* **18**(1 Pt 1), 22–26.

190. Yan, Y., Ran, X., and Wei, S. (1995). Changes of immune functions after radiation, burns and combined radiation-burn injury in rats. *Chin. Med. Sci. J.* **10**(2), 85–89.

191. Ran, X., Cheng, T., Shi, C., Xu, H., Qu, J., Yan, G., Su, Y., Wang, W., and Xu, R. (2004). The effects of total-body irradiation on the survival and skin wound healing of rats with combined radiation-wound injury. *J. Trauma* **57**(5), 1087–1093.

192. Cervany, T. J., MacVittie, T. J., and Young, R. W. (1989). Acute Radiation Syndrome in Humans. In *Textbook of Military Medicine: Medical Consequences of Nuclear Warfare*, R. I., Walker, and T. J., Cervany, Eds. TMM Publications, Office of the Surgeon General Falls Church, Virginia, pp. 15–36.

193. Hirsch, E. F., Vezina, R., Corbett, S., LaMorte, W., and Feldman, M. (1990). Combined ionizing radiation and thermal injury in the rat. Evaluation of early excision and closure of the burn wound. *J. Burn Care Rehabil.* **11**(1), 42–45.

194. Messerschmidt, O. (1966). Untersuchungen uber Kombinationsschaden. Uber die Lebenserwartung von Mausen, die mit Ganzkorperbestrahlungen in Kombination mit offenen oder geschlossenen Hautverletzungen, Bauchoperationen oder Kompressionsschaden delastet wurden. *Strahlentherapie* **131**(2), 298–311.

195. Dons, R. E., and Cervany, T. J. (1989). Triage and treatment of radiation-injured mass casualties. In R. I., Walker, and T. J., Cervany, Eds. *Textbook of Military Medicine: Medical Consequences of Nuclear Warfare*, TMM Publications, Office of the Surgeon General Falls Church, Virginia, pp. 37–54.

196. Engelhardt, M., Kaffenberger, W., Abend, M., Gerngross, H., and Willy, C. (2001). Radiation and burn trauma (combined injury). Considerations in surgical treatment. *Unfallchirurgie* **104**(4), 333–342.

197. Ledney, G. D., Elliott, T. B., Harding, R. A., Jackson, W. E. III, Inal, C. E., and Landauer, M. R. (2000). WR-151327 increases resistance to Klebsiella pneumoniae infection in mixed-field- and gamma-photon-irradiated mice. *Int. J. Radiat. Biol.* **76**(2), 261–271.

198. Landauer, M. R., Elliott, T. B., King, G. L., Bouhaouala, S. S., Wilhelmsen, C. L., Farrell, J. L., Wang, P. S., Chap, A. D., and Knudson, G. B. (2001). Performance decrement after combined exposure to ionizing radiation and Shigella sonnei. *Mil. Med.* **166**(12 Suppl), 71–73.

199. Kelly, D. J., and Rees, J. C. (1986). Effect of sublethal gamma radiation on host defenses in experimental scrub typhus. *Infect. Immun.* **52**(3), 718–724.

200. Shoemaker, M. O., Tammariello, R., Cris, Ewarning. B., Bouhaouala, S. S., Knudson, G. B., Jackson, W. E., Ludwig, G. V., and Smith, J. F. (2001). Combined effects of Venezuelan equine encephalitis IIIa virus and gamma irradiation in mice. *Mil. Med.* **166**(12 Suppl), 88–89.

# CHALLENGES TO MEDICAL COUNTERMEASURES AGAINST CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) AGENTS

ANDREA MEYERHOFF

*GexGroup Inc, Washington, D.C., and Division of Clinical Pharmacology, Johns Hopkins University School of Medicine, Baltimore, Maryland*

## 1 BACKGROUND

The public health threat of biological and chemical agents has persisted for centuries; that of radiation-emitting and nuclear agents for more than a half-century. But it is only in the past decade that the pace of efforts to address these threats has accelerated to the point where we might now take a step back and evaluate what has been accomplished and, based on what we have learned, how we might proceed. This article first recognizes the unique challenges presented by the need for medical countermeasures against chemical,

biological, radiological, and nuclear (CBRN) agents and then examines early twenty-first century efforts to develop them. Because of both the 2001 occurrence of an anthrax release in the United States and the subsequent robust investment in medical countermeasures for this and other biothreat agents, a focus on biodefense will provide useful examples. Nonetheless the issues raised, with necessary modifications, pertain equally to other threat agents as well. The subsequent discussion of future directions for CBRN drugs and vaccine research is based on unanswered questions regarding countermeasure safety and efficacy.

## 2 THREATS, CHALLENGES, SOLUTIONS

In 1998, the US Centers for Disease Control (CDC), an agency of the Department of Health and Human Services (HHS) was charged by Congress to build the National Pharmaceutical Stockpile (NPS). Its purpose was to provide emergency medical supplies in the event of a terrorist attack or naturally-occurring epidemic. A wide range of medical material made up the NPS, including antibiotics, antitoxins, and chemical antidotes to be shipped to state and local authorities within 12 hours of the declaration of an emergency. Subsequently the name NPS was changed to the Strategic National Stockpile (SNS) [1, 2].

In 1999, the CDC, in concert with the intelligence community, identified the biological agents considered to be of greatest potential concern [3]. The resultant list was divided into three categories. The pathogens in Category A were thought to represent the highest risk, warranting surveillance and the availability of therapy or prophylaxis for diseases caused by them. The threats represented by Category A pathogens guided early efforts to build the NPS and later the SNS. They are presented in Table 1.

The evaluation of medical countermeasures against Category A pathogens presents unique challenges. The diseases they cause are rare or are known to contemporary physicians and public health officials only by historical reputation. Other diseases, while continued public health problems, occur in remote areas of the world where the collection of data and conduct of clinical trials are difficult. Further, it is unethical to introduce any of the agents into a human population for any purpose, including the evaluation of drugs or vaccines.

Until 2001, there had been 18 cases of naturally occurring inhalational anthrax reported in the United States. The events of 2001 resulted in an additional 11 cases [4]. Inhalational anthrax differs from many other diseases that result from exposure to Category A biothreat agents in that there was a large outbreak of human disease in 1979 in Sverdlovsk in the

**TABLE 1 Category A Biological Agents (US CDC, June 1999)**

| Organism | Disease |
|---|---|
| *Variola major* | Smallpox |
| *Bacillus anthracis* | Anthrax |
| *Yersinia pestis* | Plague |
| *Clostridium botulinum toxin* | Botulism |
| *Francisella tularensis* | Tularemia |
| Filoviruses/Arenaviruses | Hemorrhagic fever |

former Soviet Union. This is thought to have resulted from a leak at a military research facility and resulted in at least 66 deaths. After several years an international team of pathologists published their postmortem findings on these patients, thus expanding the knowledge on the course of the infection in humans [5]. A paucity of available information on treatments used meant that systematic study of any drugs given to these anthrax patients was not possible.

This rather sparse database on inhalational anthrax is one of the more robust ones for diseases caused by Category A pathogens. Naturally occurring smallpox was declared eradicated from the world in 1980 and last seen in the United States in 1947 [6]. Few physicians practicing today have seen a case. Pneumonic plague occurs naturally, but small foci of disease have been found in remote locations that make systematic study difficult.

Intentionally caused disease by a state actor or terrorist that deploys a biological weapon may differ from what occurs naturally by a number of variables including inoculum size, route of exposure, number of individuals exposed, and rate at which an infection progresses through a population.

Thus there is little precedent of the study of such rare diseases, and little regulatory precedent that sets safety and efficacy standards for the drugs and vaccines needed to treat or protect against these diseases. Even for inhalational anthrax, noted above to be the subject of some body of data on human disease, the size of the database is scant when compared with the thousands of patients usually enrolled in Phase III clinical trials to study drugs and vaccines for more common indications.

In 2000, the Food and Drug Administration (FDA), another HHS agency, approved the first antibiotic for use in an intentional biological release when it determined that ciprofloxacin (Cipro®) was safe and effective for the postexposure prophylaxis of inhalational anthrax. The approval was based on a surrogate human marker of efficacy (Accelerated Approval Regulations) and made extensive use of data from an animal model of disease [7]. At the time, also approved for anthrax were antibiotics in both the penicillin and tetracycline classes. The data for these two classes of drugs were developed in patients with naturally-occurring disease. The stockpiling of any drugs by the US government with the plan to deploy them in the event of an emergency necessitates regulatory oversight by the FDA. Thus any drug or vaccine deployed from the SNS must meet FDA standards of safety, efficacy, and manufacturing.

The 2001 terrorist attacks of September 11, and the release of anthrax through the US Postal Service soon afterward, resulted in a concerted effort to speed the development of the required CBRN countermeasures by the US Government. The Bioterrorism Act of 2002 created a new office within HHS, the Assistant Secretary of Public Health Emergency Preparedness (ASPHEP) which was charged with overseeing this effort. Post 9/11, the National Institutes of Health (NIH) budget for basic research for drugs and vaccines for bioterrorism and other CBRN threats experience rose five-fold to $1–2 billion per year [8]. In 2004, the passage of the Project BioShield Act gave to HHS new authorities and a special reserve fund of an additional $5.6 billion for advanced product development and procurement [9].

Among the new authorities accorded to HHS by the 2004 BioShield Act was the mechanism of Emergency Use Authorization (EUA) by the FDA. With the goal of streamlining the availability of needed medical countermeasures in an emergency, the EUA permitted for the first time, the use of a drug or vaccine prior to FDA approval, that is, the use of

an investigational agent outside of the Investigational New Drug (IND) regulations and without the requirement of obtaining prior, written, informed consent [10].

Another new regulatory mechanism introduced during this period was the 2002 finalization of the Animal Efficacy Rule by the FDA, which recognized the use of animal models to demonstrate efficacy of drugs and vaccines used for CBRN countermeasures [11]. While the animal model must be found by the FDA to meet certain scientific requirements of predictability in humans, by definition each model presents gaps in disease pathology and host response between animals and humans. Any use of such countermeasures in an attack on a human population must recognize these attendant gaps and the risk they present. The use of animal models to establish efficacy and support regulatory approval creates a need, arguably an imperative, to add to such knowledge with the study of the efficacy of any such medical countermeasure if it is used in a human population.

An older regulatory mechanism that became pertinent to CBRN countermeasures was the 1997 Accelerated Approval Regulations (also known as Subpart H) that permitted the use of surrogate endpoints, and therefore smaller studies, for the evaluation of needed drugs and vaccines. As noted above, it was this mechanism that was invoked in the 2000 approval of Cipro® for post-exposure inhalational anthrax.

All three of the regulatory mechanisms described above—EUA, Animal Efficacy Rule, and Accelerated Approval Regulations—require the collection of safety data -adverse events following the emergency use of the medical countermeasure [11].

Thus by 2004, with the passage of BioShield legislation, a unique development model had evolved for medical countermeasures for CBRN defense. Rather than the traditional market forces that drive most drug and vaccine development, federal policy and funding became the driver of CBRN medical countermeasure development. The federal government had become the developer, the procurer, and the regulator of these products.

In December 2006, the Pandemic and All-Hazard Preparedness Act was passed. This bill created the Biomedical Advanced Research and Development Authority (BARDA, also known as BioShield II). It also resulted in an additional $1.07 billion for medical countermeasure development for CBRN threats and influenza for fiscal years 2006–08. The legislation established HHS ASPHEP, renamed the HHS Assistant Secretary of Preparedness and Response (ASPR), as the lead authority for policy setting and procurement for CBRN medical countermeasures and made possible "milestone payments" to companies before actual delivery of the countermeasure to the stockpile [12]. While this provision was included as a means to encourage what was only modest industry participation in medical countermeasure development under Project BioShield, it has resulted in a highly unusual situation in drug development. A company may receive federal funds before it delivers the product, indeed before it receives regulatory approval for a product intended for the SNS.

While at the time of writing this HHS/ASPR efforts are understandably focused on what is now pandemic H1N1 influenza, a review of HHS BioShield/BARDA programs since their inception provides summary information on CBRN medical countermeasures funded and stockpiled to date. These are presented in Table 2.

Most recently the Obama administration has proposed a budget to combat pandemic influenza, which uses the remaining $3 billion of the original $5.6 billion of the BioShield special reserve fund [14]. If this plan comes to pass, it is unclear how much more funding HHS will provide to CBRN medical countermeasure advanced development and procurement.

**TABLE 2 HHS Category A Biothreat, Chemical, and Radiation/Nuclear Countermeasures Funded by BioShield/BARDA, 2009 [13]**

| Agent | Vaccines | Drugs | Antitoxins |
|---|---|---|---|
| Anthrax | rPA 'next-generation'<br>1. $887 million contract let 2004; w/d 2006<br>2. New proposals under evaluation<br>AVA licensed 1971<br>1. $123 million for 10 million doses 2005<br>2. $120 million for 10 million doses 2006 | 'Quantities sufficient' for 40 million individuals[a,b†] | Monoclonal Ab<br>$165 million for 20,000 doses 2006 $151 million for 45,000 doses 2009<br>Polyclonal Ab<br>$144M for 10,000 doses 2006 |
| Smallpox | Total- enough for every American[a,c]<br>MVA- $500 million for 20 million doses for those unable to take traditional Vaccine | | |
| Botulism | | | Equine program support $50 million 2004<br>$363 million for 200,000 doses heptavalent equine 2006 |
| Plague | | | |
| Tularemia | | | |
| VHF | | | |
| Chemical agents | | | |
| Radioactive/ Nuclear agents | | KI pediatric 4.3 million bottles<br>DTPA $20 million for ~480,000 doses 2006 | |

rPA, recombinant protective antigen; w/d, withdrawn; AVA,anthrax vaccine adsorbed; Ab, antibody; MVA, modified Vaccinia Ankara, attenuated vaccine for immunosuppressed patients; KI,potassium iodide, protects from development of radiation induced thyroid cancer; Diethylenetriamine pentacetate (DTPA), chelating agent that removes radioactive particles from body; VHF,viral hemorrhagic fevers

[a]BARDA website describes these countermeasures as purchased by HHS for CBRN defense, however, they were not funded by BioShield/BARDA funds.

[b]Funded by CDC-Strategic National Stockpile.

[c]Funded by HHS 2001,$428 million for 155 million doses, non-BioShield/BARDA funds.

Newer regulatory pathways such as the Animal Efficacy Rule and EUA, may result in the use of these countermeasures without the development of data and the use of informed consent that the medical community and the general public have come to expect. Thus with the passage of the 2006 BARDA legislation it is possible for the federal government to purchase and deploy medical countermeasures at a stage far earlier in product development than has been traditionally the case. A new pathway for medical countermeasure development and use is the result and new challenges arise. The following discussion

proposes research questions to meet these challenges in medical countermeasure safety and efficacy.

## 3 FUTURE RESEARCH DIRECTIONS

Growing threat awareness in the late 1990s coupled with the terrorist attacks of 2001—9/11 and the anthrax mailings—drove the development of new funding mechanisms and new regulatory pathways to speed medical countermeasure development. Subsequent efforts recognized the similarities between public health needs for disease caused by the intentional release of a CBRN agent and epidemics of naturally occurring disease such as Severe Adult Respiratory Distress Syndrome (SARS) and influenza. The use of these new funding streams and alternate regulatory pathways raise new questions about how best to evaluate countermeasure safety and efficacy.

### 3.1 Medical Countermeasure Safety

The need for accelerated development of medical countermeasures has made use of the existing Accelerated Approval Regulations and driven the finalization of the Animal Efficacy Rule as well as the legislation of the EUA. All three of these mechanisms may permit the development of efficacy data and therefore countermeasure availability with the study of smaller numbers of patients than would otherwise be the case. Accelerated Approval Regulations, developed originally to address the critical need for drugs to treat HIV, permit the use of a validated surrogate marker of efficacy, for example, diminution of HIV viral load rather than survival rate. This results in statistically sound data with a far smaller sample size than would be necessary to recruit for a study of survival benefit [15]. The Animal Efficacy Rule permits the development of efficacy data in animal models, though it does require safety study in humans [16], and EUA is determined on a case-by-case basis depending on the safety and efficacy data available at the time of the emergency requiring the countermeasure [10]. In all three cases, there is a requirement for human safety data, but there are no thresholds that specify how much is "enough". How do we determine the necessary size of a safety database for medical countermeasures for use in a public health emergency?

A look at the anthrax attacks of 2001 provides some context in which to consider this issue. During a period of several weeks in the fall of 2001, somewhere between 10,000 and 33,000 individuals received the antibiotic ciprofloxacin. The total number of individuals to receive any antibiotic during this period was larger. The drugs that were used in this public health emergency—ciprofloxacin and members of the penicillin and doxycycline classes—were well-studied and had all been in use for decades. Ciprofloxacin, the newest of these three, had been on the market since 1987 and at the time of the anthrax mailings given to approximately 300 million ($3 \times 10^8$) individuals worldwide. An expansion by the largest estimate of individuals exposed to this drug (33,000 or $3 \times 10^4$) is a relatively small one and would not be expected to greatly increase the chance of uncovering new or unanticipated safety problems. However it should be noted that even in the case of a well-studied and well-characterized drug like ciprofloxacin, the prolonged regimen of 60 days required for postexposure prophylaxis of inhalational anthrax was found to be associated with more frequent side effects [17].

Indeed even when rigorous premarketing trials have enrolled the traditional cohort of thousands of patients, there are instances when widespread market distribution and the subsequent expansion of the safety population has revealed rare, adverse events. There are two such instances in which vaccines were subsequently removed from the market. The rotavirus vaccine, RotaShield, was tested in premarketing clinical trials that enrolled 11,000 ($\sim 10^4$) patients and in 1998 was licensed by FDA to prevent diarrhea. Nine months and about 1 million ($10^6$) doses after licensure, RotaShield was associated with an unexpectedly high rate of intestinal intussusception in pediatric patients and shortly thereafter withdrawn from the US market [18]. Also, in 1998, the recombinant Lyme disease vaccine, LYMErix, was licensed by FDA. Premarketing trials enrolled about 10,000 patients ($10^4$). Nineteen months after licensing and the distribution of 1.4 million ($10^6$) doses, questions arose about the possibility that the vaccine caused or exacerbated arthritis. Though a cause-and-effect relationship could not be established, persistent concerns about this safety issue coupled with poor sales resulted in a withdrawal from the market in 2002 [19]. These cases are presented to demonstrate that even with premarket safety evaluation in a traditional cohort of $10^3$ or $10^4$, the expansion of the size of the population exposed to a drug or vaccine that results when the product is marketed, or deployed in a public health emergency, carries with it an inherent risk of uncovering new adverse events simply by enlarging the number of individuals who receive the product.

When we consider the possibility of a highly accelerated expansion of the size of a population likely to be exposed to a new countermeasure in the event of a public health emergency, we may anticipate an even greater likelihood of uncovering a previously unseen adverse event. The rate at which patient-exposures accrue may also affect the likelihood of uncovering a new adverse event not seen in premarket study. To take a simple example, a drug that is used in 10 patients per month will require 100 months of use to expand the safety database by 1000 patients. In a public health emergency, one might imagine the same drug may be used in 10 new patients per day, thus accruing an additional 1000 patients in 100 days or 3 months. If adverse events are reported, a clustering over 3 months is far more likely to be attributable to the new drug than a more attenuated series of reports over 100 months that may never pass the threshold of "background rate."

So how do we strike a balance between availability of needed countermeasures and adequate safety study such that the risk of unforeseen serious adverse events is minimized? What is also unique about CBRN medical countermeasures stockpiled by HHS compared with drugs developed for the commercial market is that with CBRN countermeasures, the denominator is known from the beginning. As shown in Table 2, BioShield/BARDA contracts specify a certain number of doses. Risk-benefit balances differ for every countermeasure. Pharmaco-epidemiologic tools may be invoked to assist in answering such questions as: "What is the number of patients in a safety database required to give adequate support to the number of doses of a countermeasure that the government seeks to purchase? Can we assess the risk of uncovering unforeseen serious adverse events for an investigational medical countermeasure, studied in perhaps 500 ($10^2$) or 1000 ($10^3$) patients, and intended to be given in an emergency to a population of 10,000 ($10^4$), 100,000 ($10^5$), or even millions ($10^6$ or more) of individuals? How do we factor in the rate of deployment when we assess such risk? Should available safety data guide the number of doses of a countermeasure that the government intends to purchase?

Should safety database requirements be linked to the number of doses the government seeks to purchase?"

These questions are made even more acute by the prospect of the use of the EUA, in which the federal government may decide to administer a drug or vaccine that is still in its investigational stages without informed consent. Generally the design of Phase III trials, including the size of the premarket safety database, is the subject of discussion between the manufacturer and FDA. However, when the federal government is the procurer of the product, in effect an investor in the manufacturer, public health policy makers become a third party to such discussions, which may then be an issue beyond the regulatory mandate of FDA. Recourse to established pharmaco-epidemiologic tools will greatly aid such decision-making and enhance preparedness.

### 3.2 Medical Countermeasure Efficacy

Because the diseases caused by CBRN threat agents are rare and ethical considerations preclude the intentional introduction of these agents into a human population for the purposes of scientific investigation, the use of animal models under the Animal Efficacy Rule has been and is expected to be a commonly used regulatory pathway for approval of such medical countermeasures. While animal models provide insight into human disease, the accuracy of such models depends on the similarity of the disease and the immune response in animals compared to humans. The only opportunity to evaluate efficacy in the human population of a medical countermeasure approved under the Animal Efficacy Rule may be the real test of a CBRN release.

Countermeasure development invariably opens new avenues of inquiry about a drug or vaccine, and no amount of planning, no matter how meticulous, can anticipate the specific public health needs of an ongoing attack or outbreak. Every effort should be made to learn more about such medical countermeasures when used in humans, and preparedness for a CBRN release, influenza, or any other public health emergency should include prospectively designed clinical trials to evaluate the performance of these countermeasures in the human population for whom they were intended. Even when an emergency calls for the use of countermeasures that have been studied previously in humans, the deployment of such a countermeasure represents a unique real-time opportunity, perhaps an imperative, to add to our knowledge base [20].

One of the stated goals of BioShield was to bring the benefits of advances in biotechnology to counterterrorism [10]. Indeed, since the program was launched, there have been government purchases of a next-generation smallpox vaccine specifically developed for those whose immunosuppression or other underlying health problems made them unable to take the traditional live vaccinia vaccine. While its first attempt was ultimately unsuccessful, HHS has sought to fund a next-generation anthrax vaccine that was based on recombinant technology. HHS has also purchased anthrax antitoxins intended for use in the treatment of patients with inhalational anthrax. These last two examples raise new questions that warrant investigation. How do we determine to replace an existing product in the stockpile with a "next-generation" drug or vaccine? Current FDA regulations do not require a head-to-head comparison for approval or licensure. But for a product for which the federal government both purchases and sets policy, this question falls outside the mandate of FDA. Should a head-to-head comparison be required as part of the efficacy evaluation of a next-generation product? What would such trials look like? Should different criteria apply when considering a countermeasure for civilians as compared to

the US military, the latter being a relatively young and healthy population for whom countermeasure administration can be mandatory?

The development of antitoxins or anticytokine drugs envisioned as treatment modalities to be used in concert with traditional antibiotic therapy raises additional research questions. How are such products used with antibiotics? What is the appropriate timing—both relative to disease progression and relative to the administration of antibiotics—for the most effective use of such countermeasures?

Developments in existing treatment modalities may also give rise to new questions. Prior to the anthrax attacks of 2001, standard of care for the treatment of inhalational anthrax was penicillin or some other single agent active against *B. anthracis* [21]. During the attacks of 2001, 5 of 11 patients (45%) who developed inhalational anthrax died. This mortality rate was far less than the traditionally reported 80–100% mortality for this disease. Empirical data showed that most of these patients received multiple antibiotics; this was often motivated by a common practice in toxin-mediated illness in which it is believed that a second drug that inhibits protein synthesis may be of added benefit to the patient. As a result of the association of this unproven practice with an empirically improved mortality rate, there has been a change in formal CDC recommendations for the treatment of inhalational anthrax. Now the standard of care is to start with two antibiotics [22]. To date there has been no prospective, randomized, controlled trial to evaluate the efficacy or safety of single versus double drug treatment. In addition to its implications for patient care, this recommendation can have a significant effect on the cost of drugs stockpiled by the federal government to treat inhalational anthrax.

Any study of efficacy of countermeasures against CBRN agents raises the issue of the use of animal models. In a few diseases, a preferred model, such as the rhesus monkey or green monkey has been established [23]. The supply of such experimental primates is finite, in some instances extremely limited. The prospect of more efficacy studies raises the issue of how to prioritize such efforts in a public health program that is federally funded. What alternative animal models provide comparable efficacy data? Or more important, what pharmacokinetic or pharmacodynamic models that do not use animals, provide efficacy data of comparable quality?

In addition to the issues described, a number of special categories of research in countermeasure development deserve mention here. As demonstrated by the anthrax attacks of 2001, a biological release may result in the sharp acceleration of the number of individuals who receive a given countermeasure over a short period of time. Swab and culture of the nares and also of environmental surfaces produced results that were used to make treatment decisions about the need for postexposure prophylaxis. In an unprecedented effort at countermeasure standard-setting, in 2002 the White House released a statement attesting to the unreliability of several of these environmental test kits [24], thus highlighting the need for accurate and reliable diagnostics for Category A pathogens. It should be noted that FDA regards any test used to make patient care decisions as subject to the regulations—and therefore the standards—for medical diagnostic devices. While BARDA influenza efforts include funding for diagnostics, till date there is little activity in this area for CBRN threats. A review of BARDA/BioShield contracts to assess funding of diagnostics shows that over the duration of the programs, only a single 2008 “Request for Information” on dosimetry techniques useful in triage after a nuclear or radiological release has been issued [25]. When we consider the number of regulatory mechanisms

now in place to make investigational countermeasures available in the event of an emergency, including without informed consent, the need for accurate diagnostic assays is particularly acute. Risk is best mitigated when certainty regarding exposure is optimized.

The unpredictability of what the human imagination might devise for release, for example, resistant or otherwise genetically modified pathogens, coupled with the lengthy process of countermeasure research and development raises the issue of multipotential vaccines based on a warm-base manufacturing process which is modified to accommodate a specific antigen based on a specific need. Investigators at the University of Oregon funded by the Department of Defense have reported on the development of a novel vaccine vector for multiple Category A pathogens with plans to test for immunogenicity in rhesus monkeys [26]. While present BioShield/BARDA efforts remain focused on countermeasure development for individual pathogens, further study and subsequent development of such a large capacity vaccine vector would elevate preparedness to a new level.

A similarly useful effort would be to evaluate drugs that target the cytokine cascade of sepsis that results from infection with any number of pathogens, including several biothreat agents. The survival advantage conferred by Protein C for patients with severe sepsis has been followed by identification of several potential targets in the sepsis cascade, many of which have reached a stage of development that warrants clinical investigation [27]. An added advantage to such a research effort is the utility of such drugs in patients with sepsis due to naturally acquired infections, another important public health challenge.

## 4 CONCLUSIONS

The past decade has seen an acceleration of research and development in medical countermeasures for CBRN threats. Beginning with the Bioterrorism Act of 2002, and subsequent legislation creating BioShield in 2004 followed by BARDA in 2006, the federal government has invested billions of dollars in the development and procurement of drugs and vaccines to meet these threats. Unique issues raised by efforts to accelerate development and make countermeasures available in an emergency warrant scientific investigation that will best protect the public and spend taxpayer funds in this important area of need.

## REFERENCES

1. United States General Accounting Office. (1999). *Combatting terrorism: chemical and biological supplies are poorly managed*.
2. CDC/Coordinating Office for Terrorism Preparedness and Response/Strategic National Stockpile/SNS website http://www.bt.cdc.gov/stockpile/ Accessed 6/24/09.
3. Rotz, L. D., Khan, A. S., Lillibridge, S. R., Ostroff, S. M., and Hughes, J. M. (2002). Public health assessment of potential bioterrorism agents. *Emerg. Infect. Dis.* **8**(2), 225–230.
4. CDC. (2001). Update: investigation of bioterrorism-related inhalational anthrax-Connecticut 2001. *MMWR Morbid. Mortal. Wkly. Rep.* **50**(47), 1049–1051.
5. Meselson, M., Guillemin, J., Hugh-Jones, M., Langmuir, A., Popova, I., Shelokov, A., and Yampolskaya, O. (1994). The Sverdlovsk anthrax outbreak of 1979. *Science* **266**, 1202–1208.
6. Henderson, D. A., Inglesby, T. V., Bartlett, J. G., Ascher, M. S., Eitzen, E., Jahrling, P. B., Hauer, J., Layton, M., McDade, J., Osterholm, M. T., O'Toole, T., Parker, G., Perl, T., Russell, P. K., and Tona, K. (1999). Working Group on Civilian Biodefense Smallpox as a biological weapon. *JAMA* **281**(22), 2127–2137.

7. Meyerhoff, A., Albrecht, R., Meyer, J., Dionne, P., Higgins, K., and Murphy, D. (2004). US Food and Drug Administration approval of ciprofloxacin hydrochloride for management of post exposure inhalational anthrax. *Clin. Infect. Dis.* **39**, 303–308.
8. Agres, T. (2002). Bioterrorism projects boost US research budget. *The Scientist* **16**(6), 26.
9. Public Law 108: 276. (2004). *Project BioShield Act of 2004*.
10. Gottron, F. (2009). *Project BioShield: Purposes and Authorities*. Congressional Research Service, Washington, DC 7-5700.
11. Animal Efficacy Rule FR Notice. (2002). **67**(105) http://www.fda.gov/OHRMS/DOCKETS/98fr/053102a.htm
12. US Department of Health and Human Services/ Assistant Secretary for Preparedness and Response/Pandemic and All Hazards Preparedness Act website http://www.hhs.gov/aspr/opsp/pahpa/index.html Accessed 6/24/09.
13. US Department of Health and Human Services/CBRN Activities/BARDA website https://www.medicalcountermeasures.gov/BARDA/CBRN.aspx Accessed 6/23/09.
14. Hsu, S. (2009). *Bipartisan WMD panel criticizes Obama plan to fund flu vaccine*. Washington Post June 8, 2009.
15. *Code of Federal Regulations: Subpart H-Accelerated approval of new drugs for serious or life-threatening illnesses*. 1999 21 CFR. Sect 314. 500–560.
16. Murphy, D. (2003). *Center for Drugs: CT Medical Countermeasures*. FDA Science Board November 6, 2003. http://www.fda.gov/OHRMS/DOCKETS/ac/03/slides/4001s1_09_Murphy.ppt#256,1, Center for Drugs: CT Medical Countermeasures accessed 6/25/09.
17. Shepherd, C. W., Soriano-Gabarro, M., Zell, E. R., Hayslett, J., Lukacs, S., Goldstein, S., Factor, S., Jones, J., Ridzon, R., Williams, I., and Rosentein, N. (2002). Antimicrobial post-exposure prophylaxis for anthrax: adverse events and adherence. *Emerg. Infect. Dis.* **8**(10), 1124–1132.
18. Clark, F. H., Offit, P. A., Glass, R. I., and Ward, R. L. (2004). Rotavirus vaccines. In *Vaccines*, 4th ed., S. A. Plotkin, and W. A. Orenstein, Eds. WB Saunders, Philadelphia, PA, pp. 1327–1345.
19. Steere, A. C. (2004). Lyme disease vaccine. In *Vaccines*, 4th ed., S. A. Plotkin, and W. A. Orenstein, Eds, Saunders. Philadelphia, PA, pp. 1267–1282.
20. Meyerhoff, A., and Lietman, P. (2009). *All the world's a laboratory*. Op-ed New York Times, New York, NY.
21. Friedlander, A. M. (1999). Clinical aspects, diagnosis and treatment of anthrax. *J. Appl. Microbiol.* **87**(2), 303.
22. Stern, E. J., Uhde, K. B., Shadomy, S. V., and Messionnier, N. (2008). Conference report on public health and clinical guidelines for anthrax. *Emerg. Infect. Dis.* **14**(4) http://www.cdc.gov/EID/content/14/4/07-0969.htm Accessed 6/24/09.
23. FDA CDER. (2002). *Guidance for Industry: Inhalational anthrax (post-exposure developing antimicrobial drugs animal models*.
24. Executive Office of the President, Office of Science and Technology Policy. (2002). *Memorandum on hand-held anthrax test-kits*, July 19, 2002.
25. US Department of Health and Human Services/Medical Countermeasures/CBRN Acquisition Activities. website https://www.medicalcountermeasures.gov/BARDA/procurement/CBRNactivities.aspx Accessed 6/24/09.
26. Nelson, J. A., Wong, S. W., and Jarvis, M. A. (2006). *Development of a Novel Vector for Multiple CDC Category A Pathogens*. Defense Technical Information Center Annual Report, April 2005-March 2006.
27. Glück, T., and Opal, S. M. (2004). Advances in sepsis therapy. *Drugs* **64**(8), 837–859.

# MEDICAL COUNTERMEASURES AGAINST EMERGING THREAT AGENTS

GIGI KWIK GRONVALL

*Center for Biosecurity of the University of Pittsburgh Medical Center, Baltimore, Maryland*

## 1 INTRODUCTION

The outcome of an infectious disease outbreak may depend on the resources to manage it. If medical countermeasures are available, and can be delivered in time, they could potentially save lives and save medical resources. Drugs could be used to treat the ill. Vaccines could be used to protect health care workers providing care to the sick. If the disease is contagious, vaccination may limit the spread of the disease, and some vaccines may be used even after exposure to prevent symptoms. Diagnostic tests can be used to rapidly distinguish people who need treatment, saving valuable medical resources for those who need them.

Although medical countermeasures could limit the numbers of deaths in a public health emergency, they may not be available. Vaccines, drugs, and diagnostic tests take years to develop, they are expensive, and technical hurdles add more money and time to their development. If a countermeasure is not available prior to a public health emergency, it may not be available for years afterwards. For example, in 2003, the severe acute respiratory syndrome (SARS) epidemic was managed without a vaccine or drug specific to the disease. Years later, a vaccine or drug is still not available. For other diseases, the technical challenges may seem insurmountable: for example, decades of research have not yet produced an HIV/AIDS vaccine, and much more research is needed [1].

In spite of the hurdles, making medical countermeasures available for use in an emergency is a major part of the US strategy to prepare for and respond to attacks involving biological weapons [2–5], as well as infectious disease threats such as pandemic influenza [6]. As there are many disease agents for which countermeasures are needed, it is also part of the US strategy to research new ways to shorten the time it takes to make medical countermeasures, as well to procure countermeasures that could be applied more than one threat [2, 4].

## 2 MANY BIOLOGICAL THREATS NEEDING COUNTERMEASURES

Medical countermeasures are needed for an array of biological threats. There are biological agents that are thought to be particular risks for bioterrorism, such as *Bacillus anthracis*, which causes anthrax disease, and *Variola* virus, which causes smallpox.[1]

[1]This article will use “anthrax”, “smallpox”, and so on, to describe both the causative agent of disease as well as the disease itself.

There are also emerging health threats such as multidrug resistant (MDR) tuberculosis, West Nile viral encephalitis, and the ongoing possibility that H5N1 avian influenza will become transmissible from person to person. In addition, diseases such as HIV/AIDS and malaria have some treatment options, but no effective vaccine countermeasures are yet available.

The Homeland Security Presidential Directive 18 (HSPD-18), also called *Medical Countermeasures against Weapons of Mass Destruction*, describes four broad categories of biological threats for which countermeasures are needed [4]:

- *Traditional agents.* These are biological agents or toxins that are naturally occurring, and have the potential to cause mass casualties if used as a weapon. Anthrax is an example of a traditional agent. It is a naturally occurring disease, and the bacteria can be isolated from infected animals, culture collections, or laboratories. In 2008, there have been reports of natural anthrax disease in livestock in India, South Africa, and Argentina [7].
- *Enhanced agents.* These are biological agents or toxins that have been "modified or selected to enhance their ability to harm human populations or circumvent current countermeasures". An example in this category could be antibiotic resistant anthrax. The former Soviet bioweapons program developed antibiotic resistant forms of anthrax [8], and methods to create resistance in the laboratory are readily available in the open scientific literature [9–11].
- *Emerging agents.* These are naturally occurring diseases, but could cause a serious risk to human populations. SARS would be an example of an emerging agent. There are many surveillance networks in place to detect new outbreaks of naturally emerging threats, including ProMed-Mail, Global Public Health Intelligence Network, and the Global Influenza Surveillance Network. For an overview see http://www.upmc-biosecurity.org/website/special_topics/global_disease_surveillance/.
- *Advanced agents.* These agents are more engineered than "enhanced" agents, and are not naturally occurring. They are "novel pathogens or other materials of biological nature that have been artificially engineered in the laboratory to bypass traditional countermeasures or produce a more severe or otherwise enhanced spectrum of disease".

In addition to these categories, there are other lists of pathogens for which countermeasures are needed, from the Department of Health and Human Services (HHS) and the Department of Homeland Security (DHS).

### 2.1 CDC and APHIS Select Agent Lists

The possession, use, and transfer of select agents from one facility to another are regulated by the Centers for Disease Control and Prevention (CDC) within HHS, and the Animal and Plant Health Inspection Service (APHIS) within the US Department of Agriculture (USDA). The CDC and APHIS have separate lists of biological agents, but there are some that overlap both agencies, including *B. anthracis*, the causative agent of anthrax disease.

The select agent list contains biological organisms and toxins that "have the potential to pose a severe threat to public health and safety" [12]. There are 81 select agents and toxins, 13 of which are found naturally in the United States. With the exception of the

1918 influenza virus, which includes any portion of the coding region of all eight gene segments, all of the select agents are "traditional" biological threats.

To be listed as a select agent, these biological agents were evaluated for their anticipated potential health impact, their dissemination potential, the public perception of them, and the degree of preparation required for public health officials to manage an outbreak caused by the agent. The biological agents were binned into three categories: A, B, and C, with category A having the highest priority, and being the most dangerous. Category A diseases, which include anthrax, botulism, plague, smallpox, tularemia, and viral hemorrhagic fevers, were judged to be the worst: they are highly lethal, cause serious public health threats, cause social disruption, and are either easily disseminated or they spread from person to person. Category B agents, which include glanders and Q fever, are in general less lethal than A agents. Category C agents are not necessarily less lethal than the other categories, but include emerging disease threats like Nipah virus and hantavirus, which are thought to be a bioterrorism threat in the future.

### 2.2 DHS Threat Agents

The 2006 Bioterrorism Risk Assessment, carried out by the DHS, included 28 biological agents that could lead to deliberate exposure of civilian populations [13]. Genetically engineered threats, to be considered in future DHS risk assessments, will further expand the number of agents. The specific disease agents on the list have not been publicly released.

DHS also issues material threat determinations (MTDs) for those chemical, biological, radiological, and nuclear (CBRN) agents thought to pose a threat sufficient to affect US national security, and population threat assessments (PTAs) to estimate the number of people who would be exposed to these threats in "high-consequence" scenarios. The agents that have MTDs are the top priorities for countermeasure development and acquisition into the strategic national stockpile (SNS).

To date, 12 MTDs have been issued for biological agents. These include *B. anthracis*, the causative agent of anthrax disease, as well as an MDR form of the bacteria; Marburg, Ebola, and Junin viruses, which cause hemorrhagic fever; botulinum toxins, which cause botulism; *Burkholderia pseudomallei*, which causes meliodosis; *Burkholderia mallei*, which causes glanders; *Rickettsia prowazekii*, which causes typhus; variola virus, which causes smallpox; *Franciscella tularensis*, which causes tularemia; and *Yersinia pestis*, which causes plague.

## 3 DEVELOPING COUNTERMEASURES TAKES A LONG TIME AND IS TECHNICALLY AND FINANCIALLY RISKY

Ideally, medical countermeasures would be available to counter all of these disease threats, whether they are the result of natural outbreaks or bioterrorism. Medical countermeasures would also be made quickly in response to new disease threats as they arise. However, the costs and logistical and technical challenges of developing and stockpiling medical countermeasures against each threat are considerable and possibly prohibitive. In addition to the costs of developing the countermeasures, acquiring sufficient quantities for the SNS and maintaining these supplies adds further expense and time.

The costs of developing and licensing a single drug or vaccine have been estimated at $880 million to $1 billion, and it typically takes 8–10 years to reach licensure by the Food and Drug Administration (FDA) [14, 15]. Investing this time, effort, and money does not guarantee success; most drugs fail. The technical difficulties of producing an effective drug may result in a lack of therapies or vaccines for many illnesses, even though much effort and money have gone into the attempt. The FDA approves between one in five [14] or nine [16] drug candidates that enter clinical trials.

The process of developing a countermeasure either for biodefense or for an emerging pathogen that does not have frequent outbreaks may be even more difficult than the usual path to FDA licensure, because efficacy tests may not be performed in humans. Usually, a countermeasure is challenged with the disease, either in a field trial or in a controlled clinical trial setting. This is not possible to do with many diseases on the select agent list or DHS MTD list: people rarely come down with these diseases naturally, and it is not ethical to expose healthy human volunteers. For some emerging health threats, such as West Nile virus, outbreaks are sporadic and thus not suited for a traditional clinical trial.

To address the problem of countermeasure efficacy testing in humans, the FDA created the Animal Efficacy Rule in 2002 [17]. The rule states that for FDA licensure, a countermeasure must protect animals from deliberate infection, and it must be safe in humans. The Rule does not eliminate testing in humans; clinical trials are still required to evaluate safety of the medical countermeasure and to help determine the appropriate dose. Although the Rule provides a path to licensure for biodefense and emerging threat countermeasures, for many of these diseases, however, there are no well-characterized animal models available [18]. Therefore, as an additional step, scientists need to develop, test, and validate animal models, as well as determine the efficacy and optimal dose of their countermeasures [19].

The novel challenges of the Rule requirements, compared with the traditional licensure pathway, may be one reason it has rarely been used to approve new drugs. The first countermeasure approved was pyridostigmine bromide in 2003, indicated for use after exposure to Soman, a nerve agent [20]. As a different dose of the drug had previously received FDA approval for treating myasthenia gravis, the Rule was not used for a novel compound, but to extend the indicated use of an already existent countermeasure. The second, recent approval was for hydroxocobalamin, indicated for victims of cyanide terrorism as well as smoke inhalation. [21]. This drug had been approved in France in 1996 and was available in the United States at a much lower dose [22]. To date, a totally novel countermeasure has not yet been approved using the Animal Efficacy Rule, 6 years after the rule was created.

## 4 GOVERNMENT IS THE SOLE DRIVER OF BIODEFENSE MEDICAL COUNTERMEASURES

A commercial market does not exist for vaccines, drugs, and other needed countermeasures for emerging threats or biodefense. HHS acknowledges that pharmaceutical and biotechnology companies are “reluctant to develop medical countermeasures for which there is no clearly defined, robust, sustainable, commercial market. In many cases, the anticipated rate of return on development of a new medical countermeasure for a specific threat may not justify the required resource allocations” [2].

The US government has thus had to create a market, and encourage drug and vaccine developers to participate. Largely, it has done this through Project BioShield [23] and also through the Biomedical Advanced Research and Development Authority (BARDA), created through the Pandemic and All-Hazards Preparedness Act [24].

President Bush announced the creation of Project BioShield in his State of the Union address on January 28, 2003 [25], and the Project BioShield Act was signed into law on July 21, 2004 [23]. The Act created a Special Reserve Fund for use in procuring CBRN countermeasures for the stockpile. Congress advance appropriated $5.6 billion to the fund for use over 10 years (Fiscal Year 2004–2013)[26]. In addition to the fund, BioShield increased the authority and flexibility of the National Institutes of Health (NIH) to develop the so-called "qualified countermeasures" (a drug, biological product, or device that the HHS Secretary determines is a priority) for CBRN threats and it permitted the use of medical treatments not approved by the US FDA in an emergency [27].

Project BioShield was intended to encourage industry to develop medical countermeasures for CBRN threats, primarily by creating a market for such products. Having a 10-year fund specifically for procurement of countermeasures was thought to be an incentive for industry, as it reduces the usual year by year change in governmental appropriations and political priorities [28]. However, even with this security, it was generally felt that Project BioShield did not go far enough to encourage industry participation in medical countermeasure development [29].

Project BioShield had a number of limitations, including that could not be used for the advanced development of medical countermeasures, and could only be used for late-stage procurement. This created a "Valley of Death" funding gap between early stages of product development and the acquisition of medical countermeasures for the SNS [30]. In addition, 5.6 billion over 10 years was not seen as sufficient to entice involvement of larger pharmaceutical companies. Thus, the experience of those companies in bringing products to market was not available to the government. Finally, BioShield contracts put developers at risk, as the government was the sole purchaser and could cancel contracts. The largest BioShield contract awarded, $877 million contract to VaxGen for the delivery of 75 million doses of rPA (recombinant protective antigen), was canceled on December 17, 2006, for failure to meet a contract milestone [31].

Title IV within the Pandemic and All-Hazards Preparedness Act legislation [24], signed on December 19, 2006, was intended to correct some of the shortcomings in BioShield. The Act created the BARDA to support advanced-stage research and development (R&D) funding for medical countermeasures against CBRN threats to bridge the Valley of Death for countermeasure developers. It gave HHS authority to make milestone payments, among other contracting authorities, to facilitate medical countermeasure development by sharing the financial burden of development with the manufacturers.

These authorities are managed by the new BARDA office within HHS, "the focal point within HHS to accelerate, facilitate, and support the development of medical countermeasures for the public against the highest priority man-made and natural public health threats facing the Nation" [2]. Since the creation of BARDA, there has been reason for optimism: there have been several contracts awarded, and a director for the office has been announced [32].

It is too early to tell whether BARDA will be successful in its aims. Its success will depend on a great deal whether its authority is funded commensurate with its purpose, and in line with the commercial market [33]. Unfortunately, one analysis of the cost estimates for medical countermeasures against biological threats found that the current level of funding for BARDA, $102 million, would only be sufficient to support only two

medical countermeasure developments in advanced development, with only a 30% chance of either candidate being successful [34]. Considering the long list of emerging threat and biodefense agents for which countermeasures are needed, this is not encouraging.

Regardless of funds, these efforts will take a long time, and so countermeasures will not be available for many disease threats for years. Even for a known threat, it can take years to build up the capacity needed to respond: one of the goals of the National Strategy for Pandemic Influenza is to have the capacity to "vaccinate the entire US population within 6 months of the emergence of a virus with pandemic potential". This capacity will be available in 2011, but an outbreak of pandemic influenza could occur at any time [35].

## 5 A FLEXIBLE STRATEGY TO GET NEEDED MEDICAL COUNTERMEASURES

The difficulty and costs of developing and procuring medicines and vaccines for each biological threat have spurred interest in alternatives to a "one bug, one drug" strategy. These alternatives have been referred to as *flexible defense* [36], though that remains a term of art [37].

The HSPD-18, issued January 31, 2007 [4], expresses the impracticality of developing and stockpiling medical countermeasures against every possible threat. It states that the US government should pursue novel medical countermeasures that could be used against multiple threats, "a rapidly deployable and flexible capability to address both existing and evolving [CBRN] threats". HSPD-18 also requires that HHS "target some investments to support the development of broad-spectrum approaches to surveillance, diagnostics, prophylactics, and therapeutics that utilize platform technologies ... [and that flexible defense] goals could include identification and use of early markers for exposure, greater understanding of host responses to target therapeutics, and development of integrated technologies of host responses for rapid production of new countermeasures" [4].

HHS intends to develop or acquire "broad-spectrum solutions using technologies that enable more flexible next-generation interventional concepts and to consider approaches and technologies derived from the commercial drug development sector to support the biodefense mission" [5]. HHS will "work with industry, academia, public health organizations, other government agencies, and stakeholders to foster innovation and promote strategic initiatives, such as the development of rapid diagnostics, broad-spectrum antimicrobials, and next-generation vaccine manufacturing technologies" [2].

A flexible defense may technologically be a ways off, and HHS has stated that a fixed defense approach is "effective and viable for some of the highest priority threats such as smallpox and anthrax". As the list of material threats increases, and technology advances, HHS will be focusing its medical countermeasures research, development, and acquisition efforts on broad-spectrum and platform approaches [5].

HHS classifies innovative or flexible approaches into three categories: broad-spectrum medical countermeasures, broad-spectrum technologies, and broad-spectrum platforms [2].

### 5.1 Broad-Spectrum Countermeasures that could be Used Against a Wide Range of Threats

Broad-spectrum medical countermeasures could include new antibiotics, antivirals, or drugs that target the clinical consequences of an infection, such as inflammation or

sepsis (infection in the blood). Another broad-spectrum approach is to minimize the transmission of a contagious disease by reducing the bioaerosols that a patient exhales [38]. Broad-spectrum products might also include point-of-care diagnostics capable of diagnosing a variety of biological infections.

Broad-spectrum products have several theoretical advantages over other biodefense-specific countermeasures: they could be developed and stockpiled prior to an emergency, reducing the need for rapid development and manufacturing during an infectious disease crisis; development would also benefit the treatment of illnesses that are not the result of an attack or a sporadic outbreak; also, if the drugs would be effective against other bacterial or viral diseases, they could be tested for effectiveness in humans. Companies would not need to solely rely on the FDA Animal Efficacy Rule for approval of the countermeasures.

### 5.2 Broad-Spectrum Technologies that Improve Product Performance

If the process of drug and vaccine development could be made much faster and cheaper, it could be possible to produce medical countermeasures against new, unanticipated threats in time to save lives. New methods to shorten and improve the development process are needed for *all* countermeasures, not just emerging threats. FDA developed the Critical Path Initiative in 2004 [39] to "stimulate and facilitate a national effort to modernize the sciences through which FDA-regulated products are developed, evaluated, and manufactured" [40]. As part of the Initiative, there are a "list-specific opportunities that, if implemented, can help speed the development and approval of medical products" [18]. Many opportunities are targeted to other countermeasure needs, including cancer and autoimmune diseases, but some would benefit the development and manufacture of medical countermeasures against infectious disease threats, such as being able to extrapolate from animal data to human experience, improving the measurement of vaccine potency and streamlining clinical trials.

HHS cites the need for new technologies that are "broadly available to improved product performance" [2]. These technologies could make countermeasures more affordable, if they include adjuvants (which boost the effectiveness of smaller amounts of a medical countermeasure), temperature stabilization processes (to ease the distribution and storage of medical countermeasures), and innovative delivery mechanisms (such as oral doses or patches, for ease of use). Other possible technologies cited by HHS include improvements in the formulation of drugs so that they are more bioavailable and immunomodulators.

## 6 PLATFORM TECHNOLOGIES TO ENABLE RAPID, COST-EFFECTIVE DEVELOPMENT OF DRUGS AND VACCINES AGAINST A WIDE RANGE OF THREATS

One example of a platform technology is the annual influenza vaccine. Every year, the influenza strains from which the vaccine is derived may differ, but the process of selecting the strains and producing the vaccine is the same. FDA approval, once received, is not necessary for year-to-year variations of the seasonal flu vaccine. Similarly, one can envision medical countermeasures platforms for other infectious diseases. A successful platform would be useful to respond to attacks employing unanticipated threat agents or attacks requiring quantities of countermeasures that would exhaust stockpile supplies.

The capacity to very quickly produce large quantities of countermeasures might also diminish the need to maintain large and expensive national stockpiles. There are some technology platforms in development, which may eventually prove useful for emerging disease threats: RNAi, a potential platform technology that could be used in therapies against a variety of biological agents such as ebola, SARS, or influenza; prophylactic and therapeutic antibodies; DNA vaccines; and virus-like particles (VLPs).

Flexible defense technologies are being worked on in multiple areas in government. NIH has funded the bulk of countermeasure research, including alternative delivery technologies, and has pursued research on adjuvants for influenza vaccines. Within the Department of Defense (DoD), the Defense Advanced Research Projects Agency (DARPA) has pursued the Accelerated Manufacture of Pharmaceuticals program, which is intended to create a rapid, cost-effective manufacturing system capable of producing 3 million doses of good manufacturing practice (GMP)-quality vaccines or monoclonal antibodies within 12 weeks. The Defense Threat Reduction Agency (DTRA) has initiated the Transformational Medical Technologies Initiative (TMTI) program, which focuses on developing broad-spectrum defenses against intracellular bacterial pathogens and hemorrhagic fevers.

## 7 CONCLUSIONS

The availability of medical countermeasures could change the outcome of a public health emergency, whether it is caused by bioterrorism or is the result of a natural outbreak. However, countermeasures are not yet available for most potential bioterrorist threats and emerging pathogens. For unanticipated threats, countermeasures could not be developed in time to be of assistance in the public health response. In the future, a twofold approach is needed: "fixed" countermeasures for specific threats and research into a more broad-spectrum, flexible defense, approach. For both approaches, however, the funding needs to be commensurate with the task.

## REFERENCES

1. Altman, L. K. (2008). "Rethinking is urged on a vaccine for AIDS". *The N. Y. Times*, http://www.nytimes.com/2008/03/26/health/policy/26HIV.html.
2. Public Health Emergency Medical Countermeasures Enterprise Biomedical Advanced Research And Development Authority (BARDA). (2007). *DRAFT BARDA STRATEGIC PLAN for Medical Countermeasure Research, Development, and Procurement*, U.S. Department of Health and Human Services, Editor. http://www.hhs.gov/aspr/barda/phemce/enterprise/strategy/bardaplan.html.
3. The White House (2004). *Homeland Security Presidential Directive/HSPD-10:Biodefense for the 21st Century*. http://www.whitehouse.gov/homeland/20040430.html, 2008.
4. The White House (2007). *Homeland Security Presidential Directive/HSPD-18: Medical Countermeasures against Weapons of Mass Destruction*. http://www.whitehouse.gov/news/releases/2007/02/20070207-2.html, 2008.
5. US Department of Health and Human Services: Office of the Assistant Secretary for Preparedness and Response (2007). *HHS Public Health Emergency Medical Countermeasures Enterprise Implementation Plan for Chemical, Biological, Radiological and Nuclear Threats*, Federal Register, pp. 20117–20128. http://www.hhs.gov/aspr/ophemc/enterprise/strategy/phemceimplementationplan.pdf.

6. U.S. Department of Health and Human Services (2005). *HHS Pandemic Influenza Plan*. http://www.hhs.gov/pandemicflu/plan/, 2008.
7. International Society for Infectious Diseases (2008). *ProMed-Mail, May 19*.
8. Alibek, K., and Handelman, S. (1999). *Biohazard: the Chilling True Story Of The Largest Covert Biological Weapons Program In The World, Told From The Inside By The Man Who Ran It*, Random House, New York.
9. Athamna, A., Athamna, M., Abu-Rashed, N., Medlej, B., Bast, D. J., and Rubinstein, E. (2004). Selection of *Bacillus anthracis* isolates resistant to antibiotics. *J. Antimicrob. Chemother*. **54**(2), 424–428. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=15205405.
10. Athamna, A., Athamna, M., Medlej, B., Bast, D. J., and Rubinstein, E. (2004). In vitro post-antibiotic effect of fluoroquinolones, macrolides, beta-lactams, tetracyclines, vancomycin, clindamycin, linezolid, chloramphenicol, quinupristin/dalfopristin and rifampicin on *Bacillus anthracis*. *J. Antimicrob. Chemother*. **53**(4), 609–615. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=14998982.
11. Athamna, A., Massalha, M., Athamna, M., Nura, A., Medlej, B., Ofek, I., Bast, D., and Rubinstein, E. (2004). In vitro susceptibility of *Bacillus anthracis* to various antibacterial agents and their time-kill activity. *J. Antimicrob. Chemother*. **53**(2), 247–251. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=14688054.
12. Centers for Disease Control and Prevention (2008). *Select Agent Program*, cited 2008 May 14, Available from: http://www.cdc.gov/od/sap/.
13. Committee on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis; Board on Mathematical Sciences and Their Applications; Division on Engineering and Physical Sciences (2007). *Interim Report on Methodological Improvements to the Department of Homeland Security's Biological Agent Risk Analysis*, in National Research Council Of The National Academies.
14. Adams, C. P., and Brantner, V. V. (2006). Estimating the cost of new drug development: is it really 802 million dollars? *Health Aff. (Millwood)* **25**(2), 420–428. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=16522582.
15. DiMasi, J. A., Hansen, R. W., and Grabowski, H. G. (2003). The price of innovation: new estimates of drug development costs. *J. Health. Econ*. **22**(2), 151–185. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=12606142.
16. Kola, I., and Landis, J. (2004). Can the pharmaceutical industry reduce attrition rates? *Nat. Rev. Drug Discov*. **3**(8), 711–715. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=15286737.
17. Food and Drug Administration (2002). *21 CFR Parts 314 and 601: New Drug and Biological Drug Products; Evidence Needed to Demonstrate Effectiveness of New Drugs When Human Efficacy Studies Are Not Ethical or Feasible*, Department of Health and Human Services, Editor, Federal Register.
18. US Food and Drug Administration (2006). *Critical Path Opportunities List*. http://www.fda.gov/oc/initiatives/criticalpath/reports/opp_list.pdf, 2008.
19. Gronvall, G. K., Trent, D., Borio, L., Brey, R., and Nagao, L. (2007). The FDA animal efficacy rule and biodefense. *Nat. Biotechnol*. **25**(10), 1084–1087. nbt1007-1084 [pii] 10.1038/nbt1007-1084 http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=17921984.
20. US Food and Drug Administration (2003). *"FDA Approves Pyridostigmine Bromide As Pretreatment Against Nerve Gas"*, FDA News, February 5, 2003.
21. US Food and Drug Administration (2006). *"FDA Approves Drug to Treat Cyanide Poisoning"*, FDA News, December 15, 2006.

22. (2006). *"EMD Pharmaceuticals Announces Submission Of New Drug Application For Cyanokit(R) For Treatment Of Cyanide Poisoning"*, Medical News Today, June 21, 2006.
23. (2004). *An Act to amend the Public Health Service Act to provide protections and countermeasures against chemical, radiological, or nuclear agents that may be used i006E a terrorist attack against the United States by giving the National Institutes of Health contracting flexibility, infrastructure improvements, and expediting the scientific peer review process, and streamlining the Food and Drug Administration approval process of countermeasures. "Project BioShield Act of 2004", in Public Law 108-276*.
24. Bush, G. W. (2006). *A bill to amend the Public Health Service Act with respect to public health security and all-hazards preparedness and response, and for other purposes: "Pandemic and All-Hazards Preparedness Act"*, in Public Law No: 109-417 http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.03678.
25. Library of Congress (2003). *The newshour with Jim Lehrer. State of the Union address. 2003-01-28*, PBS, United States.
26. US Governments (2007). *The US Government's Fiscal Year (FY) Starts on October 1 of the Previous Year, and Extends to September 30th of the Next Year. For Example, FY2007 Starts on October 1, 2006, and Extends to September 30*.
27. Gottron, F. (2007). *Project BioShield: Appropriations, Acquisitions, and Policy Implementation Issues for Congress, in CRS Report for Congress*., Congressional Research Service.
28. Russell, P. K. (2007). Project BioShield: what it is, why it is needed, and its accomplishments so far. *Clin. Infect. Dis*. **45**(Suppl 1), S68–S72. doi: CID50039 [pii] 10.1086/518151 http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=17582574.
29. Gronvall, G. K., Smith, B. T., Matheny, J., Mair, M., Chamberlain, A., Deitch, S., Borio, L., Inglesby, T. V., and O'Toole, T. (2007). Meeting report: Biomedical Advanced Research and Development Authority (BARDA) roundtable. *Biosecur. Bioterror*. **5**(2), 174–179.
30. Marczewsk, R. W. (1997). Bridging the virtual valley of death for technology R&D. *The Scientist* **2**(11), http://www.the-scientist.com/1997/01/20/11/1.
31. Department of Health and Human Services (2006). *"Termination Letter-Contract No. HHSO10020050000001C," Letter to VaxGen, Inx*, p. 1.
32. HHS Press Office (2008). *HHS Names First Director of the Biomedical Advanced Research Development Authority*. http://www.hhs.gov/news/press/2008pres/04/20080414a.html.
33. Matheny, J., Mair, M., Mulcahy, A., and Smith, B. T. (2007). Incentives for biodefense countermeasure development. *Biosecur. Bioterror*. **5**(3), 228–238. doi: 10.1089/bsp.2007.0030 http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=17903091.
34. Center for Biosecurity of UPMC (2008). *BARDA FY09 Advanced Development Cost Estimates for Medical Countermeasures Against Biological Threats*. http://www.upmc-biosecurity.org/website/resources/commentary/2008-01-31-barda_fy09.html, 2008.
35. Homeland Security Council (U.S.) (2006). *National Strategy For Pandemic Influenza: Implementation Plan*, Homeland Security Council, Washington, DC.
36. Relman, D. A. (2006). Bioterrorism—preparing to fight the next war. *N. Engl. J. Med*. **354**(2), 113–115. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=16407505.
37. Gronvall, G. K., Matheny, J., Smith, B. T., Mair, M., Chamberlain, A. T., Deitch, S., Borio, L., Inglesby, T. V., and O'Toole, T. (2007). Flexible defenses roundtable meeting: promoting the strategic innovation of medical countermeasures. *Biosecur. Bioterror*. **5**(3), 271–277. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=17903096.

38. Fiegel, J., Clarke, R., and Edwards, D. A. (2006). Airborne infectious disease and the suppression of pulmonary bioaerosols. *Drug Discov. Today* **11**(1-2), 51–57. doi: S1359-6446(05)03687-1 [pii] 10.1016/S1359-6446(05)03687-1 http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=16478691.
39. Food and Drug Administration (2004). *Innovation or Stagnation: Challenge and Opportunity on the Critical Path to New Medical Products*.
40. Andrew, C., and Von Eschenbach, M. D. (2007). *Commissioner of Food And Drugs at a Field Hearing at the University of Utah*, United States Senate Committee on Appropriations; Subcommittee on Agriculture, Rural Development, Food and Drug Administration and Related Agencies, Salt Lake City.

## FURTHER READING

Relman, D. A. (2006). Bioterrorism—preparing to fight the next war. *N. Engl. J. Med*. **354**(2), 113–115. http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=16407505.

Gronvall, G. K., Matheny, J., Smith, B. T., Mair, M., Chamberlain, A. T., Deitch, S., Borio, L., Inglesby, T. V., and O'Toole, T. (2007). Flexible defenses roundtable meeting: promoting the strategic innovation of medical countermeasures. *Biosecur. Bioterror*. **5**(3), 271–277.

Matheny, J., Mair, M., Mulcahy, A., and Smith, B. T. (2007). Incentives for biodefense countermeasure development. *Biosecur. Bioterror*. **5**(3), 228–238. doi: 10.1089/bsp.2007.0030 http://www.ncbi.nlm.nih.gov/entrez/query.fcgi?cmd=Retrieve&db=PubMed&dopt=Citation&list_uids=17903091.

# BIODEFENSE WORKFORCE

KAVITA M. BERGER

*American Association for the Advancement of Science, Washington, D.C.*

## 1 INTRODUCTION

Biodefense is defined as defensive measures against a biological weapons attack, while biosecurity has been more broadly defined as measures to protect against harm from a biological agent and includes traditional biodefense and public health activities. Since 2001, activities associated with biodefense and biosecurity seemed to have conflated so that both terms describe the full range of activities to prevent and mitigate an attack using biological weapons.

Prior to 2001, US biodefense activities were mainly restricted to the Department of Defense (DoD). These included policy discussions, threat characterization, countermeasure development, and scientist redirection (termed *cooperative threat reduction*) activities. Toward the end of the 1990s, the Department of State (DoS) started their own scientist and facility redirection activities. A few select biosecurity programs, like the select agent program and export control program, were overseen by other US agencies. Much of the biodefense workforce came from a military, public policy, or nuclear arms control background. Civilian life scientists in the United States either were generally not aware of these activities nor were they formally trained in biological arms control and nonproliferation. Although a few scientists were working with select biological agents, their goal was not biodefense but rather to understand pathogenesis and host immune response for improved public health. Even following the public admission of the Soviet Union's large-scale offensive biological weapons program [1, 2], few practicing scientists were educated on or engaged in traditional biodefense activities. Similarly, much of the public policy or government biodefense workforce did not have formal training in biodefense policy or the biological sciences; they learned from their past nuclear arms control experiences.

Today, the situation is very different. Following 9/11 and the anthrax letters in 2001, biodefense has significantly expanded to incorporate global health, public health preparedness and response, government service, and active participation by the nongovernment research community in biodefense activities. The Department of Health and Human Services (HHS), Department of Homeland Security (DHS), United States Department of Agriculture (USDA), DoS, Department of Energy (DoE), DoD, Environmental Protection Agency (EPA), and the Intelligence Communities (IC) have responsibilities in biodefense. HHS and DHS support biodefense research, including select agents (http://www.cdc.gov/od/sap/docs/salist.pdf), at centers of research excellence in academia. HHS, DoD, and the Office of the Director of National Intelligence have advisory or expert groups involving academic scientists. Civilian scientists working on select agents have been contacted by the Federal Bureau of Investigation (FBI) during investigations for their subject-matter expertise [3, 4]. In addition, HHS contracts with private biotechnology companies to develop medical countermeasures (vaccines, drugs, delivery devices, and other medical devices) against chemical, radiological, nuclear, and biological threats that are considered of highest priority to the United States. Total funding of civilian biodefense activities rose from $576 million in 2001 to over $5 billion in 2008 [5]. Thus, the academic and private biological sciences community became immersed in the post-2001 biodefense infrastructure.

Much of the biodefense workforce is being trained on-the-job. More academic and industrial biodefense researchers are being trained in laboratories on how to work with select agents, develop diagnostic tests and medical countermeasures against priority threats, and evaluate their research for dual use potential. Public health officials and health care providers are being trained in hospitals and public health departments to properly recognize and diagnose unusual disease outbreaks and respond appropriately. Younger biosecurity experts are being trained mainly through apprenticeships in government agencies or nongovernmental organizations. This unstructured training of today's biodefense workforce fosters an environment where different biodefense communities function independent of one another and lack a clear and comprehensive understanding of the other communities.

### 1.1 Biodefense Education Programs

Education programs, though not many, have recently emerged at a few universities to address the lack of education of biological scientists and public policy or government personnel in biodefense. Three types of programs currently being developed are (i) public policy courses in biosecurity, biological weapons, and public health preparedness; (ii) courses educating practicing life scientists about biosecurity for scientific responsibility and biosafety; and (iii) bioterrorism preparedness and response courses for educating public health and health care workers in responding to a chemical, biological, radiological, or nuclear (CBRN) attack. A few examples of existing programs are described below.

Georgetown University has two programs, one for biological scientists in Biohazardous Threat Agents and Emerging Infectious Diseases (http://grad.georgetown.edu/pages/certif_biohazard.cfm), and the other for nonscientists in Biodefense and Public Policy (http://grad.georgetown.edu/pages/certif_biodefense_ppol.cfm). The first program is designed to educate scientists in the characterization of biological and chemical agents, disease surveillance, medical countermeasures, biological and radiological safety, and the history of infectious diseases. The second program is designed to educate students on the technical facets of emergency and incident response. The George Mason University offers a masters and doctoral program in biodefense (http://bioterrorism.slu.edu/DegreeProg07/IBS07index2.html), which professes to train the next generation of biodefense professionals and bridge the gap between scientists and public policy. The University of California (UC), San Diego's Institute for Global Conflict and Cooperation (http://igcc.ucsd.edu/PPBT.php), provides a 3-week short course on biodefense policy for doctoral students and postdoctoral fellows in the UC system. The University of Virginia offers a biodefense track for doctoral students in Microbiology, Immunology, and Infectious Diseases (http://www.healthsystem.virginia.edu/internet/bims/advancedresearch/biodefense_res.cfm). This program offers students the opportunity to combine their scientific courses with biodefense-related courses. Texas Tech University offers a concentration in biodefense law for law students (http://www.ttu.edu/biodefense/) and the St. Louis University School of Public Health offers a program in Biosecurity and Disaster Preparedness for health care workers and public health officials (http://www.bioterrorism.slu.edu/DegreeProg07/IBS07index2.html).

A few universities, nongovernmental organizations, and university consortiums have incorporated biosecurity into their ethics programs for scientists. These courses are focused mainly on educating life scientists about biosecurity and scientific responsibility. These courses, however, do not educate scientists from the computer, engineering, physical, and chemical sciences who work in the biological sciences (e.g. biophysics and systems biology) in biosecurity. Much of the discussion of biosecurity in these courses is related to dual use research (legitimate research that could be misused for malicious purposes) and the select agent regulations. The National Science Advisory Board for Biosecurity, an advisory committee to the US federal government on education and oversight of dual use research, has currently recommended that laboratory Principal Investigators perform initial review of their research for dual use potential, which would then be followed up with subsequent review by the Institutional Biosafety Committees (IBCs) at universities if necessary. This two-tiered review strategy requires that both individual scientists and the IBCs are capable of identifying research with dual use potential and that they consider ways to minimize potential national security risks. The Southeastern Regional Center of Excellence for Emerging Infections and Biodefense (SERCEB), an HHS center of excellence, developed an on-line education module for their

researchers regarding dual use research (http://www.serceb.org/modules/serceb_cores/index.php?id=3). Similarly, the Federation of American Scientists has developed an on-line portal (http://www.fas.org/biosecurity/education/dualuse/index.html) using case studies to educate scientists and others about potential dual use experiments and concerns. A few Americans and British have also engaged scientists abroad to evaluate the potential risks of their research and determine how to minimize those risks while still conducting their research [6–11].

As a result of the rapid growth of civilian biodefense funds and establishment of academic centers of excellence, more scientists have started working with select agents and more high-containment laboratories are being built to accommodate the increased select agent research. While all research institutions working with select agents are required to follow the biosafety guidelines listed in the Center for Disease Control and Prevention (CDC)'s Biosafety for Microbiological and Biomedical Laboratories, training biosafety officers and laboratory scientists varies among institutions. These are examples and not the only programs in existence. The National Institutes of Health administers a 2-year fellowship program, the National Biosafety and Biocontainment Training Program (http://www.nbbtp.org/), to train biosafety and biocontainment professionals. These individuals then go and train biosafety officers at institutions, who in turn train their laboratory personnel. The program's goal is to establish uniform standards by which biosafety officers can train laboratory personnel in laboratory biosafety. Emory University has a more extensive biosafety training program that incorporates training in mock biosafety level 3 and 4 laboratories (http://www.sph.emory.edu/CPHPR/biosafetytraining/index.html). In addition, the US DoS's Biosecurity Engagement Program (http://www.bepstate.net/) aims to upgrade public health and research laboratories to prevent theft of harmful agents by non-state terrorist organizations and educate the laboratory personnel on effective biosafety techniques to prevent accidental infection of laboratory workers in Asia.

### 1.2 Challenges

Several key challenges emerge from discussions surrounding the biodefense workforce. The main challenge is making the training program sustainable. Regardless of the audience, the programs must be self-sufficient and sustainable to withstand political will and funding fluctuations. The DoS's efforts for enhancing pathogen security and biosafety training in Asia is intended to be sustainable; their program is designed to train local laboratory personnel in biosafety and these individuals then go and train other local biosafety personnel and/or laboratory workers. Any education programs developed to build and maintain a knowledgeable biodefense workforce in the US would also have to sustain fluctuations in funding and political will.

Although most existing university-based biodefense programs are important for educating the future workforce in the basics of biosecurity, specialized skill sets are required for different biodefense activities. To best tailor training programs for different biodefense programs, one must assess the needs of these programs. In support of this, a published study of HHS's biodefense agencies suggests that a needs assessment, federal hiring strategies, and funding for training and salaries are all critical to improving the government biodefense workforce [12]. Another published study assessed the needs of public health officials required to prepare for and respond to a bioterrorism incident [13]. This study identified cross-disciplinary training, funding for training and salaries, and

integrated, large-scale exercises where lessons are easily learned as major components to establishing a public health workforce knowledgeable in responding to biological attacks. On the basis of a needs assessment, program specific training courses can be designed to help develop the workforce for each biodefense activity.

The skills needed for specific biodefense activities must be by definition cross-disciplinary to best address the needs of the programs (e.g. DoS's Asia pathogen security program requires an understanding in the life sciences, public health, and cultures of the countries engaged). Cross-disciplinary education is extremely important to establish and maintain a complementary, coordinated, well-integrated, and cooperative biodefense workforce, which allows people of differing expertise (i.e. scientists, health care practitioners, and the security community) to accept each other's perspectives and work together. In addition, this cross-disciplinary education extends to international relations and political science. As the US moves to engage scientists and public health workers in friendly nations or nations outside the Former Soviet Union (FSU), biodefense personnel must adapt and understand the new economic and political climates, cultures, and languages of the non-FSU nations they work with. This type of cross-disciplinary training will be essential for effective scientific and security engagement with nations. The cross-disciplinary biodefense workforce working in concert with a number of subject-matter experts will ultimately be the key to success for biodefense activities.

### 1.3 Case Study

This article focuses on the workforce and skill set needed to initially review the potential threat of an emerging biotechnology. Using the rapidly advancing technology of synthetic biology, the case study presented below highlights the skills necessary for the threat characterization workforce to address key policy questions related to advancing biotechnologies. This initial evaluation is essential for determining whether an emerging biotechnology is a potential national or international security threat or whether it is completely benign. Further policy discussions would require advice from subject-matter experts and the intelligence community. This tiered approach with a knowledgeable workforce to initially triage which technologies could pose reasonable threats to national security allows for in-depth discussion of the more serious threats while minimizing the impact on the scientific community. Since threat characterization is just one of many biodefense activities, this article ends with a short description of workforce needs in other areas of biosecurity.

## 2 CASE STUDY: SYNTHETIC BIOLOGY: NATIONAL SECURITY THREAT OR BENEFICIAL SCIENCE

Although many case studies, real or fictional, have been described to understand capabilities or concepts, few, if any, have been described to address workforce issues. The case study presented here addresses the question, "What workforce training is needed to assess the potential threat of an emerging biotechnology?" Although subsequent analyses may require subject-matter experts and intelligence information, initial evaluation of whether an advancing technology poses a potential national security threat requires knowledgeable staff to address key scientific and social questions. These questions include, but are not limited to, the following:

1. What is the current state of the science and how rapidly is it advancing?
2. Can the technology be used to generate harmful pathogens or toxins (novel or known) for nefarious purposes?
3. How effective are (synthetic) pathogens at surviving outside the laboratory and causing harm to the target population?
4. Does the technology reduce the utility of our current defenses?
5. Does the technology pose a greater threat than more traditional techniques, like isolating pathogens from the environment or sick individuals? Is this true for all pathogens or some?
6. What are the risks and benefits of the science? What are the burdens placed on science by potential risk management strategies?
7. Who has the capability to replicate the science?
8. Are there opportunities for maximizing transparency of researchers using the technology and minimizing misuse of the technology?

This case study starts by describing the technology of synthetic biology, followed by a discussion about the expertise needed to evaluate whether synthetic biology poses a threat to national security in a globalized world.

### 2.1 Background in Synthetic Biology

Narrowly defined, synthetic biology (commonly grouped with synthetic genomics) is the creation of biological organisms (or whole genomes) from scratch—i.e. an intact biological organism is generated from a complete genome made from chemically synthesized genes or small DNA fragments. It is a rapidly advancing biotechnology with many beneficial applications to medicine and public health as well as development of alternative energy sources. The biosecurity community, however, views synthetic biology as a real threat to national and international security. The speed at which the DNA synthesis technology is advancing suggests to the security community that the technology will be affordable and easily attainable within the next 5–10 years.

In 2002, the Wimmer laboratory at the State University of New York at Stony Brook published an article in *Science* on chemical synthesis of poliovirus [14]. In the publication, Wimmer and colleagues discussed how they created the poliovirus genome by joining together short fragments of DNA, which they ordered from a DNA synthesis company. To distinguish their synthetic genome from one simply isolated from a laboratory strain of poliovirus, they incorporated a very short piece of DNA into the synthetic genome sequence in a manner that would not affect the protein sequence. They used a cell-free system to grow the virus from the synthetic genome. The authors created a live poliovirus, but its ability to infect mice was greatly reduced compared to the wild-type laboratory strain. This experiment raised alarms within the scientific community as a potential security concern since it was the first time a live pathogen could be generated without an existing template. The National Research Council used this and other examples in their report, *Biotechnology Research in an Age of Terrorism*, to highlight the potential security problems associated with some biological research [15].

Shortly after Dr Wimmer's paper was published, researchers at the J. Craig Venter Institute published a paper claiming the complete chemical synthesis of a bacterial virus, bacteriophage PhiX174, in just 2 weeks [16]. The paper described in detail how the

bacteriophage was synthesized and tested. This paper alarmed the White House resulting in greater concern about synthetic biology as a potential security concern. The National Science Advisory Board for Biosecurity, created in 2004 under the auspices of the National Institutes of Health, was tasked to review synthetic biology and provide recommendations for how the federal government could oversee such research.

The American scientific community working in synthetic biology came together in 2004 to discuss the science. Since then, they held annual meetings on synthetic biology expanding their audience to include domestic and international scientists and government and nongovernmental organizations, and broadening the scope of the discussion to include social and security implications of the technology. At the second annual meeting, Synthetic Bio 2.0, in 2006, participants recognized that synthetic biology could pose some threat to national security and responded by drafting recommendations for self-governance by the scientific community. As the scientific and policy communities began considering the potential threat of synthetic biology, they responded by recommending actions that the scientific community could adopt to prevent misuse of the technology, such as monitoring synthesis requests, educating life scientists about the safety and security risks, and overseeing academic research for their dual use potential [17]. Several DNA synthesis corporations have also considered the potential threat of synthetic genomics, and developed and implemented measures to screen orders for their similarity or identity to select agents (http://polysynth.info/). [18] One company, Blue Heron, stated that they rejected at least one order for international security reasons. Despite the concerns that synthetic biology can be misused to generate harmful pathogens, researchers at the J. Craig Venter Institute continue to streamline and advance protocols for the chemical synthesis of pathogens [19].

The perception of the threat of synthetic biology has extended beyond the United States to European nations. Actions taken by Western nations and companies do not necessarily translate well to other parts of the world where the advancing biotechnology industry is expected to provide great benefit to public health and economic growth. For example, nations with economies in transition, such as India and China, have thriving biotechnology industries. Given this globalization of biotechnology and the value of advancing biotechnology to health and economies, having cross-disciplinary training in science, public health, and the cultural and political climate will allow those assessing threats, like synthetic biology, to integrate information gathered from intelligence and subject-matter experts to make informed reasonable evaluations about the risk of the emerging biotechnology.

The following sections break down the expertise needed to address key questions in assessing risk using synthetic biology as an example of an advancing biotechnology. This article will not address intelligence gathering or communication and collaboration with subject-matter experts *per se* but does recognize that these expertise are essential to fully address whether a given technology poses a threat. Existing educational programs will be referenced where appropriate.

## 2.2 Scientific Expertise Needed

Creating a dangerous pathogen or toxin from a published sequence requires obtaining the sequence, the DNA fragments or DNA synthesizer and reagents, laboratory materials, cells, and expertise needed to create the pathogen from a chemically synthesized genome as well as testing the infectivity and virulence of the pathogen in cells and/or animals,

weaponization, production, and dissemination. Although some of the steps in this process are available, inexpensive, and relatively easy to perform, others are not. Also, the fact that many large DNA synthesis companies, for example Blue Heron, are screening their orders for suspicious sequences adds a layer of complexity to the entire threat characterization process. Alternatively, isolating many harmful pathogens from nature is relatively easy and low cost. A strong science background is necessary to place the emerging technology on a spectrum of risk, which would not only include all other available techniques for creating or isolating harmful pathogens and toxins but also the risk of theft, accidental exposure, and natural infection. Placing the technology on such a risk spectrum would contribute to determining credibility of the threat, its priority compared to other threats, and potentially available options for action.

Life scientists, engineers, physicists, and computer scientists all play a role in advancing biotechnologies. The rapidly growing field of systems biology and computational biology is possible only because of the expertise of bio-savvy computer scientists. Development of medical devices, advanced technology for vaccine or drug delivery, and gene and protein arrays require knowledge in biophysics and bioengineering. Characterizing the current and future state of the technology and downstream applications requires a broad interdisciplinary training in the physical, chemical, and computer sciences as well as life sciences. Over the last 15 years, a few academic institutions have started interdisciplinary programs incorporating bioengineering, biophysics, and the life sciences. Two notable examples of this are Georgia Institute of Technology's Institute for Bioengineering and Biosciences (http://www.biology.gatech.edu/facilities/) and the Georgia Institute of Technology and Emory University Biomedical Engineering Program (http://www.bme.gatech.edu/).

Although synthetic biology requires knowledge of basic molecular biology techniques, advances in synthetic biology are dependent on DNA synthesizer technology, which is designed and built by engineers, physicists, and chemists. Four major features of DNA synthesizers contribute to the pace of its technological advancement—accuracy of the synthesized DNA, speed of generating DNA molecules, ability to multiplex, and ability to be fully automated. As these features improve, chemical synthesis of DNA is likely to become cheaper and easier to do. This not only benefits individuals who are interested in acquiring the end product, DNA fragments or genes, but also those who want to purchase older models of DNA synthesizers. Training in engineering and chemistry can greatly enhance one's ability to predict future technological advancements and how fast these advancements can occur.

Life scientists are best qualified to address the emerging capability of synthetic biology technology. The J. Craig Venter Institute reported that they synthesized the entire genome of bacteriophage PhiX174 in just 2 weeks [16]. They did not publish that they spent more than 2 years troubleshooting the system to streamline the chemical synthesis process [20]. This delay demonstrates two problems with the security community's assessment of the current capabilities of the science: (i) although a PhD in the life sciences is not a necessity, tacit knowledge of the procedure for generating the genomes and subsequent pathogens is required to troubleshoot any problems during the experiments [20] and (ii) the technological requirements needed to synthesize large pathogens and priority threat agents are orders of magnitude more complex than synthesizing a bacteriophage and small viruses and may require new scientific discoveries to achieve. Training in the life sciences would provide the necessary expertise to take into account these problems when assessing the ability of the technology to create a functional and dangerous

pathogen. Furthermore, experience in microbiology, virology, and ecology, specifically, could be very useful in determining whether a synthetic pathogen could survive outside the laboratory setting, thereby increasing the possibility it could be used to cause significant harm to human, animal, or plant populations and the surrounding environment.

This assessment may differ for chemical synthesis of toxins. Synthetic genes could serve as templates for chemical synthesis of proteins, like toxins, immunoregulators, neuroregulators. Training in the life sciences, including biochemistry and toxicology, and chemistry is necessary for assessing the impact of the chemically synthesized protein on life functions. These expertise can help when assessing the stability of the synthesized protein, determining whether it requires further chemical or structural modification to function properly and the ease of adding these modifications accurately, and predicting the body's reactions to the synthesized protein. With their advanced knowledge of the science, life scientists and chemists are well suited to determine the minimum requirements for creating harmful and functional toxins from scratch.

Assessing whether technology, such as synthetic biology, can produce biological agents that subvert or reduce the effectiveness of current defenses (vaccines, drugs, medical devices, and nonmedical interventions such as isolation) requires knowledge of epidemiology and outbreak response as well as the life sciences. Relatively few public health students get trained in infectious disease epidemiology, but being well educated in conducting epidemiologic analyses of infectious diseases and outbreak response are critical when assessing whether an emerging technology can evade current defenses. This training helps to determine whether synthetic biology can create functionally dangerous pathogens or toxins that reduce the impact of current public health interventions. Although the life sciences allow one to determine the ease of creating vaccine and drug resistant dangerous pathogens, the public health training allows one to determine possible outbreak scenarios for the synthetic pathogen or toxin. This added knowledge can help to inform whether a chemically synthesized biological agent truly has the ability to reduce the effectiveness of public health interventions.

Knowledge of the physical, chemical, and life sciences as well as public health, medicine, and veterinary medicine is important for comprehensively assessing the risks and benefits of the emerging technology as well as placing the technology on a risk spectrum with other currently available technologies. Although synthetic biology can pose national and international security risks, many legitimate laboratories are using the technology for beneficial purposes (http://sb4.biobricks.org/). The potential risk of misuse of the technology by a nefarious group and the risks associated with policies and regulations to prevent the misuse of the technology should be weighed against the potential benefits of the technology to health and agriculture. Moreover, any risk management strategy should also be weighed against the potential burdens to industry and science. Those who have knowledge of the science and consequences of regulations and policies on current research may be in the best position to consider the spectrum of risks and compare them with the benefits and burdens. Finally, interpreting scientific publications and engaging in international scientific collaborations, though currently complicated by visa issues and export control and select agent regulations, offer a sense of transparency in the international scientific community by leaving lines of scientific communication and cooperation on research activities open.

### 2.3 Cultural and Political Expertise Needed

Beyond scientific characterization of the threat, vulnerability, and consequences, determining the immediacy of the threat requires yet another set of skills. Those skills include cultural anthropology and political science as well as intelligence gathering. To understand whether a subnational group or a nation could be misusing beneficial technology or developing technologies for nefarious purposes, one has to have a good understanding of the political and economic climate, history, and cultures and religions of various nations throughout the world. Nations that do not have a history of biological weapons development or harboring terrorists may have a lower likelihood of using biotechnology for malicious purposes. However, nations that are known to have terrorist organizations living within their borders or interacting with their population may provoke a higher level of suspicion. This is also true for nations or groups that support martyrdom and have a history of violence toward other cultures, religious groups, and nations to achieve their political objectives. Thus, training in world cultures, history, and political and economic climates is essential for contextually assessing the risk of a technology. Also critical to these questions is the ability to gather human intelligence, a function which scientific collaboration and communication facilitate.

### 2.4 Suggested Training Program

Any training program developed to evaluate the risk of an advancing biotechnology to national or international security must include the relevant scientific and sociological expertise described above. This program would include courses in the life, physical, chemical, and engineering sciences, outbreak response and epidemiology as well as courses in biological weapons and biosecurity, cultural and political anthropology, and current events. One option for developing a curriculum could be to have bright scientists from interdisciplinary science programs, like those offered at Georgia Tech, and students from schools of public health, medicine, or the veterinary sciences take courses in the relevant social and political sciences. To enhance the students' experiences, they could be required to do several internships to better understand the needs of the threat characterization and other biodefense communities. Such a program would provide the broad background needed to ask key questions to triage emerging biotechnologies as potential threats or not. As previously stated, further policy discussions and threat determination would require subject-matter experts and intelligence information.

### 2.5 Conclusion

Does the current biodefense workforce have the necessary expertise to address the following question: "Is there enough evidence that unfriendly nations have the knowledge and tools to create, from published sequence, a functional dangerous pathogen or toxin that could evade existing defenses and be devastating to human, animal, or plant health or the environment?" The workforce does not currently have the specialized expertise to appropriately address this question. To assess the potential threat of synthetic biology, or any emerging biotechnology, the workforce needs to be trained in the hard sciences, epidemiology, and social sciences. With this broad, cross-disciplinary training, the workforce can ask and initially address key questions to determine whether a biotechnology poses a threat or not. Subsequent consultation with subject-matter experts and the intelligence community can enhance or diffuse that threat determination.

## 3 ADDITIONAL BIODEFENSE WORKFORCE NEEDS: GLOBAL HEALTH SECURITY AND AGRICULTURE SECURITY

### 3.1 Global Health

Prior to the anthrax mailings in 2001, the public health community was largely removed from national security activities. Since 2001, however, the public health sector has been tasked with the responsibility of preparing for and responding to CBRN attacks. The health care and public health communities are now considered vital to national security interests because they help mitigate the consequences of a CBRN attack and help recovery efforts following an incident. To fulfill this task, public health officials and health care professionals now require training in biodefense preparedness and response. This added requirement is complicated by the fact that the current public health workforce will be retiring within the next 5 years and very few public health officials are being trained to replace them. In individual hospitals and doctors' offices, few physicians and nurses are being trained in biodefense and few, if any, have experience detecting diseases caused by many of the US priority threat agents. Many developing nations do not have sufficient health care and public health capabilities to effectively identify and respond to an outbreak of potential international concern. The recently revised International Health Regulations (IHR2005), although mostly relevant to unusual CBRN disease outbreaks, were designed to push nations to upgrade their national health care systems to a minimum standard. Many nurses and physicians from developing nations leave their home country to work in developed countries, where they are able to earn more money and therefore could contribute more effectively to their family's well-being. Thus, there is a real need to train health care professionals in bioterrorism and public health response throughout the world.

### 3.2 Agriculture Security and Food Defense

The increased interdependence of nations in trade of agricultural and food products presents a very important biosecurity concern. Protecting their products from natural, accidental, or intentional contamination is in the industry's best interests and required to protect market value and consumer confidence. The DoS is working with the Asia Pacific Economic Cooperation (APEC) countries on food defense out of recognition that the food industry is critical to global economic prosperity and the availability of food (http://www.state.gov/r/pa/prs/ps/2006/75537.htm). Educating individuals on biosecurity measures to prevent contamination, identify contaminated products, and disinfect and dispose of contaminated food products is critical to international agricultural security and food defense.

## 4 CONCLUSION

Building a sustainable workforce for all biodefense activities requires training programs to meet the needs of those activities and to be cross-disciplinary and broad, sustainable, and standardized. The case study presented in this article uses synthetic biology to address the question of what expertise and training is needed for threat characterization of emerging biotechnologies. Cross-disciplinary training in the hard sciences, epidemiology, and social sciences allows the threat characterization workforce to ask and address

several key policy questions to effectively assess whether a given technology is a potential threat or not. Following this first tier of review, subject-matter experts and the intelligence community can be engaged to provide additional understanding and contextual information regarding the threat. More education programs in biodefense for scientists, the public policy workforce, public health professionals, and agricultural and food scientists are needed to build and maintain a knowledgeable and comprehensive workforce for all biosecurity programs.

## REFERENCES


1. *Concerns Renewed about Russia's Bio Weapons Program*. CBW Chronicle, 1998.
2. Weiner T. (1998). *Soviet Defector Warns of Biological Weapons*. New York times, New York, NY.
3. Dalton, R. (2001). Genetic sleuths rush to identify anthrax strains in mail attacks. *Nature* **413**(6857), 657–658.
4. Majidi V. (2008). *Science Briefing on the Anthrax Investigation*. Federal Bureau of Investigation, Washington, DC.
5. Franco, C. and Deitch, S. (2007). Billions for biodefense: federal agency biodefense funding, FY2007-FY2008. *Biosecur. Bioterror*. **5**(2), 117–133.
6. Dando, M. R. and Rappert, B. (2005). *Codes of Conduct for the Life Sciences: Some Insights from UK Academia: Department of Peace Studies*. University of Bradford, Bradford, UK.
7. Davidson, E. M., Frothingham, R., and Cook-Deegan, R. (2007). Science and security: practical experiences in dual-use review. *Science* **316**(5830), 1432–1433.
8. Harris E. (2006). Controlling Dangerous Pathogens Project. *Regional Workshop on Dual-Use Research: Meeting Report*. Teresopolis, Brazil.
9. Harris E. (2006). Controlling dangerous pathogens project. *Regional Workshop on Dual-Use Research: Meeting Report*. Matrahaza, Hungary.
10. McLeish, C. and Nightingale, P. (2005). *The BTWC Regime: The Impact of Dual Use Controls on UK Science*. Department of Peace Studies, University of Bradford, Bradford, UK.
11. Revill, J. and Dando, M. R. (2008). Life scientists and the need for a culture of responsibility: after education, what? *Sci. Public Policy*. **35**(1), 29–35.
12. (a) Partnership for Public Service (2003). Homeland insecurity: building the expertise to defend America from bioterrorism. *Biosecur. Bioterror*. **1**(3), 223–224; (b) Homeland Insecurity; Building the Expertise to Defend America from Bioterrorism: Partnership for Public Service; Washington, DC.
13. Gursky E. (2005). Epidemic proportions: building national public health capabilities to meet national security threats. In *Senate HELP Committee*, Washington, DC.
14. Cello, J., Paul, A. V., and Wimmer, E. (2002). Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template. *Science* **297**(5583), 1016–1018.
15. National Research Council (2004). *Biotechnology Research in an Age of Terrorism*. National Academies Press, Washington, DC.
16. Smith, H. O., Hutchison, C. A. III, Pfannkoch, C., and Venter, J. C. (2003). Generating a synthetic genome by whole genome assembly: phiX174 bacteriophage from synthetic oligonucleotides. *Proc. Natl. Acad. Sci. U.S.A.* **100**(26), 15440–15445.
17. Garfinkel M. S., Endy D., Epstein G., and Friedman R. (2007). *Working Papers for Synthetic Genomics: Risks and Benefits for Science and Society*, Washington, DC.

18. Bügl, H., Danner, J. P., Molinari, R. J., Mulligan, J. T., Park, H. O, Reichert, B., Roth, D. A., Wagner, R., Budowle, B., Scripp, R. M., Smith, J. A., Steele, S. J., Church, G., and Endy, D. (2007). DNA synthesis and biological security. *Nat. Biotechnol*. **25**(6), 627–629.
19. Gibson, D. G., Benders, G. A., Andrews-Pfannkoch, C., Denisova, E. A., Baden-Tillson, H., Zaveri, J., Stockwell, T. B., Brownley, A., Thomas, D. W., Algire, M. A., Merryman, C., Young, L., Noskov, V. N., Glass, J. I., Venter, J. C., Hutchison, C. A. III, Smith, H. O. (2008). Complete chemical synthesis, assembly, and cloning of a *Mycoplasma genitalium* genome. *Science* **319**(5867), 1215–1220.
20. Vogel, K. M. (2008). Framing biosecurity: an alternative to the biotech revolution model?. *Sci. Public Policy*. **35**(1), 45–54.

# HEALTH RISK ASSESSMENT FOR RADIOLOGICAL, CHEMICAL, AND BIOLOGICAL ATTACKS*

ELLEN RABER AND ROBERT D. KIRVEL
*Lawrence Livermore National Laboratory, Livermore, California*

## 1 INTRODUCTION

A working definition of "risk" in the context of human health and intentional contamination events is the probability of adverse effects resulting from exposure to an environmental agent or a mixture of agents [1]. An "agent" has been defined [2] as a chemical, physical, mineralogical, or biological entity that may cause deleterious effects in an organism after exposure to it. Risk assessment can be generally regarded as either a scientific discipline or a professional process that involves the quantitative or qualitative estimation of potentially adverse health effects arising from exposure to hazards, such

as the agents identified above. This principle and its importance regarding human health exposure are supported by guidance recently issued by the Office of Management and Budget (OMB) and the Executive Office of the President [3].

Rather than being a stand-alone process, risk assessment is usually viewed as one component of a broader process known as "risk analysis", which includes risk assessment, risk management, and risk communication [4]. Risk management is a decision-making process that accounts for political, social, economic, and engineering implications together with risk-related information to develop, analyze, and compare management options and select the appropriate managerial response to a potential chronic health hazard. Risk communication is a field in the area of environmental health through which a communicator hopes to provide the receiver with information about the expected type and magnitude of an outcome. Risk communication is typically a discussion about an adverse outcome and the probability of that outcome occurring [5]. Various aspects of risk management are discussed in more detail in other articles of this *Handbook*.

Risk assessment has a long history—often linked to Federal governmental policies—that has sometimes been characterized as "controversial" [4, p. 86; 6, p. 17]. Many different definitions of risk assessment and its current limitations can be found in the recent literature (see [6], pp. 16–17 for several examples). In a human health context, risk assessment is the evaluation of scientific information on (i) the hazardous properties of environmental agents (hazard identification or hazard characterization), (ii) the extent of human exposure to these agents (exposure assessment), and (iii) the dose–response relation (dose–response assessment). The product of a risk assessment is risk characterization, a statement integrating information from items (i) through (iii) above, to estimate the probability and degree to which exposed populations of individuals will be harmed [1].

For drinking water, the history of risk assessment got its start within the regulatory community in the 1970s with the *Safe Drinking Water Act* (reauthorized in 1996; National Primary Drinking Water Regulations, 40 CFR Part 141); for air, with the *Clean Air Act* (42 USC 7401 et seq.). To better estimate the potential hazards involved, the National Research Council (NRC) initiated studies that culminated in what is commonly known as the Red Book [7] wherein risk assessment was officially recognized as a field. Although one of the recommendations in the Red Book was that risk assessments for cancer and noncancer effects follow uniform guidelines, such assessments have generally followed different approaches [4, p. 87].

## 2 RISK-INFORMED DECISION MAKING APPLIED TO REMEDIATION AND RESTORATION

To evaluate potential residual health effects for a particular radiological, chemical, or biological agent following intentional contamination—whether to water, air, or environmental surfaces—some type of health risk assessment as previously described would be necessary. A risk-based approach means that cleanup guidelines should be based on a defined, "acceptable" or "tolerable" level of risk to health. Many factors would have to be considered in developing standards and realistic cleanup goals to protect health, property, and resources. The following considerations are among the most important.

First, it is necessary to determine whether a risk actually exists or is perceived to exist. An actual risk depends on the presence of at least three elements: a hazard as previously

discussed, a receptor (human or ecological), and a pathway (physical or environmental migration route) that connects the two. If any one of the three elements is absent, then by definition, no actual risk exists. If a risk does exist, then determining the timing and potential severity of an incident must be made. Interrelated considerations are the type of release scenario and site descriptions; contaminant migration and longevity; projected water, land, resource, or property use; and any use restrictions.

Cleanup and decontamination decisions must then be made with input from stakeholders representing both public and regulatory concerns. Relevant risk-informed decision-making considerations include the following:

- Potential acute and long-term chronic health impacts, including health effects on key populations such as pregnant women or immunocompromised individuals.
- Damage to water, land, property, and equipment as a function of cost.
- Detectability of the agent(s) in the contaminated medium and the long-term fate of contaminant(s) or degradation product(s).
- Cost of decontamination or other remediation options.
- Time constraints associated with decontamination or other remediation options.
- Availability of decontamination methods and methods for the associated sampling, analysis, and verification of decontamination.
- Aesthetic considerations.
- Other site-specific factors that might be relevant.
- Potential overreaction that may cause more panic or chaos than warranted.

An important factor underlying each risk-based decision is the uncertainty and reliability of available data. Uncertainties in the magnitude and location of residual agents, site-specific features, and prediction of natural attenuation or potential dilution effects, all contribute to decisions about whether appropriate decontamination levels have been reached. In most cases, some type of statistically valid sampling could be used to reduce uncertainty both during site characterization and regarding the likelihood that an appropriate decision has been made. The sampling strategy would take into account the way any decontaminant reagents or treatments, if used, are applied, as well as spatial or volumetric considerations regarding the contaminated site.

A recommended, limited health risk assessment approach begins with a multimedia, multipathway dose assessment. For example, the possible resuspension or transport and fate of a substance or microorganism must be determined. This means that the ability of a contaminant to move into, off of, or through contaminated materials must be determined or assumed. Consideration must be given to the mobility of a contaminant under both unusual conditions, such as fires or floods, and mundane ones, such as repainting a building. The toxicology of the agent must be evaluated; and the human morbidity, mortality, and latency of effects must be determined, if known. Integrating multimedia transport and fate with multipathway exposure (e.g. inhalation, ingestion, or dermal absorption) and physiologically based pharmacokinetics (if available) for modeling toxicity should yield an estimate of noncarcinogenic hazard and carcinogenic risk, especially from short-term exposures. If possible, an empirical biomarker or biodosimetric procedure should be identified so that those given permission to reoccupy a building or structure, or allowed to resume using a drinking-water source, can be monitored.

An alternative and commonly accepted approach is to study contaminated versus uncontaminated environments. Elevated concentrations of an agent can then be used as an index for evaluating relative contamination levels and to determine whether decontamination treatment should be repeated. For example, to evaluate coliform or *Cryptosporidium* contamination in a drinking-water source, where such microbes are indigenous at very low levels, one could measure the relative concentration in intentionally contaminated water sources versus adjacent sources not deliberately contaminated to ascertain whether decontamination should be implemented or repeated. Acceptable levels should be somewhere between background and the lowest dose for infection.

Researchers at Lawrence Livermore National Laboratory have developed a conceptual decision process for chemical and biological decontamination following a terrorist attack [8, 9]. The details of this preliminary decision framework are beyond the scope of this article. However, an important point is that the eight major decision areas defined in the framework are derived from risk-based decision making. The steps that should be followed include evaluation of the timing and severity of impact of an incident; whether specific site conditions pose unacceptable risk to health, ecosystems, or property and thereby warrant decontamination; and a definition of decontamination goals, including cleanup concentration and target time frame to achieve the goals. The framework includes key decision points for regulatory and stakeholder review. Stakeholder involvement is critical whether the risk is actual or perceived. Any perceived risk, and potential community outrage associated with the perceived risk related to an intentional contamination incident, would need to be addressed carefully. Such a risk-informed decision framework needs to be considered when applying the information provided in this article to an actual, intentional contamination event.

## 3 HAZARDS AND EXPOSURES FOR RADIOLOGICAL, CHEMICAL, AND BIOLOGICAL AGENTS

Early during any response and recovery effort following intentional contamination, it is essential to identify the agent(s) used in the attack; specific characteristics of the prepared agent and its ability to cause harm; to the extent possible, the amount of contaminant initially present (source term); mechanism of release; and the extent of spread at a contaminated site. The site-specific nature of the area and its initial or planned usage are also key to understanding the actual potential hazard(s). Such information, which pertains to the hazard posed by the agent(s), is key in defining the level of remediation and restoration that may be required. If an identified contaminant in water or air were known to dissipate quickly through degradation or natural attenuation, then simply waiting might be all that is required to reduce the health hazard. If an agent were persistent however, knowing the amount present and other details on its specific properties—such as its ability to aerosolize or reaerosolize, stay in solution, or quickly degrade to nontoxic by-products—along with environmental parameters and conditions, would help to define the type and level of remediation actually necessary.

When evaluating the potential hazards associated with water resources, one must consider the potential for contamination of both surface water and groundwater from soil contamination. The potential for contaminant transport in soils has been extensively studied, and key geochemical and hydrogeological characteristics have the ability to influence the spread of source contamination from any event [10]. The same characteristics in both

soil and water have the potential to provide conditions favorable for natural attenuation for some of the agents of concern [11]. It is important to consider such characteristics during an overall risk assessment because they may play an important role in risk-informed decision making and in determining whether actual remediation is needed.

Hazard identification involves specifying not only the agent involved but also the range of clinical outcomes in humans, which can vary from asymptomatic conditions to death. Hospitalization studies, case studies, epidemiological data, and the clinical literature are all important sources of information. The World Health Organization has outlined the format and types of information that should be included in a hazard characterization of pathogens and how the identified factors affect the likelihood of disease [12, Appendix A, p. 51]. Although the outline was developed for a food matrix, it can with slight modification be applied to water as well. Table 1 captures the principal WHO recommendations pertinent to characterizing the hazard. The words highlighted in italics modify the WHO outline and apply it more broadly to the topic being discussed in this article.

With respect to the hazards posed by biological agents, current scientific data suggest that a single microorganism (such as a single spore of *Bacillus anthracis*) could cause harm in a particular subgroup of the human population [13, 14]. Such a position, which is by no means new, is known as the single-organism hypothesis [15] or the independent-action theory [16, p. 96]. In their assessment of risks arising from exposure to microorganisms, the NRC [6] stated, " ... it has frequently been asserted that there exists a threshold (minimum infectious dose) below which there is no risk to a population. Such a concept in not consistent with the current understanding of microbial risk assessment .... [p 110]" The NRC concluded that " ... it is not possible to calculate a threshold for environmental contamination with *B. anthracis* spores (or other pathogens or toxins) below which there would be zero risk of disease." [p 112] This conclusion has important implications for dose–response assessment.

Added to the hazard issue of virulence of agents such as *B. anthracis* is the fact that spores of the genus *Bacillus* can survive in a dormant state for decades and probably much longer [17, 18]. With regard to water contamination, ingestion and cutaneous exposure pathways would represent the key exposure pathway(s) of concern. Microorganisms can potentially multiply; conversely, they might be killed by acidity in the gastrointestinal tract or through action of the immune system, and the susceptibility varies greatly in humans. Another hazard-related consideration for certain microbes is their transmissibility and the potential secondary spread of disease from one person to another, which is of enormous concern for *variola major* virus, the causative agent of the disease smallpox. This article does not specifically address the potential threat from genetically modified or engineered organisms.

In contrast to the key biological agents of concern, chemical or radiological exposures are concentration-dependent and require a certain level of exposure for illness to occur. Person-to-person transmissibility is of minimal or no concern for chemicals or radioisotopes. Unlike radiation exposures that occur daily from natural sources (e.g. cosmic radiation), humans are not normally exposed to the chemical and biological agents that have been identified by the Centers for Disease Control and Prevention (CDC) as most likely to be used in an intentional contamination event. Many of the chemical warfare agents (CWAs) are man made and do not occur naturally in the environment. Although many of the biological warfare agents actually do occur in the environment, exposure to them is much more infrequent than that to radiation. The likelihood of exposure to

**TABLE 1 Outline of the Types of Information to Include in a Hazard Characterization**

| Principal Information Required | Components Under Each Topic |
|---|---|
| Describe the pathogen or *agent* or *chemical or* host, and matrix factors and how they affect disease or *chronic* outcome(*s*) | Characteristics of the pathogen or agent, such as<br>Infectivity, virulence, or pathogenicity<br>Genetic factors (such as resistance)<br>*Type of ionizing radiation*<br>*Environmental stability (persistence)*<br>*Toxicity*<br>*Absorption or adsorption*<br>*Exposure pathways*<br>Characteristics of the host *(exposed population)*, such as<br>Immunity status<br>Age, sex, and ethnic group<br>Health behaviors<br>Physiological status<br>Genetic and environmental factors<br>Characteristics of the matrix *or environment*, such as<br>pH or *redox potential*<br>Any processing that might stress a microbial Population<br>*Porosity, permeability*<br>*Potential for UV exposure or oxidation* |
| Public health outcomes | Manifestations of disease *or potential for acute or chronic outcomes* for end points modeled |
| Dose–response relation | Summary of available data<br>Illness, given exposure<br>Sequelae given illness<br>Secondary and tertiary transmission<br>Death, given illness<br>Dose–response model<br>Sources of data used<br>Assumptions<br>Models<br>Goodness of fit to the distribution<br>Uncertainty and variability in estimates |
| Validation and peer review | — |
| References | — |

biological and chemical agents as a result of an intentional contamination event would be a function of the proximity to the source location and the exposure pathways.

Exposure to a contaminant involves contact at a boundary between a human and the environment with a contaminant of a specific concentration for a specified time [19, p. 90]. Thus, exposures in the risk assessment process have been defined (specifically for chemical risk assessment) as an average lifetime daily dose (concentration × contact rate × duration/body weight × lifetime [4, p. 88]. In the case of *Superfund*, 30 years of exposure was used as the reasonable maximum exposure; the *Clean Air Act* uses

70 years for a maximally exposed individual. But regardless of how the "average" is defined by any particular legislative statute, exposure assessments estimate the dose encountered, and dose is the amount deposited or absorbed in the body over time. However, even with good concentration data, variability in actual exposures, sensitivity, and susceptibility in a heterogeneous population make estimates of risk associated with certain agents, especially biological ones, inherently uncertain [6, p. 90]. The US Environmental Protection Agency (EPA)'s *Exposure Factors Handbook* [20, see http://www.epa.gov/ncea/pdfs/efh] is a valuable resource for information on the broad range of exposure-related factors that must be considered in quantitative risk assessment. The steps described in the EPA *Handbook* for performing an exposure assessment are as follows:

1. Determine the pathways of exposure.
2. Identify the environmental media that transport the contaminant.
3. Determine contaminant concentration.
4. Determine exposure time, frequency, and duration.
5. Identify the exposed population.

By their nature, the hazards posed by radiological agents are different from those posed by biological or chemical agents. Although some radiological agents can also be chemically toxic to humans, it is the actual radiation damage that must be evaluated for its longer-term impacts to human health. Radionuclide sources emit three principal types of potentially harmful ionizing radiation: $\alpha$ and $\beta$ particles with low and medium penetration, respectively, and $\gamma$ rays with high penetration ability [21, 22]. To give some general sense of what "penetration" means in the context of ionizing radiation, $\alpha$ particles are shielded by paper or skin, $\beta$ particles by aluminum or wood, and $\gamma$ rays by concrete. Exposure from ingestion would be the most likely mode of transport from a contaminated water supply. Regulations and guidelines for radiological, chemical, and biological agents are discussed below in that order.

## 4 REGULATIONS AND GUIDELINES FOR RADIOLOGICAL AGENTS

For weapons of mass destruction, regulations and guidelines for what constitutes a "safe" or "acceptable" human dose are clearest for radiological agents, somewhat less clear for chemical agents, and least codified by far for biological agents. For that reason, radioisotopes are discussed first.

### 4.1 Radioisotopes of Concern

The International Atomic Energy Agency (IAEA) has identified $^{192}$iridium, $^{60}$cobalt, $^{137}$cesium, $^{90}$strontium, and $^{241}$americium as the top radioactive isotopes that are involved in illicit trafficking and pose a potential security threat [23]. Several of these radionuclides are generated by, or used in, research facilities; some are used in the medical, food processing, and well logging industries; and others result from nuclear power generation. Table 2 lists the five radioisotopes of concern to the IAEA along with other relevant information. In this table, the radioactivity level associated with each radioisotope, expressed in curies (a common quantity measurement term), is also shown. A curie is the quantity of a radionuclide that has $3.7 \times 10^{10}$ disintegrations per second.

**TABLE 2 Radioisotopes of Concern, Example Applications, and Typical Curie Content [23]**

| Radioisotope | Example Applications and Sources | Typical Radioactivity Level (Curies) |
|---|---|---|
| $^{241}$Americium | Well logging, smoke detectors, medicine, industrial gauging | 0.027–22 |
| $^{137}$Cesium | Teletherapy | 13,500 |
| $^{90}$Strontium | Radioisotope thermoelectric generators | 30,000–300,000 |
| $^{60}$Cobalt | Food irradiation | 2700–11,000,000 |
| $^{192}$Iridium | Industrial radiography | 3–250 |

In addition to those radioisotopes identified by the IAEA, other radioisotopes have also been identified as environmental health threats to the public from industrial processes. Although they are not discussed here in detail, some exposure guidelines specific to water are included. These other radioisotopes may well be used or considered for some terrorist scenarios.

Health risks associated with radioisotopes are relatively well understood. In general terms, health risk depends on the dose received, type of ionizing radiation involved, and the genetic makeup of an individual, among other factors. Higher doses have serious, acute health effects; lower accumulated doses have chronic health effects often expressed as one or another type of cancer; and very low doses have no observed health effects.

Two dose-measurement terms are common (see, e.g. http://www.osha.gov, accessed Sept. 6, 2007), where "dose" means the quantity of ionizing radiation absorbed, per unit of mass, by the body or by any portion of the body. The radiation absorbed dose (rad) is a measure of dose of any ionizing radiation to body tissues in terms of the amount of energy absorbed per unit of mass of the tissue. One rad is the dose corresponding to 100 ergs of energy per gram of tissue. As a rule of thumb, a dose of 1000 rad is fatal 100% of the time; a dose of 500 rad is fatal 50% of the time; and dose of 100 rad typically results in radiation sickness. Another dose-measurement term, the roentgen equivalent man (rem), is the amount of energy absorbed into a material multiplied by the quality factor. Applying the quality factor to absorbed dose provides a dose equivalent that reflects the biological risk associated with the radiation quality. To lend some perspective on what this measure means, the total annual dose equivalent that an individual typically receives from all natural sources (such as cosmic and terrestrial radiation, food, and consumer products) is estimated to be in the range of 360 mrem/year (1 mrem = 1/1000 rem). An accumulated dose of 25 rem results, on average, in 1% risk of developing cancer. The occupational exposure limit (whole body) is 5 rem/year [29 CFR Standard 1910.1096 (b)(1)—Ionizing Radiation]. In Order 5400.5, the Department of Energy (DOE) sets the primary dose limit at 100 mrem/year for a member of the general public (see [24]). The same dose limit is used in 10 CFR 835 for members of the general public entering a controlled area, the dose limit for minors, and the threshold requiring appropriate personnel dosimetry for general workers.

### 4.2 Exposure Guidelines for Radiological Agents

A regulatory structure separate from that for chemical (and more recently, biological) agents has evolved for response guidelines associated with radiological agents, primarily driven by the Nuclear Regulatory Commission (NRC), the EPA, and the DOE. The

cleanup and final release of an area or resource that is contaminated with a radiological agent is carried out under the guiding principle of limiting the dose to the general public. The NRC, EPA, and DOE have historically approached the criteria differently: the NRC and DOE use a dose-based approach, whereas the EPA uses a risk-based approach. As a result, the EPA and NRC have different cleanup standards.

The EPA has developed updated Protective Action Guides (PAGs) intended to help state and local authorities make radiation-protection decisions during the various phases of an emergency [25]. During the early phases of response (first hours to days, corresponding to the notification and first-response phases of an incident), the PAG is to consider evacuation if the projected dose exceeds 1 rem in 4 days. During the intermediate phase (days to months after an attack, corresponding to the remediation or cleanup phase of an incident), the PAG is to relocate a population if the projected dose during the first year exceeds 2 rem and to use dose-reduction techniques if the dose is less than 2 rem. During the recovery phase (months to years after an attack), the PAG involves no set dose limits; rather, the Department of Homeland Security (DHS) along with other Federal agencies and state and local governments set the final release criteria.

Meeting a specific clearance goal can have a large impact on the total cost of remediation or cleanup following a contamination event. The EPA considers radionuclides to be carcinogens and, from a risk-based approach, requires that cleanup or clearance levels achieve a standard that places the risk of developing cancer between 1 in 1000 and 1 in 1,000,000. The result is usually a more conservative cleanup level than that mandated by the NRC.

No uniform set of cleanup standards for radionuclides exists at present. However, the DHS is in the process of issuing PAGs specifically designed to address response operations [26]. The proposed PAGs outline the projected dose of radiation to an individual, from an accidental or deliberate release of radioactive material, at which a specific protective action to reduce or avoid such a dose of radiation is recommended. The PAGs are based on four criteria: (i) to prevent acute health effects, (ii) to reduce the risk of chronic effects; (iii) to balance protection with other important factors that affect the public welfare; and (iv) to ensure that the actions taken result in more benefit than harm. Representatives from eight Federal agencies developed and approved the proposed guidance. The DHS posted its proposed guidelines in the *Federal Register*, and the public and interested stakeholders were invited to submit comments.

In the absence of uniform Federal guidelines to protect the public, emergency responders, and the surrounding environment from the effects of radiation, acceptable exposure and associated cleanup levels for water as well as other media would likely be derived from existing laws and regulations. The DHS is expected to play a key role in determining acceptable levels for final clearance of items. As per the American National Standards Institute [27], the consensus for item clearance criteria (a voluntary standard) is currently 1 mrem/year (or 10 $\mu$Sv/year) total effective dose equivalent (TEDE) above background. The stated purpose of the standard is "to provide guidance for protecting the public and the environment from radiation exposure by specifying a primary radiation dose criterion and derived screening levels for the clearance of items (which may include water-contaminated areas) that could contain radioactive material". Because Federal agencies are to use voluntary industry standards developed by the private sector when possible, this ANSI standard should play a large role in the regulatory process [28].

The guidance for concentrations of various radioactive isotopes in groundwater and drinking water is specified under several different regulations [29]. Because of the importance of groundwater as a source of drinking water for so many communities and individuals, the EPA has been designated as the responsible entity for Federal activities relating to the quality of drinking water to include groundwater and other surface water-supply resources [30]. Some of the Federal laws enacted to protect groundwater include the *Safe Drinking Water Act*, the *Resource Conservation and Recovery Act*, the *Comprehensive Environmental Response, Compensation, and Liability Act* (CERCLA, also known as the *Superfund* law), the *Federal Insecticide, Fungicide, and Rodenticide Act*, the *Toxic Substance Control Act*, and the *Clean Water Act*. The EPA standards for groundwater and drinking water are shown in the upper tier of rows of Table 3. Because it is possible that radioactive isotopes other than the five specified by the IAEA [23] could be involved in an attack involving the intentional contamination of water, other radiological contaminants are identified in Table 3 when water guidelines for them are available. The Agency for Toxic Substances and Disease Registry (ATSDR) was established by Congress in 1980 under CERCLA to conduct public health assessments at each site on the EPA National Priorities List. For some radiological contaminants, the ATSDR specifies a "comparison value", which is a concentration or amount of substance in air, water, food, or soil that is, upon exposure, unlikely to cause adverse health effects. The values identified in Table 3 as "ATSDR estimates" [31] are such values for the maximum concentration of radionuclides in water based on the consumption of 2 liters per day for 1 year, a limit of 4 mrem/year, and Federal cancer risk coefficients for environmental exposure to radionuclides.

The *Safe Drinking Water Act* (1974, amended 1986, reauthorized in 1996) specifications provided in the middle rows of Table 3 represent national primary drinking-water standards. Maximum contaminant levels (MCLs) are the highest level of a contaminant or a naturally occurring mineral that is allowed in US domestic drinking water from distributed systems. The MCLs are enforceable EPA standards for water-treatment utilities [32]. The MCL values shown in this middle part of Table 3 reflect updates per the Radionuclides Rule (final rule for radionuclides in drinking water), published in the *Federal Register* on December 7, 2000 (65 FR 76708) [33, p. I-4]. The EPA guidance from the Office of Solid Waste and Emergency Response (OSWER) under Directive 9283.1-4 is shown in the bottom rows of Table 3.

## 5 REGULATIONS AND PROPOSED GUIDELINES FOR CHEMICAL AGENTS

### 5.1 Chemical Agents of Concern

Hazardous chemicals are classified by the CDC [34] into 13 categories, which include biotoxins, blister agents and vesicants, blood agents, caustics, choking agents, nerve agents, and others. Among the blister agents, sulfur mustard (NATO code H, or distilled mustard, NATO code HD; chemical formula $C_4H_8Cl_2S$) is widely recognized as a chemical warfare agent of concern in an intentional contamination event. Among the nerve agents, the G agents sarin (NATO code GB; chemical formula $C_4H_{10}FO_2P$), cyclosarin (NATO code GF; $C_7H_{14}FO_2P$), soman (NATO code GD; $C_7H_{16}FO_2P$), tabun (NATO code GA; $C_5H_{11}N_2O_2P$), and the V agent VX ($C_{11}H_{26}NO_2PS$) are Chemical Warfare

**TABLE 3 Guidance for Radionuclides in Groundwater and Drinking Water**

| Regulation or Standard | Regulated Radionuclide |
|---|---|
| USEPA standard for groundwater [31] | 15 pCi/L gross $\alpha$ (MCL) |
| | 50 pCi/L gross $\beta$ (MCL) |
| Or | 6 pCi/L plutonium 238 (ATSDR estimate) |
| ATSDR estimate for groundwater, where a "comparison value" is specified [31] | 6 pCi/L plutonium 239/240 (ATSDR estimate) |
| | 5 pCi/L radium 226 + radium 228 (MCL) |
| | 300 pCi/L radon 222 (proposed MCL) |
| | 21 pCi/L thorium 228 (no existing MCL; ATSDR estimate) |
| | 7 pCi/L thorium 222 (no existing MCL; ATSDR estimate) |
| | 20,000 pCi/L tritium (H-3) (MCL) |
| | 30 pCi/L uranium 233/234 (no existing MCL; ATSDR estimate) |
| | 32 pCi/L uranium 235/236 (no existing MCL; ATSDR estimate) |
| | 15 pCi/L uranium 238 (as an $\alpha$ emitter; see gross $\alpha$, above) |
| MCLs specified in the Safe Drinking Water Act (40 CFR Part 141) and modified per the Radionuclides Rule, published in the *Federal Register* on December 7, 2000 (65 FR 76708) | 4 mrem/year $\beta$ + photon emitters (MCL) |
| | 15 pCi/L gross $\alpha$ particle (MCL) |
| | 5 pCi/L combined radium 226 + radium 228 (MCL) |
| | 30 $\mu$g/l uranium (MCL) |
| | For other radionuclides, no MCL in drinking water is specified |
| Office of Solid Waste and Emergency Response (OSWER) Directive 9283.1-4 | Total concentration corresponding to a 4 mrem/year limit, i.e. |
| | 200 pCi/L $^{137}$Cs |
| | 100 pCi/L $^{60}$Co |
| | 8 Ci/L $^{90}$Sr |

Agents (CWAs) of concern. In addition, three toxic industrial chemicals are often identified as being of importance: two are the blood agents cyanogen chloride (CK; chemical formula CNCl) and hydrogen cyanide (AC; chemical formula HCN); and one is the choking agent, phosgene (CG; chemical formula $COCl_2$). Of these nine chemicals, the first six listed above are referred to collectively in the following discussion as CWAs, and the last three are referred to collectively as toxic industrial chemicals (TICs). The term "chemical agents" refers to all nine collectively.

## 5.2 Exposure Guidelines for Chemical Agents of Concern

For chemical agents, data from animal models are often relied on as the basis for dose–response or potency information. Unlike biological warfare agents, chemical agents have various quantified health-based guidelines that can be used as clearance goals.

Among the authorities and agencies that have published guidelines for chemical agents are the following:

- CDC of the US Department of Health and Human Services [35, 36].
- Committee on Toxicology of the National Research Council [37–39].
- American Conference of Governmental Industrial Hygienists [40].
- USEPA's Integrated Risk Information System [1, 41].
- American Industrial Hygiene Association [42].
- USEPA, Regions 9 and 3 [43–46].
- CDC National Institute for Occupational Safety and Health (NIOSH) and Occupational Safety and Health Administration (OSHA) [47].

Whereas site-, situation-, and population-specific factors must all be considered when selecting "acceptably safe" levels for chemical agents, various scientifically defensible levels have been applied as appropriate for some CWAs and TICs. Another important definition is the acute exposure guideline levels (AEGLs). AEGLs represent federally endorsed guidance criteria for the assessment and management of single-exposure emergency events, such as accidents or intentional terrorist attacks. AEGLs, published by the National Research Council Committee on Toxicology and developed in collaboration with the USEPA National Advisory Committee for AEGLs for Hazardous Substances [37–39], are threshold airborne concentrations of a chemical above which different health effects could begin to occur among members of the general public. Three levels, called AEGL-1, AEGL-2, and AEGL-3, for each of five exposure periods (10, 30 min; 1, 4, and 8 h) are distinguished by varying degrees of severity of toxic effects.

Table 4 shows an example of how certain airborne exposure guidelines might be applied following an intentional contamination scenario. If the maximum airborne concentration resulting from an event was lower than the general population limit (GPL), it is unlikely that drinking-water resources would be affected. The GPL is an atmospheric concentration level (milligram per cubic meter) below which no adverse effects would occur in the general population, including sensitive subpopulations, assuming a continuous, daily (24/7), chronic (lifetime) exposure [48–50].

The second column of Table 4 lists the NRC-endorsed AEGL-1 concentrations—the mildest-effect tier of AEGL values—for an 8-h exposure to the six CWAs. An AEGL-1 value is defined as the airborne concentration (in milligram per cubic meter) of a substance at or above which it is predicted that the general population, including "susceptible" but excluding "hypersusceptible" individuals, could experience notable discomfort after the specified time (8 h in this example). Airborne concentrations less than AEGL-1 represent exposure levels that could produce mild odor, taste, or other sensory irritations, but nothing more serious.

Depending on the specific type of contamination event that might occur involving chemical agents, soil or other types of sediment could be susceptible to contamination. Health-based environmental screening levels (HBESLs), which are calculated using EPA chronic risk assessment methods, represent the current guidelines for soil contamination. The levels shown in the two columns on the right side of Table 4 are low-level concentrations of individual CWAs in residential and industrial soil, which, if not exceeded, are unlikely to present a human health hazard for specific exposure scenarios [52]. The values are derived from the USEPA Region 3 Risk-Based Concentration (RBC) model [44] and are appropriate for use where cumulative effects are not anticipated. Several

**TABLE 4 General Population Limits, Airborne (Inhalation, Ocular) Exposure Guidelines (AEGL-1 Values), and Health-Based Environmental Screening Levels (HBESLs) for Selected CWAs in Residential and Industrial Soil**

| CWA | GPL (mg/m3) for Chronic (Lifetime) Exposure | AEGL-1[a] Protective Estimate ($mg/m^3$) 8-h Exposure | HBESL for Residential Soil (mg/kg) | HBESL for Industrial Soil (mg/kg) |
|---|---|---|---|---|
| Tabun (GA) | $1 \times 10^{-6}$[b] | 0.0010[c] | 3.1 | 82 |
| Sarin (GB) | $1 \times 10^{-6}$[b] | 0.0010[c] | 1.6 | 41 |
| Soman (GD) and Cyclosarin (GF) | $1 \times 10^{-6}$[d] | 0.00050[c] | 0.31 | 8.2 |
| VX | $6 \times 10^{-7}$[b] | 0.000071[c] | 0.047 | 1.2 |
| Sulfur mustard (H/HD) | $2 \times 10^{-5}$[e] | 0.008[c] | 0.55 | 14 |

[a]NRC/COT [38].
[b]DHHS [35].
[c]NRC/COT [39].
[d]Department of the Army [51].
[e]DHHS [36].

assumptions underlie these values. One is that the exposure pathway is ingestion but not inhalation or dermal contact with contaminated soil. In addition, the values do not account for potential runoff or groundwater contamination, and that risk to ecological receptors is not evaluated. If groundwater were a concern, then cleanup levels would need to be re-evaluated on the basis of depth to groundwater and other parameters [53]. Hydrogeological conditions and potential contaminant transport through soils are clearly important parameters in understanding potential risk and for optimizing remediation actions.

In terms of the topic of central concern in this article, both the EPA and the military use the MCL as enforceable guidelines for CWAs in drinking water. MCLs are the highest level of a contaminant or naturally occurring mineral that is allowed in US domestic drinking water from distributed systems. MCLs are enforceable EPA standards for water-treatment utilities [32]. Table 5 lists suggested groundwater and surface water guidelines, to the extent they are specified, for the six CWAs and three TICs identified earlier as being of concern in an intentional contamination event. Furthermore, it is possible that certain chemical agents could absorb on or into certain porous media, such as concrete or porous plastics, and potentially present a continued source of exposure particularly in scenarios where liquid aerosol droplets are released. Thus Table 5 also identifies chronic reference doses (previously published RfDs or estimated $RfD_{est}$) that could be applied to meet waste-disposal requirements and landfill agreements with state and Federal agencies and help them determine that an agent is not present at levels of concern.

## 6 REGULATIONS AND GUIDELINES FOR BIOLOGICAL AGENTS

### 6.1 Biological Agents of Concern

The CDC has prioritized biological agents that pose the greatest threats to civilians for the purpose of public health preparedness activities [60]. In June 1999, a meeting of national

**TABLE 5 Drinking Water and Ingestion Guidelines for Chemical Agents**

| Agent Type and Name | Published Water Guideline | Reference Dose (RfD or $RfD_{est}$) (mg/kg/day)Ingestion: Estimate of Daily Exposure Level for General Population; Chronic Exposure Duration (7 years to Lifetime) |
|---|---|---|
| **Nerve Agents** | | |
| Tabun (GA) | Field drinking-water standard MCL[a] = 12 $\mu$g/l | $4 \times 10^{-5}$[b] |
| Sarin (GB) | Field drinking-water standard MCL[a] = 12 $\mu$g/l | $2 \times 10^{-5}$[b] |
| Soman (GD) and Cyclosarin (GF) | Field drinking-water standard MCL[a] = 12 $\mu$g/l | $4 \times 10^{-6}$[b] |
| VX | Field drinking-water standard MCL[a] = 12 $\mu$g/l | $6 \times 10^{-7}$[b] |
| **Blister Agent** | | |
| Sulfur mustard (H, HD) | Field drinking-water standard MCL[a] = 140 $\mu$g/l | $7 \times 10^{-6}$[b] |
| **Choking Agent** | | |
| Phosgene (CG) | Reactive and volatile; water guideline not applicable | Not available[c] |
| **Blood Agents** | | |
| Hydrogen cyanide (AC) | Drinking water MCL[d] = 0.2mg/l (specified by EPA for cyanide) | 0.02[e] |
| Cyanogen chloride (CK) | Regulatory status: no officially proposed primary standard[f] | 0.03 and 0.05[g] |

[a]Maximum allowable concentration in water by the combined US Forces for consumption at 5 l/day, not to exceed 7 days, as cited in Hauschild, V. USACHPPM, Table 2. Chemical agent multimedia/toxicity standards and guidelines summary table (March, 2006); available at <usachppm.apgea.army.mil/chemicalagent/PDFFiles/CWA-mediaTableMarch_2006.pdf>, accessed September 11, 2007.

[b]Opresko et al. [54] Values for nerve and sulfur mustard agents are RfD estimates ($RfD_{est}$) considered scientifically valid by the National Research Council [55, 56], but they have not been reviewed by IRIS. The value for GF is also an estimate ($RfD_{est}$) and has not been reviewed by IRIS.

[c]Not available per USEPA Integrated Risk Information System (IRIS; http://www.epa.gov/iris/subst). Phosgene RfD was under discussion as of January 31, 2006. No change in this determination as of October 31, 2006.

[d]USEPA [57].

[e]USEPA [46].

[f]USEPA [58].

[g]Opresko et al. [59]. The value of 0.03 mg/kg-day for cyanogen chloride is an estimate ($RfD_{est}$) and has not been reviewed by IRIS. USEPA Region 9 (2004), Region 9 Preliminary Remediation Goals 2004 Table. The RfD of 0.05 mg/kg/day for cyanogen chloride is from http://www.epa.gov/region09/waste/sfund/prg/index.html, accessed March 2, 2006.

experts was convened to review selection criteria. Criteria included public health impacts, delivery potential, public perception related to civil disruption, and special public health preparedness needs. Final assignments of agents into three categories (A, B, or C) were based on overall ratings in those four areas. The results are as follows:

- *Category A biological agents* are those that pose the greatest potential for adverse impact and have the highest priority for preparedness. They are *Variola major, B. anthracis*, *Yersinia pestis*, *Clostridium botulinum*, *Francisella tularensis*, Filoviruses, and Arenaviruses.
- *Category B biological agents* have a high threat potential, but less impact than that of Category A agents. They are *Coxiella burnetii, Brucell* spp., *Burkholderia pseudomallei*, Alphaviruses (VEE, EEE WEE), *Rickettsia prowazekii*, certain toxins (including ricin and *Staphylococcal enterotoxin B*), *Chlamydia psittaci*, certain food-safety threats (such as *Salmonella* spp. and *Escherichia coli* O157:H7, and certain water-safety threats (such as *Vibrio cholerae* and *Cryptosporidium parvum*).
- *Category C biological agents* are emerging threats. Examples include Nipah virus and Hantavirus.

### 6.2 Exposure Guidelines for Biological Agents of Concern

The dose–response concept has been used since at least the 1950s, and it is widely applied in industrial hygiene applications [6, p. 107]. A dose–response curve is a graph showing the quantitative relation between administered, applied, or internal exposure (dose) of an agent and specific, biologically significant changes in incidence, or degree of change, to that agent (i.e. response, such as infection, illness, or death) [modified after [1]]. Dose–response assessments differ considerably for microorganisms and chemicals agents.

Dose–response modeling has been used extensively to posit the risk associated with ingestion of organisms [61–65]. Although dose–response models have not been published for Category A biological agents in humans (ethics prohibit their use in human studies), other data are available from which to infer doses and responses for those agents (see Table 6). Mathematical models have been advocated to assist in dose–response modeling, especially for extrapolation to low doses, and such models have been used for decades in toxicology [12]. The use of animal models for extrapolating health effects to humans, and the type of mathematical model used to extrapolate from high doses to low are two of the methods in risk assessment that have been associated with controversy [4]. The two most successful of the family of mechanistic models are the exponential model and the beta-Poisson model, which vary principally in the way they treat survival probabilities. Both models assume that a single organism is sufficient to initiate infectious disease in some individuals, and that the probability of any ingested organism will survive to colonize is independent among all organisms inhaled or ingested. This modeling approach and conclusion was also reaffirmed by the 2005 National Academy of Sciences Study, which reviewed cleanup levels for biological agents following a potential indoor airport attack [6].

Whereas nearly all biological warfare agents are intended for aerosol application, many “have strong potential as waterborne threats” and could inflict heavy casualties when ingested [66, p. 975]. Perhaps most pertinent to the focus of this article is that scientific investigations have led to recommended guidelines in drinking water (Table 6)

**TABLE 6 Dose–Response Information (Published Data or Inferred) and NPDWR Drinking-Water Guidelines for Microbes Identified as Category A or B Agents by the CDC [60] and of Medical Importance in Water Per Haas et al. [4] or a "Water Threat" According to Burrows and Renner [66] or the USEPA [32]**

| Biological Agent | Dose–Response Available?[1] | Dose–Response Source[1] | Water Guideline Available?[2] |
|---|---|---|---|
| **Bacteria** | | | |
| *Bacillus anthracis*[2] | Yes | [67] | None identified |
| *Salmonella*[1] | Yes | [68–70] | No MCL identified. *Salmonella* is on the list of agents for which the EPA is developing the Groundwater Disinfection (GWD) Rule[3] |
| *Shigella*[1] | Yes | [62] | No MCL identified. *Shigella* is on the list of agents for which the EPA is developing the Groundwater Disinfection (GWD) Rule[3] |
| Enteropathic *E coli*[1] | Yes | [4] | Yes (for total coliform). MCL |
| *E. coli* O157:H7[1] | Yes in animals | [71] | violation if more than 5% of samples are total coliform positive in 1 month. Heterotrophic plate count $\leq$500 CFU/ml[3] |
| *Vibrio cholerae*[1] | Yes | [4] | No MCL identified |
| *Campylobacter*[1] | Yes | [65] | No MCL identified. *Campylobacter* is on the list of agents for which the EPA is developing the Groundwater Disinfection (GWD) Rule[3] |
| *Francisella tularensis*[1] | Yes in animals | [72] | No MCL identified |
| **Viruses** | | | |
| Adenovirus[1] | Yes | [4] | MCLs have only been specified for |
| Coxsackievirus[1] | Yes | [4] | viruses considered to be "enteric." |
| Echoviruses[3] | Yes | [4] | Recommendation is for 99.99% removal or inactivation of enteric viruses |
| | | | Adenovirus, Coxsackievirus, and Echoviruses are on the Contaminant Candidate List, but MCLs are not yet established by the EPA[2] |
| Ebola | Yes, in animals | [73] | No MCL. Ebola transmission in water is "not known" [66] |
| *Variola major*[2] | Yes | [74] | No MCL. Smallpox (from *Variola major*) is identified as a "possible" water threat [66] |
| **Protozoans** | | | |
| *Giardia lamblia* (cysts)[1] | Yes | [75] | Yes. 99.9% removal or inactivation. (Not identified by CDC as Category A, B, or C.) |
| *Cryptosporidium* (oocysts)[1] | Yes | [64]; [76]; [77] | Yes. 99% removal as of 1/1/2002 for systems serving >10,000; 99% removal as of 1/14/2005 for systems serving <10,000 |

for only some of the biological warfare agents that have been identified by the CDC [60] as priority microbes and by Haas et al. [4] or others [66] as microbes of medical importance in water. For many other biological agents, no water guidelines have been established.

Even though the US National Primary Drinking Water Regulations (NPDWRs) are enforceable and must be health protective [78], some have argued that in light of new epidemiological evidence, water-quality guidelines for pathogenic microorganisms have not kept pace with microbiological risk assessments, and that a new framework linking assessment of risks with health targets and outcomes should be used to converge on what constitutes a "tolerable risk" of infection from water [13]. However, the issue of exactly what constitutes an acceptable risk is a complex matter. The importance of education should not be underestimated when considering what risk the public is willing to accept. For example, the public accepts hospital disinfectant methods even though such methods do not guarantee zero risk. Similarly, public swimming pools are required to meet defined treatment standards that are also accepted by the public, yet there have been instances in which children have died from exposure to and ingestion of *E. coli* from public swimming pools. Examples of public health standards for swimming pools are as follows:

- Combined available chlorine $<0.2$ mg/l, and pH from 7.2 to 8.0 [79].
- 1.5 ppm free chlorine and pH from 7.2 to 8.0 (22 CCR §65529).
- Total coliform bacteria of less than 2.2 MPN (most probably number or median) per 100 ml (22 CCR §65531).
- Total coliform level using the membrane filter (MF) procedure not to exceed 2 colony forming units (CFU) per 100 ml of sample tested [79].
- Heterotrophic plate count not to exceed 200 CFU per 100 ml in 85% of samples tested [80].

Individual states have their own regulations regarding drinking water based on their stakeholders and this must be taken into account when trying to determine and/or develop guidelines related to an unnatural event. As an example, the California Code of Regulations (22 CCR, Division 4, Article 20, Article 3) specifies that a public water system is in violation of the total coliform MCL when any of the following occurs:

- For a system collecting more than 40 samples/month, more than 5% of the samples collected during any month are total coliform positive; or
- For a public water system that collects fewer than 40 samples/month, more than one sample collected during any month is total coliform positive; or
- Any repeat sample is fecal coliform positive or *E. coli* positive; or
- Any repeat sample, following a fecal coliform positive or *E. coli*-positive routine sample, is total coliform positive.

A summary of the various health factors involved in assessing microbial risks associated with drinking water can be found in Haas et al. [4], Tables 3–5 [p 101]; a summary of exposure factors in such an assessment can be found in Haas et al. [4], Tables 3–6 [p 102]. Exposure factors include transmission routes, environmental sources of microbes, their survival potential, their regrowth potential, their occurrence in raw water supplies, resistance to treatment, environmental transport, and the availability of methods for assessing

source water and treated water, among others. A variety of methods are used to isolate and identify microbes from environmental samples [81], such as those identified in *Standard Methods for the Examination of Water and Wastewater* [82]. The problem is that quantitative and statistically evaluated databases and improved models, rather than nonquantitative presence versus absence reports, are needed to assess the reduction of microbial populations through treatment and process controls. This major gap in risk assessment associated with drinking water-treatment efficacy in the United States has been clearly recognized by several experts publishing on the topic [e.g. [16]].

The challenges associated with setting an "acceptable cleanup level" leading to clearance following a biological attack are discussed in many reports [see e.g. [53, 83, 84]]. Almost all researchers writing on the topic agree that there is currently insufficient information to develop an "infectious dose" and to quantify a "safe" amount of residual biological agent in a decontaminated facility or outdoor environment [4, 6, 14, 15, 85, 86]. There exists even less information regarding safe levels for water-related resources. Currently, there are no risk-based developed guidelines for biological warfare agents that are equivalent to the AEGLs endorsed for chemical agents or the PAGs that have been developed for radiological agents.

However, after the anthrax letter attacks in the United States in 2001 and the unprecedented remediations that followed these attacks, many experts concurred that the clearance goal (acceptable level of residual contamination), at least for a *B. anthracis*-contaminated facility (indoors), should be no growth of spores on all postremediation environmental samples [see e.g. [6, 87]]. Therefore, it is anticipated that in the event of an actual biological attack on water supplies or resources, a similar type of conservative clearance goal may need to be implemented.

An issue closely associated with decontamination and clearance following any biological attack—and one that illustrates the complex nature of potential problems that can arise from remediation efforts—is the possibility that certain decontamination reagents used to address biological contamination might themselves become problematic during a cleanup operation. Some investigators have suggested that decontamination with powerful chemicals to decrease the exposure to a given microbial pathogen could result in increased exposure to those chemical contaminants used, particularly in drinking water [78]. The concern thus is health risk arising from the treatment (decontamination) process rather than the microbes per se, especially if high levels of treatment were applied over a wide area, and if the by-products of treatment were disposed as untreated wastewater and found their way into drinking-water supplies. The balancing of chemical risks associated with disinfection, potential cancer risks arising from disinfection by-products that might be formed, and the risks from biological agents themselves in water that the management option of treatment is invoked to address is "a worldwide issue in drinking water and cannot be solved without appropriate risk assessment" [16, p. 100.]. Clearly, risk trade-offs must be considered as part of the decision-making process whereby decontaminant chemicals and treatment methods are selected and applied to minimize microbial risks, but approaches to strictly limit or prevent secondary contamination of water systems should be incorporated into remediation planning. Account must be taken during remediation planning of all regulations applicable to potential waste streams that could be generated. Depending on their destination, wastewater from decontamination technologies is regulated by *Clean Water Act* pretreatment requirements specified in 33 USCA 1317, 40 CFR 403, state regulations regarding pretreatment, and any local publicly owned treatment works (POTW) pretreatment requirements.

## 7 CRITICAL NEEDS AND FUTURE DIRECTIONS

As is apparent from the literature surveyed in this article, meeting the critical needs of homeland security and counterterrorism in the area of risk assessment will be challenging. The complexities associated with evaluating human health hazards, exposures, responses, and risks, although well documented, are numerous. However, several key areas continue to represent technical gaps in addressing the issue of risk for radiological, chemical, and biological contaminants. Additional study and research in the following areas are needed to better minimize the potential human health consequences associated with radiological, chemical, and biological contamination resulting from terrorist attacks.

1. A risk assessment approach should be incorporated as a required component of decision making for ascertaining the adequacy of decontamination processes or treatments, if used, following the release of a contaminant. This need—largely in the context of indoor, surface decontamination—was acknowledged by the NRC [6, pp. 5–6]. In particular, microbial risk assessment models and tools are lacking. More generally, a scenario-specific risk assessment approach is needed to understand appropriate cleanup levels and potential residual health effects regardless of the media that are contaminated (water, air, or environmental surfaces). Key site-specific parameters and the relations among them in a given scenario must be carefully defined. They include the sources and extent of contamination, applicable receptors, and potential environmental and physical pathways between them [8].
2. Essential experimental data needed to support quantitative risk assessment are lacking for biological warfare agents in the area of dose–response relations. This need was acknowledged by the NRC [6, p. 4]. In addition, chronic low-dose exposure data needed for better risk assessments are lacking for CWAs. To develop dose–response information and better assess the human risk of exposure to biological agents, targeted research should be directed toward ways to extrapolate dose–response data between species. Use of animal and human tissues, and of *in vitro* techniques, may become increasingly important [6, p. 118]. Available dose–response data for pathogens of concern should be analyzed by nonthreshold dose–response models [6, p. 117].
3. Consensus with regard to protective estimates that can serve as clearance goals (standards) for the general public are especially needed for both water resources and soil (in terms of the potential to impact groundwater and other water resources from surface runoff) that have been contaminated with radiological, chemical, or biological agents. Such standards will require a consensus among subject-matter experts, regulatory authorities, and local, state, and Federal health agencies. With respect to drinking-water contamination and cleanup in particular, clearly defined, health-based clearance goals or national standards are lacking for some radiological isotopes of concern, certain chemical agents, and nearly all biological warfare agents that are viewed as potential threats to water.

   A national committee of experts including representatives from regulatory agencies—the EPA and CDC in particular—should be appointed to work on developing consensus-based clearance goals (standards) for the radiological, chemical, and biological agents ascertained to be of concern in the event of a terrorist attack and for which such standards are currently lacking. Review of, and comment on, proposed standards should be solicited in the *Federal Register*.

For example, no official primary drinking-water standard exists for at least one chemical agent of concern, and MCLs are generally lacking for biological warfare agents. Efforts should be made to fill these and other gaps. The experts who develop the standards must consider not only scientifically based information but also public perceptions about what is safe. Appropriate risk communication techniques, including explanations of scientific terminology and methods, should be used when making recommendations based on scientific criteria. The risk communication techniques that have been recently used in association with the demilitarization of the US chemical weapons stockpiles may provide a useful framework on which to build.

4. Additional risk-based evaluations should be performed, and explicit guidelines developed, to avoid the secondary contamination of water and wastewater systems by the application of potentially hazardous decontamination reagents, their by-products, or the degradation products of CWAs or hazardous TICs.
5. Since reauthorization of the *Safe Drinking Water Act* in 1996, there has been renewed interest in emerging microorganisms that pose increased risk to the safety of drinking-water supplies [88]. However, current methods used to monitor environmental samples, particularly biological agents in water, do not always provide the necessary levels of sensitivity that are required to ascertain the efficacy of treatment processes [16].

   To address the problem of inadequate sensitivity of some methods used to monitor environmental samples, particularly biological agents in water [16], researchers need to assemble a larger database on the inactivation or removal of microorganisms via various treatment processes, such as disinfection and filtration. Improved quantitative, statistically evaluated databases for adequate risk assessments will be useful in estimating concentrations of microbes in treated water.
6. A better understanding of natural decontamination or natural attenuation with regard to biological and chemical agents of interest is needed. Few studies have assessed the survivability of biological agents in water under various environmental conditions. Little information exists on the degradation kinetics for CWAs as a function of time under different geochemical conditions. Such factors have a major impact on risk assessment and long-term public health risks.

## ACKNOWLEDGMENT

This work was performed under the auspices of the US Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

## REFERENCES

1. USEPA/IRIS. U.S. Environmental Protection Agency, Integrated Risk Information System (2006a). *Integrated Risk Information System (IRIS) Glossary*, available at http://www.epa.gov/iris/gloss8.htm, accessed August 24, 2006.
2. USEPA. U.S. Environmental Protection Agency (2002). *Health Effects Notebook, Health Effects Glossary*, available at http://www.epa.gov/ttnatw01/hlthef/hapsec1.html.

3. Dudley, S. E. (2007). Updated principles for risk analysis. Memorandum for the heads of executive departments and agencies (M-07-24). In *Executive Office of the President, Office of Management and Budget*, S. L. Hays, Ed. Office of Science and Technology Policy, Washington, DC.
4. Haas, C. N., Rose, J. B., and Gerba, C. P. (1999). *Quantitative Microbial Risk Assessment*, John Wiley & Sons, Inc., New York, p. 449.
5. Reynolds, B. (2002). *Crisis and Emergency Risk Communication*. Centers for Disease Control and Prevention; available at http://www.maxwell.af.mil/au/awc/awcgate/cdc/cerc_book.pdf.
6. NRC. National Research Council of the National Academies (2005). *Reopening Public Facilities After a Biological Attack: A Decision Making Framework*, The National Academies Press, Washington, DC, p. 210.
7. NAS. National Academy of Sciences (1983). *Risk Assessment in the Federal Government: Managing the Process*, National Academy Press, Washington, DC.
8. Raber, E., Hirabayashi, J., Mancieri, S., Jin, A., Folks, K., and Rice, D. (1999). *Conceptual Bio-decontamination Decision Process Following a Terrorist Attack*, Lawrence Livermore National Laboratory, Livermore, CA, UCRL–AR-131181, Rev. 1.
9. Raber, E., Hirabayashi, J., Mancieri, S., Jin, A., Folks, K., Carlsen, T., and Estacio, P. (2002). Chemical and biological agent incident response and decision process for civilian and public sector facilities. *Risk Anal.* **22**(2), 195–202.
10. Yong, R. N., Mohamed, A. M. O., and Warkentin, B. P. (1992). Principles of contaminant transport in soils. In *Developments in Geotechnical Engineering*, Elsevier, Netherlands, Vol. **73**.
11. NRC. National Research Council of the National Academies (2000). *Natural Attenuation for Groundwater Remediation*, The National Academies Press, Washington, DC.
12. WHO (2003). *Hazard Characterization for Pathogens in Food and Water. Guidelines*, *Microbial Risk Assessment Series. No. 3*, World Health Organization, Food and Agriculture Organization of the United Nations, New York.
13. Bartram, J., Fewtrell, L., and Stenstrom, T. A., Eds. (2001). Harmonised assessment of risk and risk management for water-related infectious disease: an overview. In *Water Quality Section, in Guidelines, Standards and Health: Assessment of Risk and Risk Management for Water-related Infectious Disease*, L. Fewtrell, and J. Bartram, Eds. World Health Organization and IWA Publishing, London, pp. 1–16.
14. Peters, C. J., and Hartley, D. M. (2002). Anthrax inhalation and lethal human infection. *Lancet* **359**, 710–711.
15. Rubin, L. G. (1987). Bacterial colonization and infection resulting from multiplication of a single organism. *Rev. Infect. Dis.* **9**(1), 488–493.
16. Haas, C. N., Rose, J. B., and Gerba, C. P. (1999). *Quantitative Microbial Risk Assessment*. John Wiley & Sons, Inc. New York, p. 96.
17. Sneath, P. H. A. (1962). Longevity of microorganisms. *Nature* **195**, 643–646.
18. Pepper, I. L., and Gentry, T. J. (2002). Incidence of *Bacillus anthracis* in soil. *Soil Sci.* **167**, 627–635.
19. NRC. National Research Council of the National Academies (1999). *Research Priorities for Airborne Particulate Matter: II. Evaluating Research Progress and Updating the Portfolio*, The National Academies Press, Washington, DC.
20. USEPA. U.S. Environmental Protection Agency (1997). *Exposures Factors Handbook*, Office of Research and Development, Washington, DC. EPA/600/P-95/002Fa, p. 1193.
21. USEPA. U.S. Environmental Protection Agency (2002a). *What is Radiation?* Available at http://www.epa.gov/radiation/students/what.html, accessed September 7, 2004.
22. USEPA. U.S. Environmental Protection Agency (2002b). *Types of Radiation*, Available at http://www.epa.gov/radiation/students/types.html, accessed September 7, 2004.

23. IAEA. International atomic energy agency (2003). *Categorization of Radiation Sources*, July 10, IAEA-TECDOC-1344.
24. DOE. U.S. Department of Energy. (1993). *Radiation Protection of the Public and the Environment*, DOE Order 5400.5, Change 2. Available at http://www.explorer.doe.gov:1776/.
25. USEPA. U.S. Environmental Protection Agency (2007a). *Protective Action Guides*, Available at: http://www.epa.gov/radiation/rert/pags.htm, last updated July 23; accessed September 7, 2007.
26. DHS. Department of Homeland Security (2006). *Fact Sheet: Proposed Protective Action Guides for Radiological Dispersion and Improvised Nuclear Devices*, January 3. Available at http://www.dhs.gov/xnews/releases/press_release_0827.shtm, accessed September 7, 2007.
27. ANSI. American National Standards Institute (1999). *Surface and Volume Radioactivity Standards for Clearance. An American National Standard*, ANSI/HPS N13.12-1999. Health Physics Society, McLean, VA.
28. Stansbury, P. S., and Strom, D. J. (2001). *Uses of ANSI/HPS N13.12-1999 "Surface and Volume Radioactivity Standards for Clearance" and Comparison with Existing Standards*. April. Pacific Northwest National Laboratory, Richland, Washington, DC. PNNL-13484, p. 36.
29. Elcock, D., Klemic, G. A., and Taboas, A. L. (2004). Establishing remediation levels in response to a radiological dispersal event (or "dirty bomb"). *Environ. Sci. Technol.* **38**(9), 2505–2512.
30. USEPA. U.S. Environmental Protection Agency, Office of Water (1990). *Citizen's Guide to Ground-water Protection*, April. EPA 440/6-90-004.
31. DHHS. U.S. Department of Health and Human Services, Agency for Toxic Substances and Disease Registry (2004a). *Public health assessment for Lawrence Livermore National Laboratory*. June 29, available from National Technical Information Services, Springfield VA.
32. USEPA. U.S. Environmental Protection Agency (2007b). *Drinking Water Contaminants, National Primary Drinking Water Regulations. List of Drinking Water Contaminants and their MCLs*. Available at http://www.epa.gov/safewater/mcl.html, accessed September 6.
33. USEPA. U.S. Environmental Protection Agency, Office of Ground Water and Drinking Water (2002c). *Implementation guidance for radionuclides*, March. EPA 816-F-00-002.
34. CDC. Centers for Disease Control and Prevention (2003). *Emergency Preparedness and Response*, Chemical Categories (webpage last modified December 3; accessed September 7, 2007). Available at: http://www.bt.cdc.gov/agent/agentlistchem-category.asp.
35. DHHS. U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (2003). Final recommendations for protecting human health from potential adverse effects of exposure to agents GA (tabun), GB (sarin), and VX. *Fed. Regist.* **68**, 58348–58351.
36. DHHS. U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (2004b). Interim recommendations for airborne exposure limits for chemical warfare agents H and HD (sulfur mustard). *Fed. Regist.* **69**(85), 24164–24168.
37. NRC/COT. National Research Council, Committee on Toxicology (2001). *Subcommittee on Acute Exposure Guideline Levels. Standing operating procedures for developing acute exposure guideline levels for hazardous chemicals*, National Academy Press, Washington, DC.
38. NRC/COT. National Research Council, Committee on Toxicology (2002). Subcommittee on acute exposure guideline levels. Phosgene (Appendix 1, pp. 15–70), and Hydrogen cyanide (Appendix 5, pp. 211–276). In *Acute Exposure Guideline Levels for Selected Airborne Chemicals*, National Academies Press, Washington, DC, Vol. **2**.
39. NRC/COT. National Research Council, Committee on Toxicology (2003). Subcommittee on acute exposure guideline levels. Nerve agents (Appendix 1, pp. 15–300), and Sulfur mustard (Appendix 2, pp. 301–383). In *Acute Exposure Guideline Levels for Selected Airborne Chemicals*, National Academies Press, Washington, DC, Vol. **3**.

40. ACGIH. American Conference of Governmental Industrial Hygienists (2003). *TLVs and BEIs, Based on the Documentation of the Threshold Limit Values for Chemical Substances and Physical Agents and Biological Exposure Indices*, (Cyanogen Chloride, p. 24; Hydrogen Cyanide, p. 35; Phosgene, p. 47). ACGIH, Cincinnati, OH.
41. USEPA/IRIS. U.S. Environmental Protection Agency, Integrated Risk Information System (2006b). Phosgene (CASRN 75-44-5); available at http://www.epa.gov/iris/index.html.
42. AIHA. American Industrial Hygiene Association (2004). *Emergency Response Planning Guidelines and Workplace Environmental Exposure Level Guides (cyanogen chloride, p. 22; hydrogen cyanide, p. 23; phosgene, p. 23)*, 2700~Prosperity Avenue, Suite 250, Fairfax, VA.
43. USEPA. U.S. Environmental Protection Agency (1991). *Risk Assessment Guidance for Superfund, Vol.~1, Human Health Evaluation Manual. Part B, Development of Risk-based Preliminary Remediation Goals*, Publication 9285.7-01B, Office of Emergency and Remedial Response, Washington, DC, NTIS PB92-96333.
44. USEPA. U.S. Environmental Protection Agency (1996a). *EPA Region III Risk-based Concentration Table, Background Information, Development of Risk-based Concentrations*, Office of Superfund Programs, Philadelphia, PA.
45. USEPA. U.S. Environmental Protection Agency (1996b). *Soil Screening Guidance: Technical Background Document*, EPA/540/R-95/128, Office of Emergency and Remedial Response, Washington, DC, pp. PB96–963502.
46. USEPA, US Environmental Protection Agency. Integrated risk information system (IRIS) (2005). available electronically at www.epa.gov/iris.
47. NIOSH/OSHA. National Institute for Occupational Safety and Health, and Occupational Safety and Health Administration (2006). *OSHA/NIOSH Interim Guidance, Chemical-biological-radiological-nuclear (CBRN), Personal Protective Equipment Selection Matrix for First Responders*; available at: http://www.osha.gov/SLTC/emergencypreparedness/cbrnmatrix/index.html.
48. Mioduszewski, R. J., Reutter, S. A., Miller, L. L., Olajos, E. J., and Thomson, S. A. (1998). *Evaluation of Airborne Exposure Limits for G-agents: Occupational and General Population Exposure Criteria*, Edgewood Research, Development, and Engineering Center, Aberdeen Proving Ground, MD. ERDEC-TR-489.
49. DHHS. U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (1988). Final recommendations for protecting the health and safety against potential adverse effects of long-term exposure to low doses of agents GA, GB, VX, mustard agent (H, HD, T), and lewisite (L). *Fed. Regist.* **53**, 8504–8507.
50. DHHS. U.S. Department of Health and Human Services, Centers for Disease Control and Prevention (2002). Airborne exposure limits for chemical warfare agents GA (tabun), GB (sarin), and VX. *Fed. Regist.* **67**(5), 894–901.
51. Department of the Army Office of the Surgeon General Memorandum (2004). *Nerve Agent Percutaneous Exposure Criteria and Airborne Exposure Levels (AELs) for GD/GF for Use in Interim DA Guidance on Implementation of the New AELs*, 5109 Leesburg Pike, Falls Church, VA. 29 June.
52. U.S. Army Center for Health Promotion and Preventive Medicine and Oak Ridge National Laboratory (1999). *Derivation of Health-based Environmental Screening Levels for Chemical Warfare Agents. A Technical Evaluation*, Aberdeen Proving Ground, MD.
53. Raber, E., Jin, A., Noonan, K., McGuire, R., and Kirvel, R. K. (2001). Decontamination issues for chemical and biological warfare agents: how clean is clean enough? *Int. J. Environ. Health Res.* **11**, 128–148.
54. Opresko, D. M., Young, R. A., Watson, A. P., Faust, R. A., Talmage, S. S., Ross, R. H., Davidson, K. A., King, J., and Hauschild, V. (2001). Chemical warfare agents: current status of oral reference doses. *Rev. Environ. Contam. Toxicol*. **172**, 65–85.

55. NRC/COT. National Research Council, Committee on Toxicology (1999). *Review of the U.S. Army's Health Risk Assessment for Oral Exposure to Six Chemical Warfare Agents*, COT Subcommittee on Chronic Reference Dose for Chemical Warfare Agents, Committee on Toxicology, National Academy Press, Washington, DC.

56. Bakshi, K. S., Pang, S. N. J., and Snyder, R. (Eds.) (2000). Review of the Army's Health Risk Assessments for Oral Exposure to Six Chemical Warfare Agents, *J. Toxicol. Environ. Health (Part A)*. **59**, 281–526.

57. USEPA (2006). Technical fact sheet on: cyanide (part of National Primary Drinking Water Regulations), available at http://www.epa.gov/safewater/dwh/t-ioc/cyanide.html, last updated November 28; accessed September 11, 2007

58. USEPA (1999). Class V underground injection control study: App. D: maximum contaminant levels and health advisory levels, available at http://www.epa.gov/safewater /uic/classv/pdfs/appd.pdf, October 10, accessed September 11, 2007.

59. Opresko, D., Young, R., Faust, R., Talmage, S., Watson, A., Ross, R., Davidson, K., and King, J. (1998). Chemical warfare agents: estimating oral reference doses. *Rev. Environ. Contam. Toxicol*. **156**, 1–183.

60. Rotz, L. D., Khan, A. S., Lillibridge, S. R., Ostroff, S. M., and Hughes, J. M. (2002). Public health assessment of potential biological terrorism agents. *Emerg. Infect. Dis.* **8**(2), 225–230.

61. Cassin, M. H., Lammerding, A. M., Todd, E. C. D., Ross, W., and McColl, R. S. (1998). Quantitative risk assessment for *Escherichia coli* O157:H7 in ground beef hamburgers. *Int. J. Food Microbiol.* **41**, 21–44.

62. Crockett, C. S., Haas, C. N., Fazil, A., Rose, J. B., and Gerba, C. P. (1996). Prevalence of shigellosis in the U.S.: consistency with dose–response information. *Int. J. Food Microbiol.* **30**(1–2), 87–100.

63. Gale, P., Young, C., and Oakes, D. (1998). A review: development of risk assessment for BSE in the aquatic environment. *J. Appl. Microbiol.* **84**(4), 467–477.

64. Haas, C. N., Crockett, C. S., Rose, J. B., Gerba, C. P., and Fazil, A. (1996). Infectivity of *Cryptosporidium parvum* oocysts. *J. Am. Water Works Assoc.* **88**(9), 131–136.

65. Medema, G. J., Teunis, P. F. M., Havelaar, A. H., and Haas, C. N. (1996). Assessment of the dose–response relationship of *Campylobacter jejuni*. *Int. J. Exp. Pathol.* **30**(1-2), 101–112.

66. Burrows, W. D., and Renner, S. E. (1999). Biological warfare agents as threats to potable water. *Environ. Health Perspect.* **107**(12), 975–984.

67. Haas, C. N. (2002). On the risk of mortality to primates exposed to anthrax spores. *Risk Anal.* **22**(2), 189–193.

68. Fazil, A. M. (1996). *A Quantitative Risk-assessment Model for Salmonella*, Environmental Studies Institute, Drexel University, Philadelphia, PA.

69. Holcomb, D. L., Smith, M. A., Ware, G. O., Hung, Y. C., Brackett, R. E., and Doyle, M. P. (1999). Comparison of six dose–response models for use with food-borne pathogens. *Risk Anal.* **19**(6), 1091–1100.

70. Havelaar, A. H., and Garssen, J. (2000). *Dose Response Relationships for Gastrointestinal Pathogens in an Animal Model*, Bilthoven, NL, RIVM. Available from The National Academies Press at http://books.nap.edu.openbook.php?record_id=11324&page=119.

71. Haas, C. N., Thayyar-Madabusi, A., Rose, J. B., and Gerba, C. P. (2000). Development of a dose–response relationship for Escherichia coli O157:H7. *Int. J. Food Microbiol.* **56**(2–3), 153–159.

72. Oyston, P. C. F., Sjostad, A., and Titball, R. W. (2004). Tularemia: bioterrorism defense renews interest in *Franciscella tularensis*. *Nat. Rev. Microbiol.* **2**, 967–978.

73. Johnson, E., Jaax, N., White, J., and Jahrling, P. (1995). Lethal experimental infections of rhesus monkeys by aerosolized ebola virus. *Int. J. Exp. Pathol.* **76**, 227–236.

74. Wehrle, P. F., Posch, J. J., Richter, K. H., and Henderson, D. A. (1970). An airborne outbreak of smallpox in a German hospital and its significance with respect to other recent outbreaks. *Bull. WHO* **43**, 2230–2251.

75. Rose, J. B., Haas, C. N., and Regli, S. (1991). Risk assessment and the control of waterborne giardiasis. *Am. J. Public Health* **81**, 709–713.

76. Messner, M. J., Chappell, C. L., and Okhuysen, P. C. (2001). Risk assessment for *Cryptosporidium*: a hierarchical Bayesian analysis of human dose–response data. *Water Res.* **35**(16), 3934–3940.

77. Teunis, P. F. M., Chappell, C. L., and Okhuysen, P. C. (2002). *Cryptosporidium* dose response studies: variation between hosts. *Risk Anal.* **22**(3), 475–485.

78. Macler, B. A., and Regli, S. (1993). Use of microbial risk assessment in setting United States drinking water standards. *Int. J. Food Microbiol.* **18**(4), 245–256.

79. U.S. Army (1993). *Occupational and Environmental; Health Swimming Pools and Bathing Facilities*, Technical bulletin TB MED575.

80. USEPA. U.S. Environmental Protection Agency (1979). *Swimming Pool Water Disinfectants*, DIS/TTS-12/Apr.23, Efficacy data requirements. available at http://www.epa.gov/oppad001/dis_tss_docs/dis-12.htm, accessed September 26, 2007.

81. Hurst, C. J., Knudsen, G. R., McInerney, M. J., Stetzenbach, L. D., Walter, M. V., Eds. (1997). *Manual of Environmental Microbiology*, ASM Press, Washington DC.

82. American Public Health Association, American Water Works association, and the Water Environmental Federation (1992). In A. E. Greenberg, L. S. Clesceri, and A. D. Eaton, Eds. *Standards Methods for the Examination of Water and Wastewater*, 18th ed. APHA, AWWA, and WEF, Baltimore MD.

83. Presidential/Congressional Commission on Risk Assessment and Risk Management (1997). *Final Report, Volume 1, Framework for Environmental Health Risk Management, and Volume 2, Risk Assessment and Risk Management in Regulatory Decision-making*, Presidential/ Congressional Commission on Risk Assessment and Risk Management, Washington, DC. Available at: http://www.riskworld.com/Nreports/nr7me001.htm, accessed August 1, 2007.

84. Government Accounting Office (2003). Report GAO-03-787T, May 19.

85. Johnson, B. (2003). OSHA infectious dose white paper. *Appl. Biosafety* **8**(4), 160–165.

86. Raber, E., Carlsen, T., Folks, K., Kirvel, R., Daniels, J., and Bogen, K. (2004). How clean is clean enough? recent developments in response to threats posed by chemical and biological warfare agents. *Int. J. Environ. Health Res.* **14**(1), 31–41.

87. Canter, D. A. (2005). Addressing residual risk issues at anthrax cleanups: how clean is safe? *J. Toxicol. Environ. Health, Part A* **68**, 1017–1032.

88. MacKenzie, W. R., Hoxie, N. J., Proctor, M. E., Gradus, S., Blair, K. A., Peterson, D. E., Kazmierczak, J. J., Fox, K., Addiss, D. G., Rose, J. B., and Davis, J. P. (1994). Massive waterborne outbreak of *Cryptosporidium* infection associated with a filtered public water supply, Milwaukee, Wisconsin, March and April, 1993. *N. Engl. J.* **331**(3), 161–167.

# TRANSPORTATION SECURITY

# ROLES AND IMPLICATIONS OF TRANSPORTATION SYSTEMS IN HOMELAND SECURITY

David Ekern
*Virginia Department of Transportation, Richmond, Virginia*
Joe Crossett
*High Street Consulting Group, Pittsburgh, Pennsylvania*

## 1 INTRODUCTION

In the United States, state Departments of Transportation (DOTs), working with agencies at the local and federal governmental levels, have responsibility for planning, delivering, operating, and maintaining a vast surface transportation network that includes not only four million miles of roads serving local, regional, and national travel needs [1], but also many rail lines, bus and rail transit systems, ferries, ports, and waterways. The emergency preparedness capabilities that public-sector transportation agencies are acquiring are critical to safe and efficient operation of the nation's transportation network in the twenty-first century.

Surface transportation is uniquely positioned among critical infrastructures and key resources in terms of its management by agencies with broad policy responsibility, public accountability, large and distributed workforces, heavy equipment, communications infrastructure, and ability to directly and swiftly take action (akin to the private sector). This institutional heft and continuous programmatic investment provide a stable base for a campaign to systematically reduce risk exposure over time through hazards capital budgeting.

Whether moving by car, truck, bus, train, ferry, bicycle, or on foot, Americans depend on surface transportation for safe and predictable mobility. On trips through town or across the country, vehicles drive an estimated eight billion miles on roads in the United States every day [1] and a considerable share of daily travel is associated with moving the estimated 89% of all freight by value that is shipped on highways [2].

The apparent scale and redundancy of the nation's transportation network gives a false sense of security, but in many parts of the country that network is straining to keep

up with the transportation demands of society and the economy. A single unexpected interruption in one location may have a dramatic ripple effect on travel across a wide region.

In August 2007, for example, the collapse of Minnesota's busiest bridge (I-35W) that carried 140,000 vehicles a day over the Mississippi River between downtown Minneapolis and its northern suburbs, not only caused tragic loss of life, but is also expected to have an economic impact of about $60 million in road user detour costs incurred before it is fully replaced [3] at an expected cost of at least $393 million. The US Department of Transportation estimates that there are at least 1000 bridges across the country where substantial casualties and economic disruption would result from isolated terrorist attacks [4].

Homeland security is one among many threats to safe and efficient operation of the nation's transportation network. An act of terrorism at a busy bottleneck or malevolent destruction of a major bridge would almost certainly cause unacceptable loss of life and temporary disruption of economic stability and necessitates costly infrastructure repairs. Historically, a range of threats, such as floods, earthquakes, extreme weather, wildfires, or major traffic incidents, have all proven capable of generating similarly adverse outcomes.

As travel grows with economic prosperity, lower density land use, and more mobile populations, incidents of any kind pose greater potential to disrupt the transportation network. Transportation agencies have no choice but to enhance their emergency preparedness capabilities to ensure that they can meet five fundamental responsibilities [5]:

1. prevent incidents within their control and responsibility;
2. protect transportation users, agency personnel, and critical infrastructure;
3. support regional, state, and local emergency responders with resources, including facilities, equipment, and personnel;
4. recover swiftly from incidents; and
5. evaluate response(s) and continually improve plans, training, skills, and protocols.

Meeting these responsibilities requires the engagement of skilled employees in a transportation agency, leadership by senior executives, and critical targeted investment in technology, people, and infrastructure.

Fortunately, transportation agencies can build from a strong foundation as they enhance their emergency preparedness capabilities. This is because, successful prevention, protection, response, and recovery from terrorist attacks depend on many of the same technologies, staff skills, and organizational structures needed to handle other hazards. As a consequence, many transportation agencies, including over 90% of state DOTs, have in place all-hazards emergency preparedness plans that enable them to respond to serious incidents regardless of their cause [6].

No two transportation agencies share exactly the same characteristics and one-size-fits-all fixes are not the solution for stronger homeland security, but some common themes are emerging that merit further scrutiny. These include organizational elements and planning approaches that are critical to developing effective all-hazards emergency preparedness capabilities and building the roles that transportation agencies are expected to perform in preventing, preparing for, responding to, and recovering from serious incidents.

## 2 ORGANIZATIONAL ELEMENTS OF PREPAREDNESS

A transportation agency's organizational structure is the framework that allows it to establish successful all-hazards emergency preparedness capabilities. The agency must be willing to blend new all-hazards functions with traditional organizational elements. Transportation agencies with strong all-hazards emergency management programs exhibit the following organizational elements [7].

### 2.1 A High Level All-Hazards Manager

State DOTs are recognizing that all-hazards preparedness cannot be achieved without a full-time, senior-level manager who is the agency's focal point for building and maintaining its all-hazards management capabilities. Many all-hazards preparedness activities involve sharing ideas among traditional transportation disciplines, such as traffic operations, maintenance, engineering, and construction, so the all-hazards manager in a transportation agency must have a broad understanding of many disciplines, from traffic operations and highway maintenance to information technology or bridge and tunnel design. The all-hazards emergency manager must be in close communication with executive staff so that critical issues before, during, and after incidents can be quickly raised to the highest levels, as needed. Many state DOTs have learned that colocation of all-hazards emergency management with their maintenance and operations functions makes sense because this is where the greatest overlap occurs among field staff awareness, emergency traffic operations, and other direct service activities. This becomes an even stronger function when colocation can be integrated with public safety agencies.

### 2.2 All-Hazards Leadership Team

The all-hazards manager should form and lead an interdisciplinary team that brings together key agency personnel from disciplines, such as maintenance, traffic operations, planning, design, and construction on a regular schedule. The functions of the team should include regular review of emergency incident reports, trends, program audit findings, and preparation of recommendations to senior management on changes in emergency preparedness plans and processes.

### 2.3 All-Hazards Technical Specialist Staff

Depending on factors, such as the size of the agency, existing staff capabilities, and criticality of risks, one or more additional staff are needed to support the all-hazards manager. Core focus areas of experienced specialist(s) include responsibility for training, exercises, evacuations, technology, and intelligence. In large state DOTs, the headquarters all-hazards and security team must have close links to districts that act for the DOT on the frontline during incidents. Each DOT district must have an experienced professional whose responsibilities include all-hazards emergency preparedness.

### 2.4 External Partnerships

Organizational exchange must be strengthened between transportation agencies and partners, such as emergency management agencies, the first responder community, law

enforcement, public health, and intelligence. An effective all-hazards manager must be active in a wide variety of state and federal networks for addressing emergency management issues. These connections promote sharing of ideas and information among disciplines and agencies, which can greatly enhance a DOT's all-hazards preparedness program.

## 3 ALL-HAZARDS EMERGENCY PREPAREDNESS PLANS

Transportation agencies' all-hazards emergency preparedness plans are vital to prevention, protection, response, and recovery from emergencies of all kinds. They enable every employee to understand their responsibilities; they help leadership hold staff accountable; and they allow the agency to work effectively with other organizations. Exemplary transportation agencies stand out because they have concentrated on integrating their plans into a single plan document. Their plans feature the following elements [7].

### 3.1 Consistency with National Emergency Planning Principles

The National Incident Management System (NIMS), Incident Command System (ICS), and National Response Framework (NRF) are initiatives headed up by the US Department of Homeland Security and they are the standard for emergency management planning. Many transportation agencies have built their emergency preparedness plans around NIMS, ICS, and the NRF.

### 3.2 A Single Emergency Preparedness Plan

A transportation agency's emergency preparedness plan must be an overarching document that is adopted by senior leadership and is the day-to-day resource within the agency for describing all general incident management planning, emergency operations center activation, and command and control and communications architecture that are applicable to incidents.

### 3.3 Hazard Type Annexes

Hazard annexes can be attached to the primary emergency preparedness plan, which provide details about threat-specific roles and responsibilities for addressing specific hazards, such as terrorism, biochemical, nuclear, fire, tornado, earthquake, snowstorm, or flood emergencies. Likewise, an annex can be included for continuity of operations planning, which describes how the agency will continue to operate if a disaster impacts key infrastructure or critical assets.

### 3.4 Distribution and Regular Updating

Appropriate staff must have ready access to the latest version of the emergency preparedness plan. Furthermore, the plan and its annexes must be treated as a living document that is adapted as changes in the local operating environment and global situation dictate.

The cycle for conducting a comprehensive update of the plan could be as frequent as once a year, but should certainly occur at least once every two years.

## 4 INCIDENT PREVENTION CAPABILITIES

Terrorist attacks differ from natural and accidental disasters because they are intentionally perpetrated acts that could possibly be prevented or deterred. The heightened threat of terrorism has led transportation agencies to pay much closer attention to countermeasures for preventing malevolent attacks against assets.

State and federal transportation agencies are working together with researchers to use seismically safe technologies and knowledge to enhance the blast resilience of their transportation structures. Blasts, such as those caused by a truck bomb parked near a bridge for example, have very similar structural effects to those that take place in an earthquake. Some of the tools and techniques developed over the past 25 years to make structures seismically safe may be used to make structures more resistant to terrorist attacks. These include use of redundant structural systems that are designed to reduce the risk of catastrophic collapse by transferring loads supported by lost or damaged columns to columns still intact, and structural dampers that are designed to absorb and reduce damaging vibrations.

The cost of installing countermeasures for even a handful of transportation infrastructure assets is high. Much of the transportation system is characterized by features, such as physical robustness, system redundancy, and limited potential for mass casualties that make it a relatively unappealing terrorist target. By contrast, specific transportation facilities, such as those that span large natural barriers, such as rivers, bays, or mountains, and serve unique regional or national transportation and economic roles, may be attractive targets. Key transportation agency prevention capabilities should include the following elements.

### 4.1 Risk Management

Risk assessment or vulnerability assessment involves considering the probability of an event and its likely consequences on people and assets. Transportation agencies are constantly refining risk management techniques to identify and protect high risk assets, such as multitier bridges, overpasses that traverse navigable waters, flammable pipeline crossings, tunnels, heavily congested truck routes, and roadways adjacent to other targets. Armed with accurate information about risks, transportation agencies can identify and implement cost-effective countermeasures to reduce risks to transportation assets, including risks from natural disasters and from sources of intentional harm such as terrorism.

### 4.2 Deterrence and Detection Improvements

Transportation agencies are putting in place a variety of deterrent and detection measures for better protecting critical facilities and assets. These measures work by creating a greater likelihood that potential aggressors will be caught and may even be deterred from

attacking an asset. The effectiveness of deterrence varies with the aggressor's sophistication, the asset's attractiveness, and the aggressor's objective.

Measures undertaken by transportation agencies include installation of fences to increase standoff distances from vulnerable structural components such as bridge piers or tunnel ventilation systems; secure access to structures; better lighting; electronic detection systems; elimination of parking areas beneath structures; security patrols and cameras; use of identification badges for employees and visitors; and background investigations on employees and contractors with access to critical information and facilities.

### 4.3 Infrastructure Hardening

As facilities are added or renovated on the transportation network and old structures are replaced or rehabilitated, transportation agencies must take advantage of opportunities to incorporate more advanced design features for critical infrastructure assets, which make them more resilient to attacks, such as location and design considerations, pier placement, and blast survivability.

### 4.4 Public Awareness Building

Transportation agencies are using communication tools, such as rest stop information centers, highway variable message signs, and congestion reporting websites to implement high visibility emergency awareness programs for the public, which emphasize the importance of vigilance and provide clear direction on reporting of suspicious activities.

### 4.5 Information Sharing

Transportation agencies must regularly participate in a variety of forums for sharing threat and intelligence information, including networks or arrangements with state and local emergency management, law enforcement, and homeland security officials. For example, transportation's large workforce of broadly distributed field staff can be trained and encouraged to report anomalies as part of their day-to-day responsibilities and to provide local intelligence input to fusion centers, which, in turn, may use the supplied intelligence to detect preoperational surveillance activities. To date, across the country tens of thousands of frontline transportation workers in all modes have been trained; this active network makes it harder for would-be attackers to conduct their preoperational surveillance.

### 4.6 Control of Sensitive Information

Transportation agencies must take steps to control access to documents that contain sensitive information about security critical systems and facilities. Steps include creation of an oversight committee for setting sensitive information policies; development of protocols to cover handling of access to documents, marking documents, storing documents, and requests for documents; establishment of a single point of contact for managing sensitive information; identification and protection of documents, such as vulnerability or risk assessments, emergency response plans, and other documents on security critical systems; and education of staff about sensitive information handling protocols.

## 5 INCIDENT PREPAREDNESS CAPABILITIES

Transportation agencies do not lead emergency preparedness, response, and recovery efforts, but they can and do play a vital support role to first responder, public safety, and law enforcement partners.

Since they do not have high visibility roles, transportation agencies are perceived by others as public works agencies with limited support capabilities. Public safety and emergency management agencies, meanwhile, may not understand how to assess an emergency situation in terms of its likely impacts on the transportation system. Technical resources—such as advanced surveillance systems possessed by state DOTs—are not well known to the public safety community, and are underutilized.

All-hazards preparedness means that transportation agencies are ready to work with emergency responders whenever an incident occurs. When incidents directly affect the transportation network, DOT field personnel must become first responder so preparedness is critical. Preparatory actions enable a transportation agency to anticipate and minimize the impacts of incidents via advance planning. Many preparatory actions are relevant regardless of threat or hazard type. Key preparatory capabilities often include the following elements.

### 5.1 Employee Training

Training ensures that transportation agency employees are educated about their emergency management roles, responsibilities, and duties, and ensures proficiency in their performance. Establishing all-hazards training programs that are consistent with Department of Homeland Security, Federal Emergency Management Agency, and Transportation Security Administration curriculums to provide training to all employees in security awareness, emergency response, and critical infrastructure protection. Advanced training programs must be provided for managers, including CEOs, senior staff, maintenance operations managers, and all-hazards managers. All-hazards training programs are in development, which are consistent with Department of Homeland Security, Federal Emergency Management Agency, and Transportation Security Administration curricula to provide training to all employees in security awareness, emergency response, and critical infrastructure protection.

### 5.2 Drills and Exercises

Transportation agencies should conduct their own tabletop and functional drills at least every 3–6 months to exercise emergency management plans and participate as active players in full-scale exercises held at least annually. They must use drills and exercises to develop follow-up actions, including debriefings and updates to plans, protocols, and processes to incorporate after-action findings.

### 5.3 Enhanced Traffic Management Centers

Many DOTs are developing and expanding sophisticated “intelligent transportation systems” that use electronic technology, such as traffic cameras, ramp monitoring, roadway sensors, and message signs to monitor and manage traffic in urban areas. Transportation agencies are upgrading their transportation management center (TMC) capabilities

from passive information collection to fusing multiple sources of data that are capable of supporting on-scene responders and the general public during incidents. These changes involve "24-7" operational requirements, access to special agency information systems, and should require the TMC to evolve into an auxiliary emergency operations center, closely networked with other emergency responding agencies and centers. As we move deeper into the twenty-first century, colocation of TMCs, emergency operations centers, and public safety answering points will become a critical security and economic necessity.

### 5.4 Emergency Traffic Operations

Transportation agencies must establish procedures for working with state and local emergency responders to provide emergency traffic operations during an incident. This should include determining how to assign equipment, such as mobile signs, trailblazer detour signs, and barriers as well as development of procedures for use of DOT maintenance and safety patrol personnel in assisting police in road closures and traffic management in major emergencies when police resources are stretched thin.

### 5.5 Evacuation Planning

Transportation agencies must work with personnel from city and county transportation, police, fire, and emergency management agencies; metropolitan planning organizations; and major hospitals to develop plans for primary and alternative evacuation routes for major population centers. This work usually includes identification of preplanned detour routes for the Interstate highway system and major thoroughfares, maps of each major highway access point showing where emergency vehicles should be parked to block traffic, permanent ramp gates at critical interstate entrances, and assistance in preparation of major metropolitan areas and downtown evacuation plans.

### 5.6 Communications Interoperability

Transportation agencies must participate in communications interoperability initiatives with first responders who have security responsibilities. This includes multiple means for disseminating emergency notifications, including web distribution, blast fax systems, radio codes, paging, and telephone calling lists, as well as development of an integrated communications system and establishment of mobile emergency response command centers to support various radio frequencies, including those for state DOT, state patrol, and local police and fire departments.

### 5.7 Equipment, Facility and Personnel Inventory Management

Transportation agencies are developing geographic information system-based databases for tracking their emergency response resources, including specific equipment and its location, and personnel and their home addresses. This enables managers to quickly pinpoint the closest available resources to emergency or incident sites. The systems are often accessible via laptop computer to supervisors in the field. Critical vehicles are equipped with automatic vehicle location transponders to enable rapid location of vehicles

during emergencies and appropriate personnel, such as motorist assistance patrols and state patrol officers should be equipped with respirator masks or place gas masks.

## 6 INCIDENT RESPONSE AND RECOVERY CAPABILITIES

Transportation agencies have maintenance forces and equipment active across the transportation network. As a result, they can play key response and recovery roles during and after an incident. For example, on a weekday in July, 2001, just before rush hour in Baltimore, a CSX freight train derailed and caught fire in a rail tunnel directly beneath the downtown's central business district. By 4:30 p.m., the City Fire Department had ordered all major roads into the city to close including several interstate routes. Maryland DOT's modal agencies played vital roles throughout the tunnel fire in maintaining traffic flow. The coordinated highways action response team (CHART) posted notices on variable message signs notifying motorists on closure of major routes into the city. State toll authority personnel coordinated temporary closure of I-395 into Baltimore. The state's transit operators coordinated light rail, bus, and commuter rail operations.

As the story of a major incident begins to leave the headlines, recovery efforts are just starting, particularly when infrastructure damage is severe. If transportation facilities are targeted or they experience ancillary damage, a stiff economic toll may be exerted if they are closed to traffic, particularly when alternate routes are not readily available. In such instances, pressure to rebuild quickly is often intense. Transportation agencies are equipped to oversee hundreds of infrastructure construction projects every year. Their access to heavy equipment and contracting capabilities make them uniquely qualified to lead reconstruction efforts.

The Los Angeles earthquake generated a year's worth of reconstruction work in a single event. The dramatic roadway damage caused by the earthquake placed a significant strain on auto-dependent southern California. Bridges and roads were completely knocked out at four locations on several interstate and state highways. CALTRANS, the state's DOT, however, had its first emergency debris and demolition contracts in place by 7:00 a.m. that day. CALTRANS maintenance crews implemented initial detours, while commuter rail and bus service was expanded to provide transportation alternatives. CALTRANS highway advisory radio, variable message signs, closed circuit television camera (CCTV), speed monitoring loop detectors, and traffic signal timing capabilities helped keep traffic moving in the days and weeks after the earthquake. Subsequent recovery efforts involved round-the-clock operations to accelerate reconstruction of earthquake resistant structures. CALTRANS' Traffic Management Center served as the center for mobility decision-making throughout the recovery.

Capabilities developed by transportation agencies to support responders during an incident and return to normal include the following.

### 6.1 Mobilization of Equipment, People, and Private Sector Resources

Mobilization of emergency transportation operations by transportation agencies and their partners involves assembling and organizing resources, including people, equipment, communications systems, expert technical support, and public information systems and

protocols. It is a capability that requires that the right people will deploy appropriate resources at the correct time.

Effective mobilization requires a partnership of local, regional, state, and federal agencies. Joint preparedness training is important, while response and recovery voice and data communications must be interoperable, and information must be shared. Key roles for transportation agencies include the following.

- Dispatch of personnel to incident scenes, including specialized service patrols and incident response teams to help secure the incident scene; provide emergency medical aid; support fire, rescue, and emergency medical services in their operations; relocate or remove vehicles and debris from the roadway; assist stranded motorists and others on the roadway; provide for emergency traffic control; and initiate longer-term traffic control for approaching traffic and affected areas.
- Arranging emergency contracts to engage specialty towing and recovery services or special clearance equipment in a timely manner and to minimize responder risk and traffic disruption.
- Assessment of transportation infrastructure condition and closure of unsafe components.
- Transportation of equipment, personnel, and supplies for supporting emergency activities, and provision of any highway clearances and waivers needed to speed up such movements.
- Provision of transportation-related resources, such as vehicle repair facilities, fleet parking, and storage areas to be used for servicing, refueling, parking, and storage of emergency vehicles.
- Provision of general traffic management assistance, including posting of temporary signing, portable variable message signs, temporary traffic controls, one-way systems, barricades, detour routings, lowering of freeway speed limits through use of dynamic message signs or variable speed limit signs, modification of ramp metering rates or signal timing to slow the flow of traffic, use of flashing beacons and Highway Advisory Radio to issue public warnings and advisories, and provision of vehicular traffic flow data and information from permanent and temporary monitoring sites.
- Use of traffic management centers operated by DOTs in many larger cities that offer electronic technology, such as traffic cameras, ramp monitoring, and roadway sensors, to monitor and manage traffic.
- Design and implementation of alternate transportation services to temporarily replace capacity lost to disaster damage.
- Provision of information for the public about issues, such as road closures, infrastructure damage, debris removal, and restoration activities via contacts with radio, television, and other commercial media and use of technologies, such as highway advisory radio, 511 travel information, variable message signs, and Internet web pages.

## 6.2 Recovery of Transportation Infrastructure

As emergency management activities switch from response to recovery, transportation agencies play either a key supporting role or a leading role if transportation facilities

have been damaged. Recovery of transportation infrastructure helps communities reestablish economic and social vitality. Key roles for transportation agencies include the following.

- Deployment of trained and skilled teams for rapid clean up, repair, and inspection of incident areas.
- Restoration of critical transportation routes and facilities, *via* deployment of emergency contracting procedures for restoration of transportation assets, services, and systems.
- Issuance or waiver of permits and other assistance required to restore utility lines or pipes that are immediately adjacent to, or run over or under transportation infrastructure.
- Continuing to keep travelers informed about important information on road closures, detours, and evacuation routes to travelers.
- Assistance with site investigation procedures, including crime scene preservation and documentation, use of data collection technology, and team procedures to minimize disruptions to traffic and responder exposure on roadways.
- Documentation of expenses used in cleanup or incident management for possible reimbursement by FEMA or other entity.
- Establishment of an employee assistance program and mental health services for responders, which includes professional counseling and peer discussion groups.
- Audits of entire incident response after each event and revisions to plans and procedures as necessary to improve the key activities of prevention, mitigation, preparation, response, and recovery in the future.

## 7 CONCLUSIONS

The costs of failure to prepare for a terrorist attack that affects the nation's transportation infrastructure, in terms of loss of life and economic disruption, could be catastrophic. Transportation agencies were able to act swiftly on September 11, 2001, and in other major incidents because they were already equipped to meet the challenges of responding to and recovering from the devastation caused by natural and man-made disasters. When incidents, such as hurricanes, wildfires, earthquakes, snowstorms, or major traffic crashes threaten safety and mobility, transportation agency personnel and equipment are part of response and recovery activities. Their sophisticated traffic management systems helps keep traffic moving, their information systems help keep communications flowing, and their construction expertise helps speed recovery.

The threat of terrorism, however, poses new challenges for transportation agencies. Because 80% of state DOTs report they have incurred additional costs to improve transportation security, continual investment in training, equipment, infrastructure hardening, and research for transportation agencies is vital.

## REFERENCES

1. Federal Highway Administration (2007). *Highway Statistics 2005*, US Department of Transportation, Washington, DC.

2. Douglas B., Ham and Stephen Lockwood, Parsons Brinkerhoff Inc., with Science Applications International Corporation (2002). *National Needs Assessment for Ensuring Transportation Infrastructure Security*, National Cooperative Highway Research Program, Washington, DC.
3. Minnesota Department of Employment and Economic Development and Minnesota Department of Transportation (2007). *Economic Impacts of the I-35W Bridge Collapse*, Minneapolis, MN.
4. Federal Highway Administration (2002). *Our Nation's Highways*, US Department of Transportation, Washington, DC.
5. American Association of State Highway and Transportation Officials (2008). *Fundamentals of All Hazards Security Management for State DOTs*, Washington, DC.
6. American Association of State Highway and Transportation Officials (2004). *2003 Survey of State Transportation Agencies–Summary of Results*, Washington, DC.
7. American Association of State Highway and Transportation Officials (2008). *Fundamentals of All Hazards Security Management for State DOTs*, Washington, DC.

## FURTHER READING

Blue Ribbon Panel on Bridge and Tunnel Security (2003). *Recommendations for Bridge and Tunnel Security*, Federal Highway Administration and American Association of State Highway and Transportation Officials, Washington, DC.

Boyd, A., Caton, J., Singleton, A., Bromley, P., Yorks, C. (2005). *TCRP Report 86 / NCHRP Report 525, Transportation Security, Volume 8: Continuity of Operations (COOP) Planning Guidelines for Transportation Agencies*, Transportation Research Board, Washington, DC.

DeBlasio, A. J., Regan, T. J., Zirker, M., Fichter, K., Lovejoy, K., and Morin, D. (2004). *Effects of Catastrophic Events on Transportation System Management and Operations: Comparative Analysis*, Volpe National Transportation Systems Center, Department of Transportation, Federal Highway Administration, Cambridge, MA and Washington, DC.

McCormick, T. (2006). Incorporated; *TCRP Report 86 / NCHRP Report 525, Transportation Security, Volume 9: Guidelines for Transportation Emergency Training Exercises*, Transportation Research Board, Washington, DC.

National Cooperative Highway Research Program Project 20-59(23), *A Guide to Emergency Response Planning at State Transportation Agencies*, Transportation Research Board, Washington, DC [final report anticipated 2009].

Parsons Brinckerhoff Quade and Douglas, Incorporated, Science Applications International Corporation, Interactive Elements Incorporated (2006). *TCRP Report 86 / NCHRP Report 525, Transportation Security, Volume 12: Making Transportation Tunnels Safe and Secure*, Transportation Research Board, Washington, DC.

Science Applications International Corporation (2004). *NCHRP Report 525, Transportation Security, Volume 1: Responding to Threats: A Field Personnel Manual*, Transportation Research Board, Washington, DC.

Science Applications International Corporation and PB Consult (2008). *NCHRP Report 525, Transportation Security, Volume 13: Costing Asset Protection for Transportation Portfolio Risk Management*, Transportation Research Board, Washington, DC, [forthcoming].

*Transportation Security-Related Publications*, (2008). Transportation Research Board, Washington, DC, trb.org/securitypubs.

# TRANSPORTATION SYSTEM AS A SECURITY CHALLENGE

MICHAEL D. MEYER
*Georgia Transportation Institute, Georgia Institute of Technology, Atlanta, Georgia*

## 1 INTRODUCTION

Over the past 30 years, more terrorist attacks have occurred against transportation facilities and services in the world than any other target [1, 2]. The main reason for this is that the extent and use of transportation systems make them highly valued targets, not only for the relative ease by which they can be attacked but also because of the highly visible and lasting psychological effect the attacks will have on the day-to-day lives of those who need transportation for their livelihood. For example, given the highly publicized attacks against the public transportation systems in London and Madrid, it is not hard to imagine that commuters in these cities will continue to wonder for some time if another attack is imminent. The important role that the transportation system plays in the nation's economy makes it a strategic economic target as well. Given the vulnerability of transportation networks to attack, providing security for the nation's transportation system is one of the most difficult challenges facing transportation and security organizations in today's world—and will likely to remain so in the foreseeable future (see, for example, [3–7]).

The purpose of this article is to define the context of the transportation security challenge as it relates to the characteristics of transportation systems. What are the characteristics of transportation systems that make the provision of security so challenging? How do these characteristics relate to the types of strategies that should be considered as part of a comprehensive program?

## 2 SECURITY-RELATED CHARACTERISTICS OF TRANSPORTATION SYSTEMS

It is difficult to describe the transportation system in general terms, especially when interested in potential attacks against the facilities and services that comprise it. These facilities and services, and their respective vulnerabilities, are very different. For example, public transportation systems by their very nature tend to concentrate riders on a limited number of transit routes and at an even smaller number of terminals and transfer points. Attacks against such a system could be concentrated on a few strategic components of the system, resulting in likely harm to large numbers of people. The highway system, on the other hand, is extensive and offers many redundant paths through the road network,

although in some cases such as bridges, there are strategic links that, if severed, would cause great disruption. Even with such differences, the transportation system does exhibit some generic characteristics that are important points of departure for any discussion of the challenge of providing security on this system.

## 2.1 Extent of the Transportation System

The United States has the most extensive and advanced transportation system in the world. Although some components of this system, such as urban transit and intercity passenger systems, are not as prominent as those in other countries, overall there is no other country that exhibits a greater level of mobility and accessibility provided by its transportation system. However, the consequence of having such an extensive and accessible system is that there are many opportunities to disrupt system operations—in other words, there are many potential strategic targets.

Table 1 provides an estimate of the extent of the different components of the US transportation system [8]. Not all of these components offer appealing targets to attacks. For example, the vast majority of the approximately 4 million miles of roads in the United States carry limited traffic volumes and do not serve any strategic economic purpose. A subset of this larger road network, the 162,373 miles of roads designated as part of the National Highway System, consists of the more important roads from the perspective of national connectivity, but even here, disruption to many of these roads would not have significant impact on economic activity. Similarly for bridges and tunnels, of the hundreds of thousands of such facilities in the US transportation system, 450 bridges and 50 tunnels are considered to be of strategic value in that their destruction would have significant economic consequences as determined from the criteria in Table 2 [9]. Similar observations can be made of the other components of the nation's transportation system. However, if the objective of an attack is to expose the vulnerability of the transportation system and not necessarily to cause the maximum amount of harm, then the sheer extent of the nation's transportation system makes it almost impossible to deter such an attack.

Table 3 shows another characteristic of the extent of the transportation system, this being the numerous components that make up the system [10]. The transportation system described in this table is for a road network, but similar types of components comprise almost any transportation system. Disrupting any of these components will disrupt a significant portion of the system; the large extent of the transportation system makes it very vulnerable to attack.

## 2.2 Network Characteristics

Every transportation system can be described in terms of networks, an interconnected set of links and nodes that provide for the movement of people and goods from an origin to a destination. Several characteristics of networks can be detrimental to providing effective transportation security throughout the system.

Transportation flows moving through a network most often traverse some critical link or node that can serve as a congestion bottleneck if disrupted. Thus, for example, freight containers arrive in the United States at ports are transshipped to either a truck or train, moved to an inland location, transferred to a truck, and delivered to the final destination. This movement includes at least two critical nodes—the port and the inland intermodal yard—the productivity of which significantly affects the overall efficiency of the trip.

**TABLE 1 Extent of the US Transportation System (2005)**

*Highway*
Public roads
- 46,873 miles of interstate highway
- 115,500 miles of other National Highway System roads
- 3,849,259 miles of other roads
- 580,000 bridges

*Air*
Public-use airports
- 5,270 airports

Airports serving large certificated carriers
- 26 large hub areas (69 airports), 484 million enplaned passengers
- 37 medium hub areas (60 airports), 141 million enplaned passengers
- 66 small hub areas (82 airports), 53 million enplaned passengers
- 930 nonhub areas (968 airports), 23 million enplaned passengers

*Rail*
Miles of railroad operated
- 95,664 miles by Class I freight railroads
- 15,388 miles by regional freight railroads
- 29,197 miles by local freight railroads
- 23,000 miles by Amtrak (passenger) (2004)

*Urban Transit (2004)*
Directional route miles
- Bus: 165,854
- Trolley bus: 425
- Commuter rail: 4,407
- Heavy rail: 1,596
- Light rail: 1,097

Stations
- Commuter rail: 1,153
- Heavy rail: 1,023
- Light rail: 723

*Water*
Navigable channels
- 26,000 miles (2003)

Ferry routes
- 623 directional route miles (2004)

Commercial waterway facilities (2004)
- Great Lakes: 600 deep-draft
- Great Lakes: 154 shallow-draft
- Inland: 2,320 shallow-draft
- Ocean: 4,298 deep-draft
- Ocean: 1,761 shallow-draft
- Locks: 257

*Pipeline*
Oil
- Crude lines: 60,043 miles of pipe
- Product lines: 71,310 miles of pipe

(*continued overleaf*)

**TABLE 1 (*Continued*)**

| |
|---|
| Gas (2004) |
| Transmission: 298,900 miles of pipe |
| Distribution: 1,139,800 miles of pipe |

*Source:* [8].

**TABLE 2 Determination of "Critical" Bridges**

| Criticality Factor | Function of: | Proxy | Source |
|---|---|---|---|
| | | Main span >165 ft | |
| Casualty risk | Users exposed | Average daily traffic (ADT) >40,000 | National Bridge Inventory (NBI) |
| Economic disruption | Role in national economy | ADT >40,000 | NBI |
| | | Functional system: interstate plus STRAHNET[a] | |
| | | Navigation preservation | |
| | Replacement/ down time | Main span length >165 ft and structure types | NBI |
| | Replacement cost | Main span length | NBI |
| | Redundancy | Detour distance >3 miles for ADT >60,000 | NBI |
| Military function | Support power projection platform | ON STRAHNET and/or on MTMC[b], power projection routes serving forts <400 miles from ports with main span >165 ft; no ADT limits | MTMC |
| | | Metro size (top 78) | |
| Emergency relief function | Major evacuation routes | Functional system: freeways, expressways, and principal arterials | Federal Highway Administration (FHWA) |
| National recognition | Symbolic importance | 5% of critical bridges | NA |
| Other | Collateral exposure | Roads on dams, pipelines, utilities, and so on. | NA |

[a]STRAHNET is the strategic defense highway network.
[b]MTMC is the military traffic management command.

*Source:* [9].

In passenger transportation, the critical nodes would include airports, train stations, bus terminals, and so on. The net effect of this network characteristic is to concentrate flows at well defined locations, resulting in potential targets that not only provide the maximum harmful physical and psychological effect at that location (for example, harming large numbers of people at a rail terminal), but which could also produce economic effects beyond that location (for example, the domino effect in the logistics supply chain of not being able to transship goods at a port).

**TABLE 3 Critical Highway System Assets**

| Infrastructure | Facilities | Equipment | Personnel |
|---|---|---|---|
| Arterial roads | Chemical storage areas | Hazardous materials | Contractors |
| Interstate roads | Fueling stations | Roadway monitoring | Employees |
| Bridges | Headquarters | Signal and control systems | Vendors |
| Overpasses | Maintenance yards | Variable messaging systems | Visitors |
| Barriers | Materials testing labs | Communications systems | |
| Roads on dams | Ports of entry | Vehicles | |
| Tunnels | District/regional complexes | | |
| | Rest areas | | |
| | Storm water pump stations | | |
| | Toll booths | | |
| | Traffic operations centers | | |
| | Vehicle inspection stations | | |
| | Weigh stations | | |

*Source:* [10].

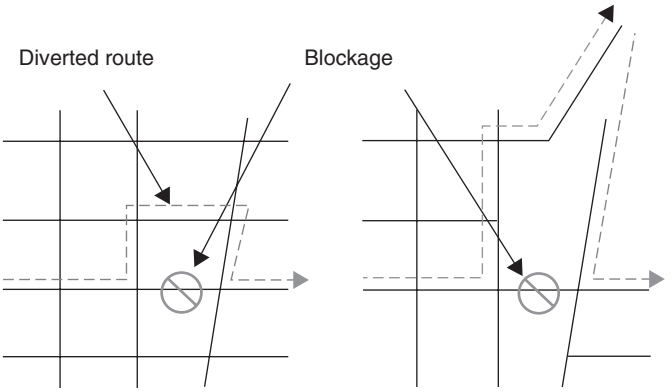



**FIGURE 1** Effect of network design on disruption: (a) network redundancy and (b) critical link disruption.

The above discussion focused on critical network nodes, but a similar phenomenon occurs in networks when, for efficiency or cost reasons, movements are "funneled" into critical links. Figure 1 illustrates this phenomenon. As shown in the figure, a disruption to the network in Figure 1a would cause much less disruption to network flows than severing a network critical link as shown in Figure 1b. The network redundancy shown in Figure 1a allows a network to recover more quickly by moving flows through different parts of the network, whereas the lack of such redundancy in the second network has more serious economic consequences and, depending on the circumstances, potentially catastrophic impacts.

The level of redundancy in the US transportation system varies by mode and by geographic area, depending largely on how a network has been designed. The national railroad network, for example, has a high level of redundancy built into it. A disrupted link at

one location could be handled by rerouting cargo along other network paths or, for certain types of cargo, even by transferring the goods to trucks, both options most likely increasing the costs of transport. At national flow levels similar network redundancy exists for the air, road, and port networks. The most disruptive aspects associated with deficient network redundancy occur at smaller geographic scales. Thus, for example, severing a critical bridge over a river in a major metropolitan area could be very disruptive for local travelers and to the local economy, even though flows going through the metropolitan area would most likely find alternative bypass routes. Given the transportation network design in most metropolitan areas, which often does not provide much network redundancy, there are numerous opportunities to create significant disruption in the nation's metropolitan areas.

Another characteristic of a network, especially one that is connected to a much larger transportation system, is the spatial nature of movement along the network links. In other words, a person or commodity located at one location at time $t$ will most likely be located somewhere else on the network at time $t + 1$. Thus, for attacks whose intent is to spread fear and disruption as wide spread as possible, such as the release of a biological agent in an airport whose effects might not be felt hours or days after the release, the structure of the transportation network permits the potential spread of harmful pathogens worldwide. Given the size and extent of a typical transportation network, tracking those entities that have been exposed or infected by some form of contagion would be challenging.

### 2.3 Transportation Nodes as Gateways

Transportation systems provide the major points of access into the United States, both for international freight and passengers. Thus, they can be viewed as one of the most vulnerable points of access for someone entering the United States with the intention to cause harm. For freight movements, they represent gateways to the US economy for much of the international trade entering the country. For example, it is estimated that over 26 million containers enter US ports each year, originating from all directions. Table 4 shows container flow through the top 30 container ports in the United States. With the flow of containers, which occurs at ports throughout the country, security monitoring of container movement becomes an important, albeit challenging, task.

The international nature of freight movement introduces additional complexity into transportation security. For example, a recent report from the Department of Homeland Security identified the following principles in enhancing the security of the international supply chain [11].

1. Accurate data in the form of advance electronic information is necessary to support the risk assessment of the cargo. This information is needed early in the process to identify high-risk cargo before it approaches the United States. In the case of containers, the information is needed before vessel loading in a foreign port.
2. Information must be appropriately shared among US government agencies and US trading partners, while simultaneously being safeguarded from improper disclosure.
3. Secure cargo requires a procedure to ensure that the cargo conforms to the cargo information electronically transmitted to the authorities. This process connects first-hand knowledge of the cargo with the validation of the cargo information. This process also ensures that safeguards are in place to prevent unlawful materials (or

**TABLE 4 Top US Container Ports, Twenty-Foot Equivalent Units (TEUs), 2005**

| Port | Rank | Import | Export | Net |
|---|---|---|---|---|
| Los Angeles, CA | 1 | 4864 | 1043 | 3821 |
| Long Beach, CA | 2 | 4378 | 1024 | 3355 |
| New York, NY | 3 | 3387 | 972 | 2415 |
| Charleston, SC | 4 | 1509 | 615 | 894 |
| Savannah, GA | 5 | 1469 | 670 | 800 |
| Oakland, CA | 6 | 1374 | 611 | 763 |
| Seattle, WA | 7 | 1339 | 464 | 875 |
| Norfolk, VA | 8 | 1319 | 540 | 779 |
| Houston, TX | 9 | 1222 | 599 | 623 |
| Tacoma, WA | 10 | 1155 | 362 | 793 |
| Miami, FL | 11 | 772 | 324 | 448 |
| Port Everglades, FL | 12 | 578 | 302 | 276 |
| Baltimore, MD | 13 | 382 | 137 | 244 |
| San Juan, PR | 14 | 213 | 48 | 165 |
| Gulfport, MS | 15 | 182 | 73 | 109 |
| New Orleans, LA | 16 | 174 | 101 | 73 |
| Wilmington, DE | 17 | 162 | 41 | 120 |
| West Palm Beach, FL | 18 | 159 | 121 | 39 |
| Philadelphia, PA | 19 | 158 | 20 | 139 |
| Jacksonville, FL | 20 | 144 | 99 | 45 |
| Boston, MA | 21 | 130 | 56 | 74 |
| Portland, OR | 22 | 120 | 60 | 61 |
| Newport News, VA | 23 | 103 | 42 | 61 |
| Wilmington, NC | 24 | 101 | 33 | 69 |
| Chester, PA | 25 | 101 | 45 | 56 |
| Freeport, TX | 26 | 54 | 26 | 28 |
| Honolulu, HI | 27 | 51 | 28 | 23 |
| San Diego, CA | 28 | 49 | 3 | 46 |
| Richmond-Petersburg, VA | 29 | 41 | 19 | 21 |
| Anchorage, AK | 30 | 33 | 32 | <1 |
| United States, total | | 25,868 | 8578 | 17,290 |

*Source:* [8].

persons) from being combined with the legitimate cargo. This part also includes a risk management process that includes the scanning and/or inspection of cargo identified as high risk before loading at foreign ports and, in some cases, after arrival at the US port.

4. Secure transit is a procedure designed to ensure that cargo remains secure as it enters and moves through the supply chain. Successful implementation requires a method of detecting if security has been compromised during transit and a response protocol to be enacted in the event of such a compromise. Securing the conveyances and transportation facilities used in the movement of commerce is critical to maintaining the security of the cargo while it is in transit.

5. Improvements to security—must be addressed in a way that will ensure consistency and substantive improvements across the supply chain. This can only be achieved via engagement with the appropriate international organizations, for example, the World Customs Organization (WCO) and the International Maritime Organization (IMO), and international trade partners in the development of standards. Standards are the only meaningful way that the government will be able to ensure that a high level of security across the supply chain.

As indicated, the extent of the security needs for international freight movement extends far beyond the borders of the United States.

The security challenge at international gateways will become even more significant in the future given expected trade flows into the United States. Figure 2, for example, shows the value of international trade crossing US borders and how it has changed dramatically since 1980 [12]. Almost every economic forecast of future trade shows continued growth in the amounts of international freight entering the United States.

## 2.4 Transportation as a Means

Transportation systems, by their very nature, exist to allow people and goods to accomplish some other objective. Thus, for example, we make trips not because of the pleasure of traveling in a vehicle or of moving along a road, but rather to arrive at work, deliver goods, go to school, take the kids to soccer practice, and so on. In technical terms, this is referred to as *derived demand*. It is assumed that the major purpose of a transportation service or facility is to allow a trip to be made as quickly as possible in order to accomplish some end goal.

The importance of this transportation system characteristic to security is that when the transportation system is disrupted, there are potentially significant consequences

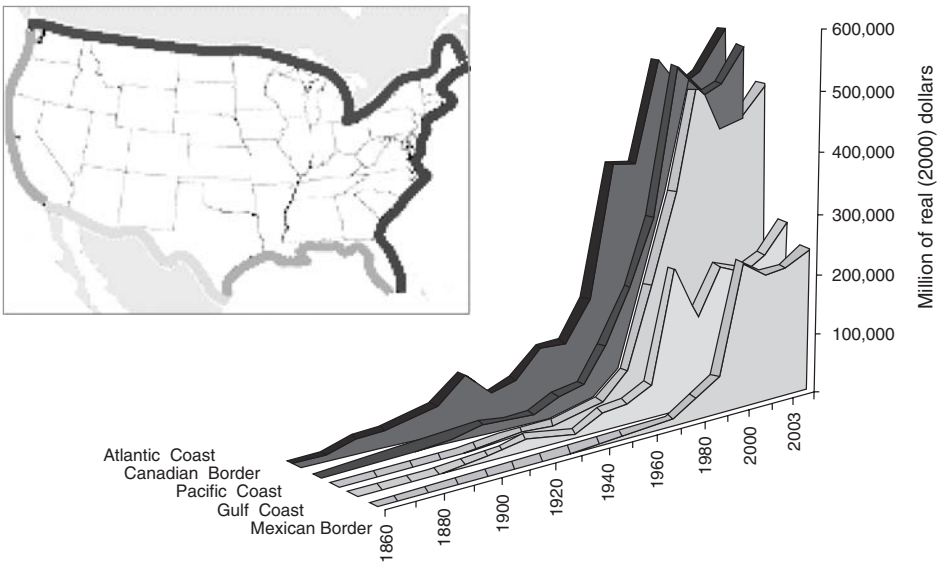



**FIGURE 2** Growth in US trade by border crossing ($2000). (Source: [12]).

to other societal functions. The impact of severing a highway or rail link at a major US port could have significant impact on the nation's economy. Or as was seen after the 9/11 terrorist attacks, the economic consequences to the US airline industry of a loss in customer confidence in air travel caused significant economic losses to US airlines.

The transportation of hazardous materials represents a particularly dangerous use of the transportation system, but one that is necessary in today's economy [13]. The delivery and disposal of hazardous materials reflect the types of economic activities that characterize today's manufacturing, service, medical, and research/development industries. Approximately 800,000 shipments of hazardous materials are transported on the US road and inland water networks each day, with over 4 billion tons being transported each year [13]. Roads and waterways account for 95% of these shipments. Not only severing a link in these networks would cause disruption to these movements, but also if hazardous materials were involved in the aftermath, the consequences to the local population could be much more severe.

### 2.5 Time Lag to Recover

Transportation networks are infrastructure intensive. Because of the time it takes to design and build any major infrastructure facility, physically destroying or making a structure or facility incapable of serving its function will most often require an in-kind replacement. In many locations in the United States, this infrastructure is nearing the end of its useful life, thus potentially making it easier to destroy. Although physical structures take little time to destroy, they do take time to replace. Thus, destroying a critical piece of infrastructure could have long-lasting effects given the time it takes for reconstruction. Many of the major interstate highway bridges destroyed by Hurricane Katrina, for example, have taken anywhere from 9 to 18 months to put back into service—and this was an expedited recovery program.

### 2.6 System Command, Control, and Communications

Transportation networks are often managed by command and control systems. Passenger and freight rail flows, for example, are directed by signaling and scheduling systems that provide safe movement often over tracks that serve both flows. Air traffic control systems provide similar functions for aviation. Increasingly, most metropolitan areas have traffic management systems that monitor road network operations and provide information to travelers. Although most of these command, control, and communications systems have redundancy and backups built into their structure, some level of disruption would result by removing these systems from direct contact over the networks they control, by either physical or cyber attacks.

Another important aspect of the system control nature of traffic flows is that system efficiency and reliability objectives often result in scheduled operations, thus providing commonly available knowledge on when trains, buses, and planes will be arriving at a given point.

### 2.7 Institutional Structure

Given the importance of transportation to the nation, states, metropolitan areas, and local governments, there are many organizations that have responsibility for some element of

this system. This is also true for private companies that provide transport services (such as carriers) and those who need such services (such as shippers). In the United States, the federal government has numerous agencies that have some say in transportation policy and finance; there are 50 state departments of transportation (53 if you consider the transportation agencies for the District of Columbia, Puerto Rico, and Guam); 376 metropolitan planning organizations (MPOs) having responsibility for coordinating metropolitan-level transportation planning activities; 6429 transit agencies; 6000 city, county or township transportation departments; 85 major port authorities; and an estimated 200 special purpose transportation authorities such as toll agencies or park districts that control key roads. With respect to security, there are thousands of police and security organizations that will likely interact with transportation agencies in response to a particular incident.

The benefit of having so many organizations is that they can specialize in providing the most cost-effective service for the markets they serve. However, the problem becomes one of coordinating all of the different participants that might be relevant to a specific issue [14]. Figure 3 illustrates this concept as it relates to security planning for urban transit systems. As noted, the larger the metropolitan area, the larger the number of likely transit providers and the greater the need for planning security in a coordinated manner [15].

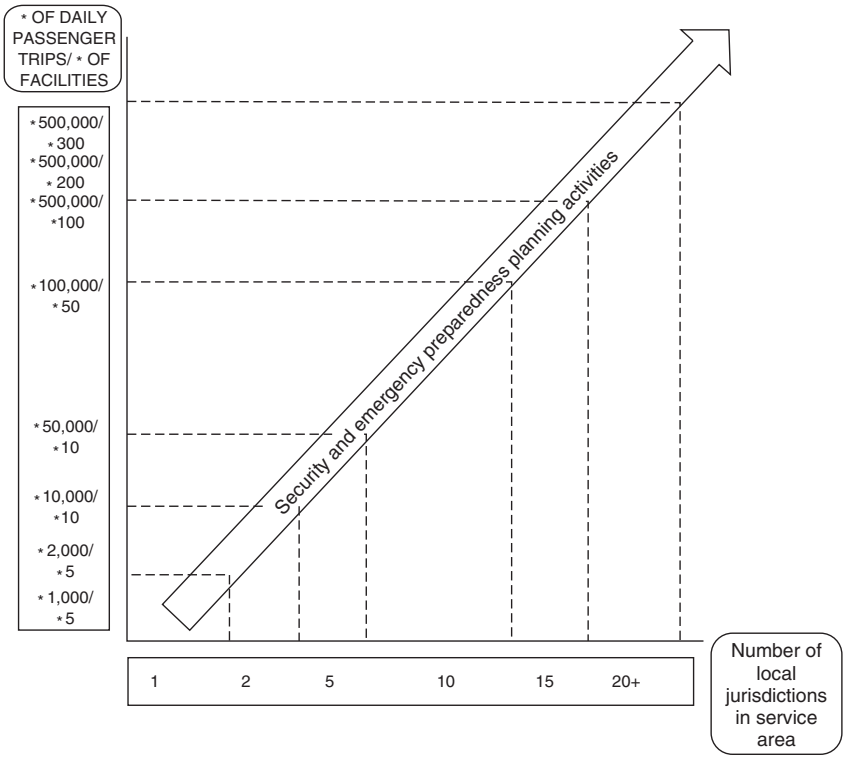



**FIGURE 3** Requirements for security and emergency preparedness. (Source: [15]).

Federal law requires that every urbanized area over 50,000 population must have an organization called the *metropolitan planning organization* (MPO) that is responsible for coordinating the transportation planning process for that urbanized area. In most cases, the MPO acts as a forum for collective transportation decision making as it relates to regional transportation investments, as well as addressing other issues of regional concern. In all but a rare number of circumstances, the MPO is primarily a planning agency; it is not an operating or implementing agency, and thus it depends on the willingness of transportation agencies and service providers to implement adopted regional strategies. This role is one that presents significant challenges for issues such as security that cross jurisdictional boundaries, especially given the fact that police and security agencies have seldom participated in the regional transportation planning process. As noted by Meyer [16] in a meeting focusing on the potential role of MPOs in security planning, possible MPO-led actions might include the following:

Given the MPO's strengths in *technical analysis and transportation planning*,

- conduct vulnerability analyses on regional transportation facilities and services;
- analyze transportation network for redundancies in moving large numbers of people (e.g. modeling person and vehicle flows with major links removed or reversed, accommodating street closures, adaptive signal control strategies, and impact of traveler information systems), and strategies for dealing with "choke" points such as tollbooths;
- analyze transportation network for emergency route planning/strategic gaps in the network.

Given the MPO's responsibilities for *funding strategies and projects*,

- fund new strategies/technologies/projects that can help prevent events;
- fund and perhaps coordinate regional transportation surveillance system that can identify potential danger before its occurring;
- fund communications systems and other technology to speed response to incident;
- fund programs and projects to recover from an attack.

Given the MPO's role as a *forum for cooperative decision making*, the following are the actions that seem most appropriate for the MPO in the context of security/disaster planning:

- providing a forum for security/safety agencies to coordinate surveillance and prevention strategies;
- coordinating drills and exercises among transportation providers to practice emergency plans;
- coordinating with security officials in the development of prevention strategies;
- providing forum for discussions on coordinating emergency response;
- coordinating public information dissemination strategies;
- acting as a forum for developing appropriate recovery strategies;
- coordinate the stockpiling of strategic road/bridge components for rapid reconstruction;
- coordinate changes to multiagency actions that will improve future responses.

The institutional coordination challenge becomes even more complex when the multitude of private transport carriers (such as trucking firms, railroads, and barge companies) and shippers become part of the larger security discussion.

## 3 ATLANTA AS AN EXAMPLE

The Atlanta metropolitan area is used as an example of the transportation security challenge facing a typical metropolitan area. Since 2000, the Atlanta area has been the fastest growing metropolitan area in the United States, with an estimated population of approximately 4.2 million in 2007. There are 16,000 miles of road in this region (excluding relatively minor streets and alleyways), including 987 freeway miles and 200 bridges. On a daily basis, over 154 million vehicle miles (number of vehicles times average miles traveled) occur on the road network. The world's busiest airport is located just south of the downtown, and the metropolitan area serves as an intermodal hub for two of the nation's major railroads. Much of the freight entering the United States through the port of Savannah (one of the largest container ports in the United States) passes through Atlanta on either truck or rail. There are six transit agencies in the region. The Metropolitan Atlanta Rapid Transit Authority (MARTA), the largest, carries 450,000 passengers on an average day on both 451 buses and in 184 subway cars that are used on a 38-station rapid rail system. The subway network is designed in a north/south and east/west line configuration, with both lines meeting in a major downtown rail station. Disrupting this downtown station would, in essence, disable the entire rail network. Several military bases and airfields are located in the region, each requiring convenient and reliable access to the nation's transportation system.

With respect to other strategic assets, Atlanta region is the fourth largest logistics center in the United States, is considered one the nation's largest telecommunications centers, and is home of the Centers for Disease Control, itself considered a vulnerable target due to activities relating to disease and pathogen research. The international headquarters of CNN in Atlanta guarantees that any major incident in the transportation system will be broadcast to the world very shortly after it occurs.

The freeway system is one of the most heavily congested in the United States, in some locations carrying over 300,000 vehicles per day. The design of the freeway system is such that there is very little redundancy in paths through the network. Indeed, vehicle crashes on the freeway link through the center of the downtown regularly bring much of the freeway system to a standstill. The freeway system is thus very vulnerable to disruption.

Institutionally, the region reflects the complexity of other major metropolitan areas. Being the state capital, Atlanta has numerous state agencies responsible for transportation and enforcement. It houses the state's emergency response center for disaster response. Atlanta is also a major federal center and is thus home to numerous federal transportation, security, and enforcement agencies. There are 10 core counties in the Atlanta region (28 in the expanded study area), 65 cities and towns, and an estimated 25 agencies that focus primarily on transportation issues. The Board of Directors of the Atlanta Regional Commission, the region's MPO, includes 39 members, of which 23 are elected

officials, 15 are citizen appointees, and 1 represents the state's department of community affairs.

The state department of transportation operates a regional traffic management center that includes video surveillance on most of the region's interstate highway system, as well as real time information dissemination via variable message signs and digital messaging. MARTA has real time surveillance of subway operations, including a system to identify the location of buses and rail cars on the network.

Enforcement on the region's highway network is primarily the responsibility of local police, although the state police do have a limited presence on the interstate highway network. MARTA has its own police department, as do major institutions such as the numerous universities in the region. The airport, which is part of the Atlanta city government, is policed by the Atlanta police department. Memoranda of agreement for mutual aid have been established among the region's police, fire, and emergency response units.

Atlanta's transportation system is a microcosm of the transportation system characteristics described earlier. It is heavily used, and serves critical economic purposes. It is very vulnerable having several choke points that could bring much of the region's transportation system to a standstill if disrupted. The airport and freight rail lines serve major international gateways, thus creating even more of a challenge in monitoring and policing the movement of people and goods. Institutionally, the region has many agencies and organizations with some interest and responsibility in transportation, and although transportation officials often claim that transportation decision making is efficient and effective, there is a long history in the region of a fragmented institutional structure for operating the transportation system. And finally, the visibility of Atlanta's transportation system in this case to the world (because of CNN) makes it a tempting target for those wishing to "make a statement" about how vulnerable the transportation system really is.

Although every metropolitan area is unique in its institutional structure and transportation system characteristics, it is not a stretch to suggest that the Atlanta is a good example to varying degrees of the other 375 metropolitan areas in the United States. Some are more complex; some are less so. However, the level of vulnerability to disruption and the often complex institutional structure for decision making are characteristics that will be found in all parts of the country.

## 4 SUMMARY

The primary intent of this article has been to describe the characteristics of the transportation system, which make it so vulnerable to disruption. Other articles in this book focus on the specific types of strategies that can be used to avoid or at least minimize the damage caused by attacks against this system. It seems clear from the historical record, and from a description of the extent of the transportation system, that it will be very difficult, if not impossible, to protect every component of the nation's transportation system. As has been seen in other countries, there are many ways of disrupting transportation services and of spreading fear among the population.

Transportation and the mobility it provides is too fundamental to today's society for it not to be a logical target for terrorist attack. Through rigorous vulnerability and risk

assessment efforts, however, the most important parts of this system can be protected. The challenge to transportation and security officials is to develop a collaborative process for developing and using a security-conscious approach toward transportation planning and decision making.

## REFERENCES


1. Committee on R&D Strategies to Improve Surface Transportation Security (1998). *Improving Surface Transportation Security. National Materials Advisory Board, Commission on Engineering and Technical Systems, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, and Transportation Research Board*, National Academy Press, Washington, DC.
2. California Department of Transportation (1996). *Terrorism in Surface Transportation: A Symposium*, Sacramento, CA, March 1.
3. Fritelli, J. (2003). *Maritime Security: Overview of Issues*, Congressional Research Service, Library of Congress, Washington, DC, December 5.
4. Lake, J., Robinson, W., and Seghetti, L. (2005). *Border and Transportation Security: The Complexity of the Challenge*, Congressional Research Service, Library of Congress, Washington, DC, March 29.
5. Parfomak, P. (2004). *Pipeline Security: An Overview of Federal Activities and Current Policy Issues*, Congressional Research Service, Library of Congress, Washington, DC, February 5.
6. Fritelli, J. (2005). *Transportation Security: Issues for the 109th Congress*, Congressional Research Service, Library of Congress, Washington, DC, June 15.
7. General Accounting Office (2002). *AVIATION SECURITY: Transportation Security Administration Faces Immediate and Long-Term Challenges*, Washington, D, July 25.
8. Bureau of Transportation Statistics (2007). *Transportation Statistics*, U.S. Department of Transportation, Washington, DC.
9. Ham, D., and Lockwood., S. (2002). *National Needs Assessment for Ensuring Transportation Infrastructure Security*, Report prepared for the American Association of State Highway and Transportation Officials, Washington, DC, October.
10. Science Applications International Corporation (2002). *A Guide to Highway Vulnerability Assessment for Critical Asset Identification and Protection*, Report prepared for the American State Highway and Transportation Officials' Security Task Force, Washington, DC, May.
11. Department of Homeland Security (2007). *Strategy to Enhance International Supply Chain Security*, Washington, DC, July 1.
12. American Association of State Highway and Transportation Officials (2007). *Freight Bottom Line Report*, Washington, DC.
13. Rothberg, P. (2001). *Hazardous Materials Transportation: Vulnerability to Terrorists, Federal Activities, and Options to Reduce Risks*, Congressional Research Service, Library of Congress, Washington, DC, October 15.
14. Meyer, M., Campbell, S. and Coogan, M. (2005). Collaboration: Key to Success in Transportation. In *Journal of the Transportation Research Board 1924*, National Academy Press, Washington, DC.
15. Balog, J., Boyd, A., and Caton, J. (2003). *The Public Transportation System Security and Emergency Preparedness Planning Guide*. Report DOT-VNTSC-FTA-03-01. Volpe National Transportation Systems Center, Cambridge, MA, January.
16. Meyer. M. (2006). Role of MPOs and Transportation Security. *Presentation to the Puget Sound Regional Council*. Seattle, WA, May.

# POPULATION EVACUATIONS

OSCAR FRANZESE

*Center for Transportation Analysis, Oak Ridge National Laboratory, National Transportation Research Center, Knoxville, Tennessee*

## 1 INTRODUCTION

For any emergency, originated from either a natural disaster (hurricanes, floods, forest fires, etc.) or a man-made event (a release of a toxic gas to the atmosphere, a radiological accident at a nuclear plant, etc.), there are six basic aspects that need to be considered: prevention, preparedness, detection, protection, response, and recovery. Different emergency management activities are associated with each one of these six aspects and many agencies at local, state, and federal levels cutting across several jurisdictions are generally involved.

Specifically related to the preparedness, response, and recovery tasks, emergency evacuation is, perhaps, the most viable alternative that can be undertaken in response to natural and man-made disasters involving large geographic areas. Other significant protective actions include sheltering in place and sheltering at public (government designated) facilities. Depending on the type of event, these two protective actions (evacuation and sheltering) can be combined and integrated to achieve the maximum risk reduction of the threatened population. In any case, sheltering always requires the mobilization of the population either at the beginning (sheltering at a public facility) or at the end (evacuation of the area in which shelter-in-place has been implemented after the threat has passed) and therefore, in what follows, it will be included in the broader category of emergency evacuation.

Emergency evacuation can be divided into two main phases: the planning phase and the implementation phase. The former is associated with the preparedness and the recovery tasks and, in general, focuses on the creation of evacuation plans for the area potentially at risk. These planning activities involve the development and evaluation of various alternatives (all of them with strong traffic management components), and the identification of the best course of action to be implemented in case a regional evacuation is required. The latter, which is the implementation phase, in which the selected alternative is deployed in the field, is associated with the response and recovery tasks.

The type of event (threat) plays a very significant role in the planning and implementation of emergency evacuations, since it dictates what type of protective actions (e.g. vehicular evacuation only, sheltering of some areas, and evacuation of others) are potentially feasible. As important as the type of threat in the evaluation and implementation of an emergency evacuation are the characteristics of the transportation network of the area at risk (and beyond), as well as the distribution and reaction times of the population to be evacuated. All this information is discussed in the next section. Following that, the different models that are used in planning and evaluation of emergency

evacuations are presented. Those include not only traffic simulation models, but also pedestrian simulation and threat evolution models. A discussion focusing on the integration of these models is also included in that section. The requirements for implementation of the selected plan of action are presented in the following section, which is followed by a discussion on "no-advance notice" evacuations. The final section presents future research needs in this area.

## 2 OVERVIEW OF RELEVANT INFORMATION FOR EMERGENCY EVACUATION MODELING

For the planning phase, the estimate of the time required for evacuation (i.e. the time associated with clearing the population in an area at risk to areas considered safe) as well as the spatial and temporal determination of traffic congested areas—which, in turn, affects the percentage of the population at risk during the evacuation; i.e. population clearance—is a key variable in evaluating the effectiveness of evacuation as a protective action option. The quantification of these decision variables requires the integration of traffic simulation models and demographic information models and the location and availability of shelters, among others. Traffic simulation models—that are traditionally used in developing and assessing emergency evacuations—permit to combine the demand that the transportation network of the area at risk will be experiencing during the evacuation and recovery stages, with the capacity of that transportation network to determine how congestions patterns will evolve during both stages.

Traditionally, when considering the type of problem described here, two geographic boundaries are customarily defined around the location of the event: (i) the immediate response zone (IRZ) and (ii) the protective action zone (PAZ). The IRZ is defined as an area where an effective and prompt response is critical in order to avoid the loss of human lives while the PAZ is an area slightly farther and removed from immediate danger but one that can be potentially threatened depending upon the type of disaster and weather conditions. Beyond the PAZ, there is an area known as the *precautionary zone* or *PZ*, where no adverse effects may be expected for the population [1, 2]. The boundaries of the IRZ and PAZ are delineated by models that predict how the threat would evolve spatially, and these boundaries may be static or dynamic depending on the type of threat. For all practical purposes, it is assumed that when reaching the PZ the evacuating population is no longer at risk; therefore, the boundary of the PAZ delimits the transportation network that needs to be considered when assessing evacuation as a protective action alternative.

When dealing with evacuation only, the intersection of the evacuation routes with the boundary of the PAZ defines the exit points of the network, which from the modeling standpoint determines when a vehicle has been evacuated. If sheltering is also considered, then there will be destination points (i.e. shelters) within the PAZ at which vehicles/passengers may be considered to have been evacuated. If due to the type of event there is a need to evacuate these shelters after the threat has passed, then a delayed evacuation for these places has to be considered and modeled. Similarly, when considering sheltering in place as a protective action to be deployed in some areas within IRZ/PAZ, the effect would be a reduction in the demand of vehicles accessing the network at the beginning of the evacuation and depending on the threat, an increase in that demand at a later time.

### 2.1 Demographic Model

The determination of traffic demand estimates (i.e. the number of evacuees and evacuating vehicles by location) is a critical piece of information needed in assessing the feasibility of emergency evacuation and other protective action alternatives. This traffic demand that is a necessary input to determine evacuation times, is obtained from demographic data models. To construct these models, it is possible to assume that during the interval of time between late-evening and early morning hours the vast majority of an area's population is at its place of residence. Therefore, the primary source of data on the study area's nighttime population is, in general, census information. The spatial location of the daytime population is a far more difficult problem to solve, with no standardized procedures for generating estimates of at-work daytime populations. The level of confidence in determining the location and number of the daytime population is, therefore, much lower than that of the nighttime population. These uncertainties could have a great impact in the evacuation evaluation and analysis tasks since evacuation time estimates, and the strategies to minimize those times, are very sensitive to the spatial distribution of the population at risk.

Research is being conducted to minimize these demographic uncertainties. One such effort is the LandScan USA effort that is part of the LandScan global population project sponsored by the Department of Defense [3–5]. The LandScan USA project focuses on the development of very high resolution population distributions (i.e. 3 s $\times$ 3 s, or 90 m $\times$ 90 m, cells) data set for the entire United States. This population distribution grid is more spatially refined than the census block-level resolution, and includes spatial distributions for "residential nighttime population" as well as for "daytime population", for every hour of the day.

Besides the distribution of the population within the area potentially at risk, the reaction of the population to the order to evacuate also plays a very significant role in the viability of an emergency evacuation. The emerging traffic congestion patterns that would be observed during the evacuation of the affected area (and in consequence the evacuation time of the population at risk) greatly depend on the dynamic characteristics of the demographic model. Relatively, small variations in departing times, intermediate stops, and final destinations can produce significant changes in congestion patterns and, hence, evacuation times. Therefore, it is necessary to determine as accurately as possible these demographic dynamic characteristics.

Some research has been conducted in this area to determine what is known as *population mobilization curves* or *departing times*, although much works needs to be addressed on this critical topic. The work of Sorensen et al. [6, 7] has concentrated on the reaction times for release of toxic gases to the atmosphere, while others [8] have focused on hurricanes. The mobilization curves greatly depend on the type of event. Therefore, each particular threat and even geographic area (due to, e.g., population age distributions) has an associated mobilization curve that needs to be known with a sufficient degree of certainty in order to be able to predict evacuation times.

Also related to the traffic demand generated in an emergency evacuation is the vehicle occupancy information. This parameter depends on many factors, including the type of disaster, the location of the evacuating population (i.e. urban vs. rural areas), and the time of the day [9].

Other relevant issues regarding the behavior of populations during emergency evacuations are related to the determination (and modeling) of intermediate stops before leaving the area at risk, the selection of the final destinations, and the relocation of the displaced

population. Intermediate stops, such as parents stopping at their children's schools to gather them before leaving the area, can create unanticipated traffic flows that could greatly affect the evacuation times of the area at risk. Moreover, and depending on the geographic area under consideration, this may be an inward traffic flow (i.e. going toward the source of the threat), and can potentially impede or delay the movement of emergency vehicles. The selection of the final destinations is also a critical piece of information that can greatly impact the modeling and results of emergency evacuation simulations. Very little research exists on these topics.

## 2.2 Network Topology, Capacity, and Geometry

The characteristics defining the transportation network of the area at risk obviously play a critical role in the determination of the feasibility of an emergency evacuation. While the demographic model provides the demand-side of this problem, the capacity (in a broad sense) of the transportation network dictates whether or not there will be a reasonable interval of time available for the evacuation given that expected dynamic demand. This "network capacity" relates mostly to the physical characteristics of the network (number of lanes, lane widths, type of traffic controller, ramp metering, slopes, etc.), but also to the performance of the vehicles (e.g. a truck cannot climb a very steep slope at the same speed of a car, thus reducing capacity of that particular roadways segment).

As discussed previously, once the boundaries of the emergency planning zones (EPZs) have been delineated and include the area potentially at risk, it is necessary to have an accurate and reasonably detailed representation of the highway network within these zones to estimate evacuation times and to develop evacuation plans. The network data describes the topology of the roadway system and its characteristics, including geometry and channelization of traffic, traffic control devices, and other traffic parameters. Some of this information (e.g. network topology and geometry) can be obtained reasonably easily from maps or GIS (geographic information systems) databases. The remaining information; that is, traffic control settings, speed limits, and other traffic parameters, has to be gathered from other sources and, in general, is not as readily available, at least not in the format that is required by the traffic simulation models used to develop and evaluate the evacuation plans. In particular, the traffic control settings of actuated and semiactuated controllers (the most commonly used traffic signal equipment in major arterials in the United States) can be very demanding in terms of the parameters that define the operations of such devices. This information is necessary, at least to evaluate the "do-nothing" alternative (i.e. evacuation under regular network conditions and without any traffic management strategy deployed), which in some cases may become the *de-facto* deployed alternative. Most of the delay in a network occurs at the intersections, and therefore those should be modeled as accurately as possible. The problem of gathering all this information becomes more acute when one moves from a planning environment to assessments of emergency evacuations with no-advance notice (see discussion below).

There is also the issue of a constantly changing environment. That is, it is safe to say that while these traffic parameters hardly vary over time (unless, for example, new land-use developments bring larger traffic demands), changes in the capacity of the roadway system are very likely. Road or lane closures due to construction and road maintenance are a common sight in urban and rural areas alike. While this information has a relative low value during normal conditions (except, of course, for travelers), in case of an emergency evacuation it becomes crucial. Traffic management strategies may

depend heavily on the topology of the network; knowing which streets are unavailable or have a significant capacity reduction may be the difference between a successful strategy implementation and an aggravation of the problem. Some research has been conducted in this area to try to take advantage of remote sensing technology to automatically detect changes in roadway capacities (e.g. lane closures) and to incorporate that information directly into traffic simulations models in an attempt to determine the currency and validity of evacuation plans [10, 11].

### 2.3 Threat Evolution

Each type of threat, being either a consequence of a natural or a man-made disaster, has a particular temporal and spatial evolution. These predictions are extremely important since they not only delineate the areas that would be most affected by the threat but also provide information regarding when that peak is likely to occur. There are many models currently available, which can provide information in this regard.

Models such as ADMS 3 (atmospheric dispersion modeling system) [12], American Meterological Society/Environmental Protection Agency Regulatory Model (AERMOD) [13], PUFF-PLUME [14], and HPAC (hazard prediction and assessment capability) [15], among others permit to assess the atmospheric dispersion of vapors, particles, or liquid droplets from multiple sources and calculate concentrations of these gases spatially and temporally. Many of these plume dispersion models accept arbitrary meteorological inputs going from simple surface wind speed and direction up to multidimensional grids containing wind and temperature information to account for dense gas effects and dynamic plume rise as well as time- and space-dependent boundary layers, and flow over complex terrain.

For storm surges predictions for hurricane flooding there are many models available, including SLOSH (sea, lake, and overland surges for hurricanes) [16], ADCIRC (advanced circulation model) [17], CEST (coastal and estuarine storm tide model), and FVCOM (finite-volume coastal ocean model) [18] among many others. These models, together with existing hydrologic flood prediction models, fire propagation models, and tsunami propagation models provide analytical capabilities to assess and evaluate the potential consequences of these threats.

Although at the present time there are no integrated models that combine threat evolution with traffic simulation, this is a necessary step in the evaluation of emergency evacuations and sheltering as protective action alternatives. An integration of these threat evolution models and traffic simulation models is discussed below.

### 2.4 Real-Time Information

If vehicular evacuation (i.e. either the “do-nothing” alternative or an option that calls for the deployment of a traffic management strategy) is determined to be the optimal protective action for the conditions analyzed, a plan that implements the selected alternative must be deployed. In that case, it is paramount to collect real-time traffic and road conditions, as well as weather information, to support the emergency evacuation operations decision-making process and to keep informed the evacuating population.

The need for real-time information adds another (perhaps the biggest) layer of complexity to the problem at hand. Intelligent transportation systems (ITS) are capable of

delivering real-time information about traffic, and in some cases weather, but up to now the deployment of these systems has been sparse, at best, and concentrated only on major urban areas. Emergency evacuation of areas outside these instrumented regions (i.e. most of the country) will have to proceed without real-time traffic information or using field staff reports produced by handheld traffic counters, which, in general, cannot provide complete and/or accurate coverage of the entire system.

There is undergoing research [19] that is evaluating new technology, capable of generating travel times and other traffic information through fast-deployable sensors that can be set up in any area that requires evacuation and can provide real-time traffic information on selected segments of roadways.

## 3 MODELING EVACUATIONS

The first step in modeling an emergency evacuation consists in gathering the basic information described previously. This includes the delineation of the IRZ and PAZ areas (usually done with the assistance of a threat evolution model); the creation of a demographic model detailing the spatial distribution of the population that can potentially be affected; and the gathering of information describing the geometric/operational characteristics and topology of the transportation network. Combining these three data sources, a traffic simulation model of the area to be evacuated is usually developed and run, producing output that basically defines the location of each evacuating vehicle at given intervals of time.

This modeling task takes place during the planning phase and a traffic simulation model is used to analyze different scenarios and courses of action. Generally, a "do-nothing" alternative—i.e. evacuation without any traffic management strategy deployed—is compared against alternatives that basically increase the capacity of the evacuation routes—for example, reverse-lane strategies, traffic signal strategies—and/or try to "smooth out" demand peaks—for example, holding traffic at certain intersections while allowing traffic on the main evacuation route to go through. If the event could be predicted beforehand, other countermeasures, such as building new or upgrading existing evacuation routes and other long-term strategies, can be modeled to assess their impact in reducing the expected time to evacuate (ETTE) the area at risk.

The traffic simulation model used has to be not only reasonably accurate, but also be able to simulate with high level of fidelity the different components of a transportation network (including traffic controllers, driver behavioral characteristics, vehicle performances, and many other aspects and elements). Very few of these traffic simulation models are specifically tailored to evaluate emergency evacuations providing specific outputs such as ETTE, clearance time (i.e. the percentage of the population that is still within the area at risk during the evacuation, and other measure of effectiveness that are specific of this type of problems). Nevertheless, general purpose traffic simulation models (e.g. CORSIM [20] and VISSIM [21]) can also be adapted, although with some constraints, to model an emergency evacuation. In general, these traffic simulation models deal with just a single mode of transportation (i.e. passenger cars) and in some cases are able to simulate public transit as well. However, no multimodal models exist that can combine pedestrian and vehicular interactions.

### 3.1 Traffic Simulation Models

There are basically three types of traffic simulation models: (i) macroscopic, (ii) mesoscopic, and (iii) microscopic models. If the model traces the vehicles' movements implicitly and link performances (i.e. modeled segments of roadways) are expressed in an aggregated way, the simulation is defined as macroscopic. If the model follows the vehicles' movements explicitly, two cases are possible, depending on whether link performances are expressed in an aggregate or disaggregate way. In the first case, the simulation is mesoscopic, otherwise it is microscopic.

Due to the way in which vehicles are modeled and result statistics kept, the macroscopic models are the fastest (in terms of CPU time), followed by mesoscopic and microscopic models, in that order, for the same network and inputs. The speed of execution is one of the main characteristics of a traffic simulation model. In an ideal environment, the traffic simulation model should be run many times (i.e. many replications) to obtain probability distributions of the measures of effectiveness (MOEs) on which the decisions (whether to evacuate or shelter the population, which areas to evacuate or shelter, when to evacuate, etc.) will be made. The modeling process is an iterative one, especially when the "best alternative" is sought, so it should be possible to run the necessary replications fast and then run the model again after adjustments are made based on the results of previous runs.

Depending on the type of disaster being evaluated, emergency evacuations may involve the analysis of very large geographic areas, in many cases in the order of several thousands of square miles. The modeling of different traffic management strategies under these conditions can be very taxing in terms of computer run time, even with today's fast computers. Particularly, when using microscopic simulation models for the evaluation of these alternatives with the additional requirement of running many replications (to obtain statistically significant comparisons of alternatives), the speed of computation problem is aggravated. In fact, the fine granularity that microscopic traffic simulation models provide is not necessary, at least during the planning phase, except to simulate some detailed and localized traffic management strategies such as, for example, the optimization of traffic controllers along an arterial within the area at risk. Depending on the type of event being analyzed, macrosimulation models that can run very fast permitting the rapid modeling and evaluation of different strategies are more appropriate.

One such macrosimulation model is the Oak Ridge Evacuation Modeling System (OREMS), which is based on the Federal Highway Administration—Traffic Simulation Family of Models (FHWA-TRAF) family simulation models and was developed for the Federal Emergency Management Agency (FEMA) and the US Army under the Chemical Stockpile Emergency Preparedness Program (CSEPP). This traffic simulation model was specifically developed to analyze large-scale emergency evacuations, permitting to experiment with alternate routes, destinations, traffic control and management strategies, and evacuee response rates. For any scenario, it is possible to identify evacuation or clearance times, traffic operational characteristics, such as average evacuation speed, bottlenecks, and other information necessary to develop effective evacuation plans, at any spatial level of aggregation from a single segment of freeway to the entire evacuating area [22].

Whether a microscopic or a macroscopic simulation model is used, validation of that model is extremely important but difficult, particularly for emergency evacuations since these are very rare events. Nevertheless, the models should be calibrated and validated,

at least using normal traffic conditions to roughly determine the level of accuracy that can be expected in modeling an emergency evacuation of the area potentially at risk.

### 3.2 Trip Distribution and Traffic Assignment Model

In general, before running the traffic simulation model, it is necessary to know where the demand will be generated during an evacuation, and equally or even more importantly, where these travelers will go. In many cases when modeling an emergency evacuation, the former (i.e., the population distribution) can be determined with an accuracy that is proportional to the effort invested in creating the demographic models described previously. The latter (i.e., the identification of destination points), however, is more difficult to obtain, but can be derived by using so called trip distribution models. Those, in general, are simplistic models and may not address the issue of intermediate destinations (and dwelling times at these locations) discussed before.

The other set of models that are used in conjunction with traffic simulation models are traffic assignment models. These models basically "map" on the transportation network, the paths that will be followed by vehicles that want to reach a given destination when departing from a given origin at a given time. There are many traffic assignment models, but the most common are static traffic assignments (STAs) and dynamic traffic assignments (DTAs). In the planning mode, as well as in the operation model, DTA should be used only if it is possible to assume that (i) there will be a way of determining traffic conditions on the transportation network in real-time, and (ii) it is possible to convey information to the traveling population. If any one of these assumptions does not hold, then using a DTA model will produce more optimistic results (i.e. less congested network and therefore smaller ETTE) that it would be expected in a real evacuation of the same area that is being modeled (assuming that the demographic and transportation network models are reasonably correct). This is because, DTA models will find "excess" capacity in the network (i.e. less congested paths between an origin and destination) and reroute some of the demand through these paths. This will only be reproduced in an actual evacuation if there is a way to obtain real-time traffic information (to know the status of the network and to be able to predict how the congestion patterns would evolve) and if it is also possible to inform the driving population of the availability of these less congested paths.

There is, however, a case where even without real-time traffic information and/or a way of conveying information to travelers it would be reasonable (an in fact desirable) to use DTA. A DTA model can be assumed to hold in a localized area such as, for example, the trip from home or work to the nearest freeway on-ramp. This is because, in this case, due to his/her familiarity with the network, it is possible to assume that the traveler can react to congested roads by selecting other paths that will take that traveler from the origin (home or office) to the destination (nearest freeway on-ramp) of this leg of the trip. Beyond that, some other traffic assignment model should be used, where the main assumption is that the driver only has a limited number of routes (i.e. a limited knowledge and familiarity with the transportation network) from which he/she can choose.

### 3.3 Multimodal Evacuations

The models described previously assume, in general, that in an emergency evacuation the population would evacuate the area traveling on a vehicle from origin to destination. This

is clearly not the case in many instances, particularly those cases that involve events in downtown areas of large cities. New trends in the revitalization of downtown areas across the nation have produced development configurations, which purposely induce pedestrian movements. Shopping and other service areas, and more importantly, large sport venues have been built in these downtown districts without their own parking facilities to compel visitors to walk around the area. Instead, distributed parking facilities, which during the working hours service offices, are used during the evenings by downtown visitors and also during sport events. The distributed parking facilities across downtown for patrons of these venues could generate significant levels of traffic congestion due to heavy pedestrian volumes in the area if evacuation is required.

This presents a difficult modeling problem that the traffic simulation models described before cannot solve because they are designed to handle just vehicular movements. There are many pedestrian simulation models available that have been developed over many years with empirical studies going back almost five decades. Those early studies resulted in guidelines to design facilities that are efficient, safe, and aesthetically pleasant to be used by pedestrian [23, 24]. Models that simulate the behavior of large crowds are regularly used to study and evaluate practical solutions in terms of both crowd safety and emergency evacuation when designing large buildings and other structures. Pedestrian movement models exist to simulate the flow of large crowds, and are used to assess evacuation strategies for sites with multiple buildings and to study large-scale evacuations from buildings, offices, and sports venues.

Those sophisticated models can be used for the planning of evacuation in areas with very high pedestrian densities likely to be created, for example, by spectators evacuating large sport venues in these newly redesigned downtown areas. However, they cannot model the pedestrian–vehicle conflicts that would naturally arise, when evacuating pedestrians try to reach the scattered parking lots to access their vehicles and leave the area. These pedestrian models can also be used for the analysis of particular threats such as tsunamis where the more efficient course of action is a vertical evacuation; that is, the access to shelters that are high above ground level such that at risk population can quickly reach a safe area and be out of harm from the threat.

In many cases, it is necessary to use public transportation to move people out of the area[1], especially those parked in the vicinity of the venue with a sport event in progress. The use of public transportation and its interaction with pedestrian flows are also important for the evacuation of special populations such as the elderly and the poor who may not have accessibility to any other means of transportation to evacuate the area at risk.

All these cases require multimodal simulation models to study the different protective action alternatives. There are very few studies dealing with multimodal issues in emergency evacuations, and even fewer studying the complex interrelationships between vehicles and pedestrians. In one such study, these interactions as well as behavior that is unique to parking lots are implemented in a model that can simulate the evacuation of large parking lots [25].

[1]Under certain weapons of mass destruction scenarios producing an intense electromagnetic pulse, the sophisticated computerized components of today's vehicles may be damaged rendering those vehicles undrivable. As a consequence, streets may be blocked by many stopped vehicles; in that case it would be more efficient to clear few roads and use buses from outside the area to evacuate the affected population.

### 3.4 Integration of Threat and Evacuation Models

When modeling and evaluating vehicular evacuations as a protective action alternative, the ETTE (in conjunction with clearance information) is the decision variable that is used to determine the merits of a proposed evacuation plan and any traffic management strategy. The ETTE is the predominant decision variable when studying evacuations due to natural disasters, such as hurricanes and forest fires, since in these cases there is enough advance notice such that it is feasible for the evacuating population to clear the area at risk before the threat arrives. That is, in these cases the ETTE provides an estimation of when the mobilization should start given the predicted time of arrival of the threat.

In other cases, particularly for man-made disasters such as the release of a toxic gas to the atmosphere, ETTE may not be the correct decision variable. The reason for this is that in these instances, because of the short reaction time available to clear the area at risk, it is likely that the threat could be in contact with the evacuating population. Therefore, a more appropriated decision variable to assess protective action alternatives for these cases is the number of affected people that will suffer consequences—i.e. expected fatalities (EF) and expected number of people with permanent disabilities (ED)—if that particular alternative is deployed (note: in both cases, other decision variables such as deployment costs are also considered, but in general those variables play a secondary role).

At the present time there are no models that integrate both traffic simulation and plume dispersion models to evaluate evacuation plans for this type of scenarios, which after 9/11 have become more likely to occur. Analyzing those scenarios using the traditional ETTE computation approach could result in a decision process that may select the wrong protective action strategies, which, if implemented, could result in the loss of many lives. However, an integration of these two types of models (plume dispersion and traffic simulation) is a reasonably simple task, which could significantly improve the current decision-making process for these type of problems. A brief description of how this task could be accomplished is given below.

***3.4.1 Traffic Simulation and Threat Evolution Model Integration.*** From the previous discussions about traffic simulation models, it is obvious that those models do not provide a direct way of quantifying the outcomes of different alternatives in terms of EF and ED. However, they supply important and intermediate information, such as temporal and spatial distribution of the evacuating population, which can be used to estimate these variables. That is, the traffic information can be combined with threat evolution models (i.e. plume dispersion models in this scenario) to obtain probability distributions of EF and ED for each alternative analyzed, thus allowing the evaluation of the different strategies and ultimately, with the intervention of a relevant decision maker, the selection of the "best one". Notice that, unless an alternative stochastically dominate all the others, there is no quantitative methodology (other than naïve approaches such as using the averages of the distributions) to select the "best" strategy without the intervention of some relevant decision maker who could evaluate, explicitly or implicitly, trade-offs among the distribution of the different outcomes of the alternatives being analyzed.

The plume dispersion models produce temporal and spatial distributions of the concentrations of the released agent, based on topography and predicted weather conditions. Due to the fact that weather conditions are not known with certainty (e.g. at any given time there is a certain probability $p_1$ that the wind will blow from sector—i.e. direction—$s_1$, a probability $p_2$ that it will blow from sector $s_2$, ..., a probability $p_n$ that it will blow

from sector $s_n$, with $\sum_{i=1}^{n} p_i = 1$), the concentration distributions of the released agent are stochastic. That is, each concentration distribution (in time and space) will have a certain probability of occurrence attached to it. These concentration distributions can be overlaid, both spatially and temporally, on a map of the area affected, which translates into information about the dynamics of the concentration of the agent on each link or roadway segment of the transportation network and on each point where there is population.

With information about the network topology and attributes, as well as the demographic model completed, a traffic simulation model can be created and run, first for a "do-nothing alternative" (i.e. the network as it is, without any traffic management alternative deployed) and then with different strategies deployed. The output of any of these alternatives consists basically a list of travel times on each of the network links and the number of vehicles that enter, are on, and exit the link at fixed intervals of time (as low as 1 s-interval for some traffic simulation models). Moreover, since at the start of the evacuation the total number of vehicles at each network entry point within the affected area is known (from the demographic model), the outputs also provide information about the spatial distribution of the "not-yet" departed population by time. By merging this information with the distribution of the concentration of the agent it is possible to compute the dosage that the passengers of each vehicle are likely to accumulate from the moment the evacuation starts until that vehicle crosses the PAZ. The accumulated dosages then translate into number of EF and ED, with a certain probability of occurrence. This probability is the results from combining (through the simulation and integration of the results from both models) the probability of observing the particular concentration that gave rise to the observed dosages and probability distributions of the outputs of the traffic simulation model if many replications are considered. Repeating this computational process for all the possible concentration distributions (i.e. $n$ distributions and each replication $r$), it is possible to construct probability distributions of EF and ED for the particular alternative being analyzed.

Figures 1–4 illustrate this process. The first figure presents a map of an affected area, where the location of the event is shown as a circle located on the north-central part of that map. Given a scenario $i$ (let us say, certain weather conditions that can occur with probability $p_i$), the evolution of the plume is represented spatially and temporally in Figure 1 by superimposing on the map snapshots of the plume at constant intervals of time, with different levels of concentration represented by areas of different colors within the profile of the plume. The white circle southwest of the event shows an urban area that could be affected and where some protective action (e.g. evacuation) may need to be taken. To analyze the evacuation of that urban area, it is necessary to generate a demographic model and a transportation network model, which are inputs to the traffic simulation model. In turn, the outputs of the latter are combined with the plume dispersion model information to obtain a dosage distribution similar to the one shown in Figure 2, which would produce estimates of $EF_i$ and $ED_j$ based on the type of agent, and would be assigned a probability $p_i$ of being observed, for replication $r_m$ (for simplicity reasons in presenting these graphs, these computations are based on just one replication of the traffic simulation model).

The particular scenario shown in Figure 1 is not a deterministic one,—i.e. $p_i$ is greater than 0 but less than 1—and therefore there are other scenarios, such as scenario $j$, for example, that are also likely to be observed (see Fig.3). The dosage distribution for scenario $j$ is represented in Figure 4; with the characteristics of the agent, estimates

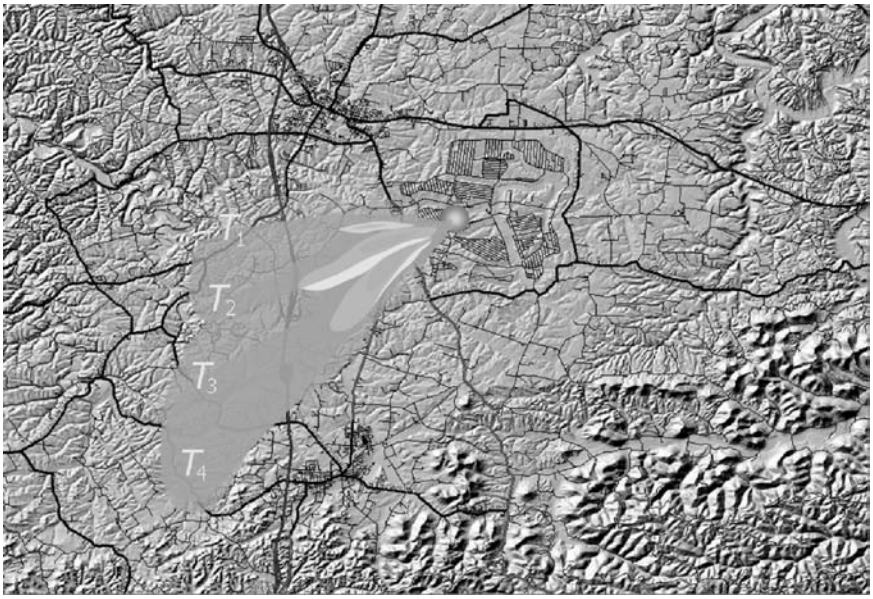



**FIGURE 1** Area at risk and plume dispersion evolution for scenario $i$.

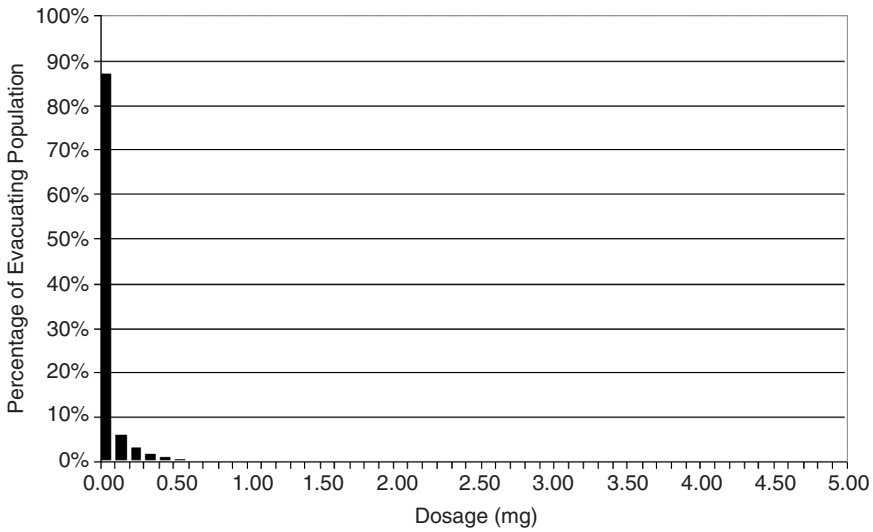



**FIGURE 2** Population dosage distribution for scenario $i$.

$EF_j$ and $ED_j$ can be determined from that dosage profile, and these estimates would be observed with probability $p_j$ (i.e. the probability of occurrence of scenario $j$). Repeating this procedure for all possible scenarios, a probability distribution of EF and ED can be constructed, which would represent the outcomes of the alternative under consideration (in this case, the "do-nothing alternative"; or in other words, evacuate under day-to-day network operation conditions).

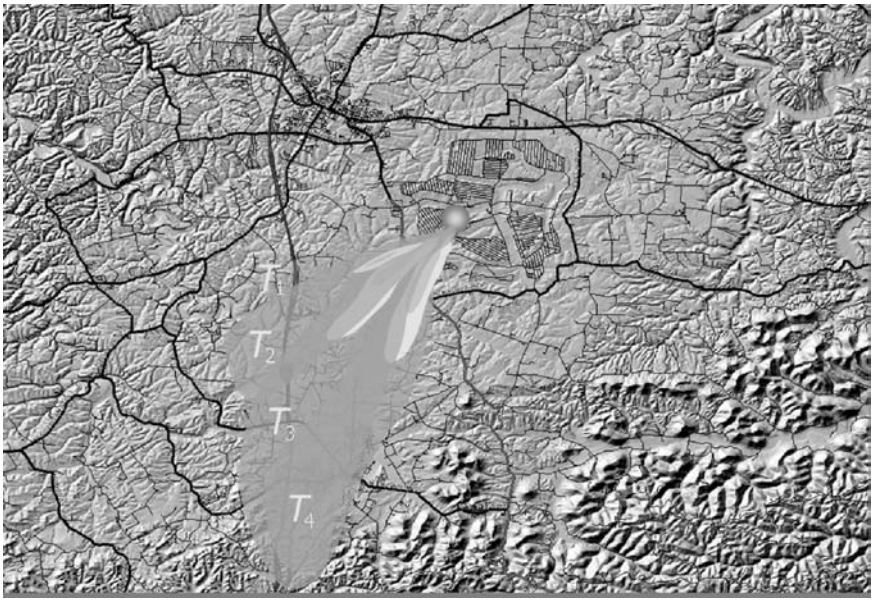



**FIGURE 3** Plume dispersion evolution for scenario $j$.

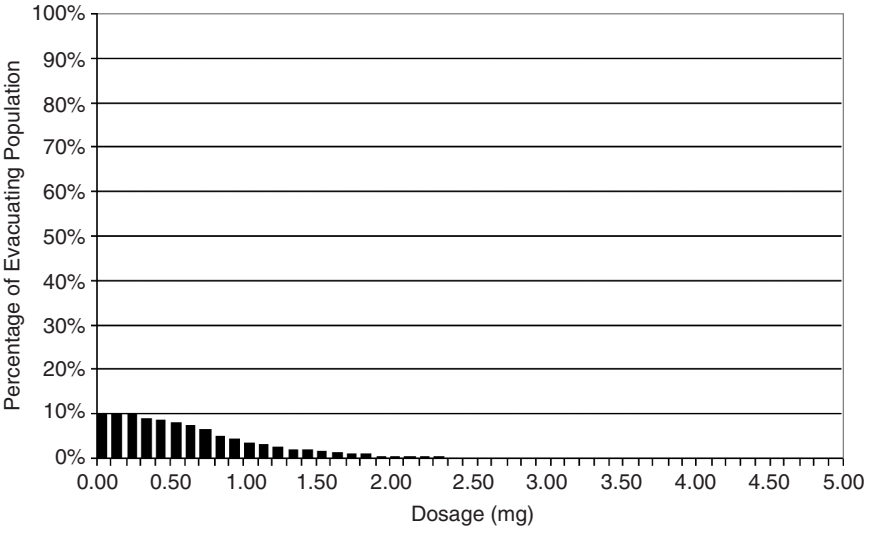



**FIGURE 4** Population dosage distribution for scenario $j$.

Figure 4 also shows that the exposure of the population to the agent under scenario $j$ is larger than that of scenario $i$. Of course, this dosage profile also depends on the type traffic management strategy deployed. So, if Figure 4 represents the dosage profile for scenario $j$ under a "do-nothing" evacuation strategy, a "reverse-lane" strategy may change that profile to one that could be closer to that of Figure 2, if, for example, the

evacuation time under this new strategy is reduced enough so that the population is outside the dangerous area before the plume reaches it.

## 4 EVACUATION OPERATIONS

Independently of the methodology used to determine the feasibility of an emergency evacuation as a protective action alternative, if the threat under analysis materializes then the planned strategies (the arterials/freeway segments that would operate in a reverse-lane fashion, the intersections that would be controlled by security personnel, etc.) have to be implemented. Even with the best tool to evaluate every possible traffic strategy and to create an efficient evacuation plan, it is not possible to anticipate what will actually happen during the evacuation. Because of this, it is necessary to collect, in real-time, traffic and road condition information to support the emergency evacuation operations' decision-making process and to keep informed the evacuating population.

During an emergency evacuation, continuous information on traffic conditions must be collected in order to assess the progress of the evacuation and to optimize evacuation operations to ensure the safety of the population. Where deployed, ITS can provide real-time traffic information. However, the coverage of this type of infrastructure is mostly restricted to large metropolitan areas, and in the majority of these cases only on freeways, with just a few urban areas having also arterial coverage. As mentioned previously, research is being conducted to provide real-time traffic information where there is no infrastructure deployed.

In order to evaluate how the evacuation plan is performing, the traffic simulation models used to develop the deployed traffic management strategies must be able to accept real-time information from the field. Where the traffic is flowing normally, this real-time information is compared to the traffic conditions obtained from the traffic simulation to determine if the evacuation plan is proceeding according to predictions. If the evacuation is not proceeding as planned,—for example, the evacuation time under current conditions will be longer than predicted—and there is a risk that bad weather, or any other conditions related to the disaster that triggered the evacuation may endanger the life of travelers or state officials in the field (highway patrolmen, Department of Transportation (DOT) personnel, etc.), then the traffic simulation model can be used to analyze and evaluate new traffic strategies. An example of such strategy is traffic rerouting in an attempt to expedite the evacuation. The same approach is used when an incident is detected. If the evolution of the threat has to be taken into consideration, then the complexity of the operations increases significantly.

Obviously, to implement these new strategies it is necessary to provide information to the public in the areas affected. This is a difficult task since at the present time it is almost impossible to communicate detailed routing instructions to a large pool of drivers as it would be required to adapt new traffic management strategies in real-time. New technologies such as those proposed under the US DOT VII (Vehicle-Infrastructure Integration) initiative [28] will one day make possible not only to get field information in real-time, but also to communicate instructions to drivers in a hazardous area. In the meantime, one of the few options to deploy on-the-fly rerouting strategies on the field is to manually control the traffic at key intersections.

## 5 NO-ADVANCE NOTICE EVACUATIONS

There are many situations in which it is possible to plan in advance for an emergency evacuation. Those scenarios include, for example, an explosion at a chemical processing facility or a radiological accident at a nuclear plant. In these cases, if an accident or a terrorist attack were to happen, then the best evacuation plan for the prevailing network and weather conditions would be deployed. As discussed previously, during the deployment or implementation phase, traffic conditions, collected in real time, would provide feedback information to some command and control center to permit assessing whether operations are proceeding as planned or if changes are needed to assure the safety of the evacuating public. Ideally, these evacuation plans, as well as other protective action measures, are developed ahead of time in preparation for such an event. As a result of these plans, long-term improvements to the transportation network may be undertaken to maximize the safety of the population. These types of situations are mainly characterized by the static nature of the potential source of the disaster (i.e. the facilities where an accident or an attack could happen are at fixed locations), or by the predictability of the threat (e.g. coast areas subject to hurricanes).

In other instances,—for example, the derailment of a train transporting hazardous materials—there may not be any previously developed plan to be implemented and decisions must be made *ad hoc* on if and how to identify and proceed with the best course of action to minimize losses. Those scenarios have two characteristics that make the analysis particularly difficult. The first one is related to the location of the event, which, by its very nature, does not have a particular location and it can happen anywhere in the nation. The second characteristic is that the type of event requires any mitigating strategy to be deployed within a very short window of time after the event has been identified. These two characteristics impose a heavy tax on any analytical tool used to support the decision-making process, since the tool has to be able to generate outcomes of all the possible strategies within a very short notice and with no advance groundwork.

Research has been conducted in this area [26, 27] to develop a prototype decision tool that can provide within a very short notice the inputs—both the demographic and the transportation network models—for the traffic simulation model. After the IRZ and PAZ have been identified either by the user of the tool or by a threat evolution model, a network creation module generates, in real-time and almost without human intervention[2], the topology and attributes of the transportation network for those cases in which this information cannot be extracted from existing databases. The network capacity attributes, particularly the traffic control settings, are generated using stochastic models that are based on information collected by the US DOT Federal Highway Administration. At the same time that the transportation network is being generated, a demographic model of the population within the at-risk area is built using information derived from LandScan USA for the region surrounding the event. This information consists not only of the spatial distribution and size of the population to be evacuated, but also of what is known as *mobilization curves*.

[2]Some human intervention is always required to resolve some inconsistencies and connectivity issues in the transportation network.

## 6 CONCLUSIONS AND RESEARCH NEEDS

The evacuation of large populations due to either natural or man-made disasters is a very complex problem involving many different issues, both technical and institutional/jurisdictional. This paper concentrated on the former and discussed the critical components that are necessary to plan for and implement a large-scale vehicular evacuation.

Two basic models are required to determine the feasibility of evacuation as a protective action alternative: a demographic and a transportation network models. The demographic model covers many aspects of the population within the potential area at risk, including its spatial distribution, reaction times (or mobilization times), selection of intermediate and destination points, and other information. All this provides the demand-side of this problem; the capacity side involves the information about the transportation network, including geometry, topology, traffic signal settings, and other traffic parameters. As discussed here, at the present time only a subset of scenarios can be modeled with reasonable accuracy, and although this field of research has received considerable attention after 9/11, much remains to be done.

The spatial distribution of the population during the daytime is still an issue that needs to be resolved, although substantial research is being conducted in this area. Mobilization times (or reaction time) of the affected population strongly depend on the type of disaster being analyzed and are only known, with certain accuracy, for very few of them. Little is known about the selection of destinations and intermediate stops during an evacuation and the relationship, from a behavioral point of view, of these choices to the type of event. The congestion patterns that would develop during an evacuation are tightly related to this demographic information making it crucial for the analysis of these problems.

Work is also required in relationship to the capacity side of the problem; that is, the definition of the characteristics of the transportation network. The determination of these characteristics is a lengthy process and one that does not end once the evacuation plans have been developed. Those plans are intimately related to the topology (i.e. connectivity) and capacity (number of lanes on each roadway segment, traffic control settings, etc.) of the transportation network and require constant update if they are going to be useful when needed. Some research is being conducted in this area to simplify both the creation and update process of the transportation network information, but there are areas that need further research, especially those related to the gathering of relevant traffic parameter information that cannot be found on GIS databases or determined through remote sensing technology (e.g. information about traffic control settings).

Once all the relevant information has been gathered, the evaluation of the proposed alternatives and traffic management strategies to be deployed during an evacuation requires the usage of a simulation model. Traffic simulation software has been available for many decades now to analyze general (i.e. day-to-day) traffic operation problems. Even before 9/11, some of these models (e.g. OREMS) have been specifically adapted to study and evaluate vehicular evacuations, and after 2001 other general purpose traffic simulation models have been used for the analysis of these types of problems.

Many issues still remain to be addressed in this area. One of the most important ones is related to the modeling of multimodal evacuations, including not only transit but also

pedestrian flow modeling and the interactions between pedestrians and vehicles that can arise under certain scenarios (e.g. evacuation sport venues located in downtown areas). The validation of these new models, and even the existing ones, for their use in assessing emergency evacuations is also a task that remains mostly unfinished.

Although, threat evolution models are somehow used in the modeling process (at least to determine the EPZs), the integration of these models and traffic simulation models is necessary to correctly evaluate alternatives under some scenarios. The typical decision variable to assess emergency evacuation plans (i.e. ETTE) may not be the correct measure to analyze certain problems, since there may be certain cases in which alternatives with shorter ETTE may have larger expected casualties than other ones with higher ETTE.

All these issues are related to the planning phase of emergency evacuations. If the evacuation plans need to be deployed, then real-time traffic information needs to be collected to determine whether the evacuation is proceeding according to plan or any changes are required. If changes are needed (almost a certainty), then availability of real-time information distribution is also required. Some efforts are underway to provide this type of capabilities until systems such as the ones proposed under the VII initiative are fully deployed.

## REFERENCES


1. Franzese, O., and Han, L. (2002). Using traffic simulation for emergency and disaster evacuation planning. *Presented at the 81st Annual Meeting of the Transportation Research Board*. Washington, DC, January 2002.
2. Franzese, O., and Han, L. (2001). A methodology for the assessment of traffic management strategies for large-scale emergency evacuations. *Proceedings of the 11th Annual Meeting of ITS America*. Miami, FL.
3. Dobson, J., Bright, E., Coleman, P., Durfee, R., and Worley, B. (2000). LandScan: a global population database for estimating populations at risk. *Photogramm. Eng. Remote Sens.* **66**(7), 849–857.
4. Dobson, J., Bright, E., Coleman, P., and Bhaduri, B. (2003). *LandScan2000: A New Global Population Geography, Remotely-sensed Cities*. V. Mesev (Ed.). Taylor & Francis, London, pp. 267–279.
5. Bhaduri, B., Bright, E., Coleman, P., and Dobson, J. (2002). LandScan: locating people is what matters. *Geoinformatics* **5**(2), 34–37.
6. Sorensen, J. H. (1991). When shall we leave? Factors affecting the timing of evacuation departures. *Int. J. Mass Emerg. Disasters* **9**(2), 153–165.
7. Rogers, G. O., and Sorensen, J. H. (1988). Diffusion of emergency warning. *Environ. Prof.* **10**, 281–294.
8. Baker, E. (1991). Hurricane evacuation behavior. *Int. J. Mass Emerg. Disasters* **9**(2), 287–310.
9. Davis, S., and Diegel, S. (2007). *Transportation Energy Data Book: Edition 26, ORNL-6978*, Oak Ridge National Laboratory, Oak Ridge, TN.
10. Franzese, O., and Xiong, D. (2001). Maintaining large-scale emergency evacuation traffic networks using remote sensing and GIS. *Presented at the GIS-T 2001 Conference*. Virginia, April 2001.

11. Franzese, O., and Xiong, D. (2001). *Emergency Evacuation Plans and Remote Sensing Information: A Demonstration Project for the Sequoyah Nuclear Plant in Hamilton Co. TN*. Oak Ridge National Laboratory, Oak Ridge, TN.
12. Carruthers, D., Holroyd, R., Hunt, J., Weng, W., Robins, A., Apsley, D., Thompson, D., and Smith, F. (1994). UK-ADMS: a new approach to modelling dispersion in the earth's atmospheric boundary layer. *J. Wind Eng. Ind. Aerodyn.* **52**, 139–153.
13. AERMOD, http://www.epa.gov/scram001/dispersion_prefrec.htm#aermod. Site accessed on September 30 (2007).
14. Hoel, D. (1992). *PFPL, Puff-Plume Atmospheric Deposition Model*, ESTSC—000205D078000; NESC—9800. Savannah River Laboratory, Savannah, GA.
15. HPAC (Hazard Prediction and Assessment Capability model), http://www.dtra.mil/newsservices/fact_sheets/display.cfm?fs=hpac. Site accessed on September 30 (2007).
16. SLOSH (Sea, Lake, and Overland Surges for Hurricanes), http://www.fema.gov/plan/prevent/nhp/slosh_link.shtm. Site accessed on September 30 (2007).
17. Luettich, R., Westerink, J. J., and Scheffner, N. (1992). *ADCIRC: An Advanced Three-dimensional Circulation Model for Shelves, Coasts, and Estuaries*, Report 1: Theory and Methodology of ADCIRC-2DDI and ADCIRC-3DL, Coastal Engineering Research Center, Vicksburg, MS, http://www.smast.umassd.edu/Fisheries/modelerFV/aboutFVCOM.php. Site accessed on September 15, 2008.
18. FVCOM (Finite-Volume Coastal Ocean Model), http://www.codfish.smast.umassd.edu/FVCOM.html. Site accessed on September 15, 2008.
19. Franzese, O., and Zhang, L. *Real-time Traffic Information for Emergency Evacuation Operations*, Project sponsored by MS DHS through the South East Regional Research Initiative (SERRI). ORNL, Project currently underway.
20. Federal Highway Administration (2007). CORSIM (Corridor Simulation Model), http://www.smast.umassd.edu/Fisheries/modelerFV/aboutFVCOM.php. Site accessed on September 15, 2008.
21. VISSIM, http://www.english.ptv.de/cgi-bin/traffic/traf_vissim.pl. Site accessed on September 30 (2007).
22. Franzese, O., Joshi, S., and Banerjee, H. (2003). *OREMS 2.6 User's Guide*. Oak Ridge National Laboratory, Oak Ridge, TN.
23. Willis, A., Kukla, R., Kerridge, J., and Hine, J. (2001). Laying the foundations: the use of video footage to explore pedestrian dynamics in PEDFLOW. In *Pedestrian and Evacuation Dynamics*, M. Schreckenberg, and S. D. Sharma, Eds. Springer, Berlin, pp. 181–186.
24. Helbing, D., Farkas, I., Molnar, P., and Vicsek, T. (2001). Simulation of pedestrian crowds in normal and evacuation situations. In *Pedestrian and Evacuation Dynamics*, M. Schreckenberg, and S. D. Sharma, Eds. Springer, Berlin, pp. 21–58.
25. Blum, J., and Eskandarian, A. (2004). The impact of multi-modal transportation on the evacuation efficiency of building complexes. *Proceedings of the 7th International IEEE Conference on Intelligent Transportation Systems*, Washington, DC.
26. Franzese, O., and Sorensen, J. (2004). Intelligent consequence management: dynamic weather information for the emergency evacuation component. *Proceedings of the ITS America 14th Annual Meeting*. San Antonio, TX.
27. Franzese, O., and Sorensen, J. (2004). Fast deployable system for consequence management: the emergency evacuation component. *Proceedings of the 2004 ITS Safety and Security Conference*. Miami Beach, FL.
28. Vehicle-Infrastructure Integration (VII) Initiative, http://www.its.dot.gov/vii/. Site accessed on September 30 (2007).

# EMERGENCY TRANSPORTATION OPERATIONS AND CONTROL

VINCENT PEARCE
*U.S. Department of Transportation, Washington, D.C.*

## 1 OBJECTIVES

Here we address three of the important objectives to consider when carrying out emergency transportation operations. The first is to obtain the necessary situational awareness. Situational awareness is the phrase used to describe having sufficient information and understanding in order to make and carry out decisions. Typically situational awareness requires information with three characteristics: timeliness, accuracy, and completeness.

Planning and decision making occur based upon the information obtained through situational awareness. Often the necessary decisions are multifaceted and may require the support of tools, models, simulations, or other products that analyze the data and provide feedback in a manner or form that makes it usable to decision makers and to those who will then implement the decisions.

Carrying out the decisions should result in influencing the behavior of the population and the responders. This means that decisions must include not only the desired outcome, but also the manner in which it will be communicated to achieve the desired outcome. In some cases, the action desired is communicated directly, such as by changing the timing of traffic signals. In many other cases, the action desired is also communicated indirectly. This is being achieved through sharing information in a manner that persuades the population to take the desired actions, such as traveling at specific times and along specific routes.

A possible additional objective, typically not separated from the others, is the ability to modify the chosen strategy after it is implemented on the basis of the results and changing conditions. This capture and consideration of feedback from the actions occurs at many levels, from the most strategic consideration to the finest tactical action.

## 2 REQUIREMENT

The requirements of an emergency transportation operations program begin with monitoring the transportation conditions. This includes both the status of the infrastructure/systems and the operational conditions. The information needs to arrive in real time and needs to be capable of being converted to usable form. Raw output from many of the sensor systems available is not usable. Further, the information needs to be filtered, as there is potentially far too much information to absorb and to choose from for the operators. The varying types of information may need to be integrated or "fused" in order for

the decision makers to comprehend what is often referred to as the *common operational picture*. The preexisting information, such as the characterization of the roadway itself, also needs to be in a usable form, so that operational conditions can be overlaid upon it, impacts understood and predicted, and alternatives identified and analyzed.

Tools to support the decision-making process need to be capable of working in the kind of environment that will exist in emergency operations. Typically, one of the most critical features is the ability to process quickly. Models that take hours to run are of little use. Once processed, the output needs to be expressed in manners that are easily understood by an audience with a widely varying level of technical expertise. Often, critical decisions such as when to initiate an evacuation order are passed on to elected or senior appointed officials who may have no grasp of the technical fundamentals at all. Making the output usable may also require the ability to integrate the output with other data, either output from other processes or actual real-time data, a further form of "fusion."

Influencing the behavior of the responders is relatively easy in a classic command and control environment; they are given direction and they proceed using the training, information, and tools that they have received. Influencing the behavior of the general public is considerably more challenging. Much of this is achieved by informing the public of the situation, the decisions, and the likely conditions, and providing such recommendations as may make sense. Classic examples include sharing information on shelter and hotel availability and on road conditions to potential evacuees. The end objective is to get the evacuees from a specific area to take specific routes to specific shelters, thus making effective use of the transport and shelter capacity that is available, while perhaps also sustaining some transport capacity for responders as well. Under normal emergency operations conditions, it is essentially impossible (and may thus be unrealistic) to force evacuees onto specific routes. Particularly in situations where the population would be evacuating from their work locations due to an unexpected incident, planning assumptions such as "everyone in the southern half of the city will evacuate south" may be totally unrealistic, due often to family commitments, that may cause evacuees to actually move closer to the hazard they flee away from it.

The requirements necessary in order to control and direct the population's actions, to the degree possible, are often technology driven. The tools used to control traffic, whether on roads or on other modes of transport, are typically composed of electronic and electromechanical devices. In situations where such devices do not exist, or where actions are needed that are outside the available working parameters of the existing equipment (such as a signal timing plan that has not been loaded into the necessary signal controllers), it may be necessary to place temporary devices such as signs, or even humans, into the operating environment to carry out the direction and control. The effectiveness of the technology depends, as it does every day, upon the technology's flexibility, speed, accessibility, and other design and operational factors.

## 3 MODES OF TRANSPORTATION

Technically, all modes of transport can be and periodically are applied to emergency transportation operations. For example, while planning evacuation for the 12 most impacted parishes in southern Louisiana, the heaviest transportation components are road, rail, transit, and aviation. Maritime has also figured in the evacuation, not only in New Orleans

but also in moving people out of New York City following the 9/11 attacks, and later when the blackout of 2003 struck.

Obviously, each mode has its unique characteristics. Some modes are owned and operated by government agencies, some by pseudogovernment entities, and others by the private sector either for their own profit or under contract to government. Each mode is regulated differently and each has its own command, control, and communications structure. Capabilities may also vary considerably from one jurisdiction to another.

It is particularly important to remember that all modes may be at play, or may have something to offer in planning for and carrying out emergency transportation operations, and that allowances must be made for the uniqueness of each. Integration between modes, or at least reasonable synchronization and coordination of actions by different modes, is vital. For example, instituting contraflow travel, in a manner that stops evacuation buses from returning to pick up additional evacuees, or slows down the progress of busloads of evacuees being taken to train stations or airports is a dangerous outcome of poor coordination. Post-Katrina evacuation planning in Louisiana has highlighted the importance of intermodal connections, as well as intramodal connections such as when school buses bring evacuees to a pickup point, where motor coaches then board and take them to further destinations.

## 4 EMERGENCY TRANSPORTATION OPERATIONS ON HIGHWAYS

When it comes to determining how to carry out emergency operations, roadways are often classified into two fundamental categories: controlled access and uncontrolled access. Which of these two categories describes a given roadway has a significant influence on the emergency transportation operations strategies that can be carried out on that facility.

Controlled access facilities, such as interstates, ordinarily allow the free flow of traffic with few controlling devices. Ramp meters can control access to the facility, but other than high occupancy vehicle lanes with either indicators or possibly gates, most controlled access facilities allow a free flow of the traffic. Thus, if emergency operations dictate that changes in traffic flow on the controlled access facility are needed, manual intervention combining information and signs/barrels/cones/personnel will be required. An excellent example is contraflow, where vehicles are allowed to travel "the wrong way" on highways that have been closed to and cleared of traffic desiring to travel in the "normal" direction. Strict measures are necessary to control the ability of motorists to get on to and off of the contraflow lanes, as well as considerable information to allow the motorists to operate safely and efficiently in an operating environment that is totally unfamiliar (it has been remarked that driving in a contraflow situation is somewhat disorienting).

Uncontrolled access facilities such as typical city streets allow many more tools, particularly traffic signals, which help to carry out emergency transportation operations. Within limits, traffic signal timings facilitate control of flow speed and volume in each direction, including even potential ingress to and egress from the facility. Signals may have limited impact; however, as congestion builds up, travel conditions exert a greater influence on speed and throughput than the signal timing itself does during free flow conditions. In the extreme, conditions may develop where ordinary signal timing, operating under far-beyond-saturation conditions of an evacuation, may stimulate unpredictable motorist behavior, such as violating red lights deliberately after excessive wait periods.

## 5 TECHNOLOGIES

There are many forms of technology that can support emergency transportation operations. Sensors are available using many different technologies to feed into situational awareness. Each sensor technology has its own unique characteristics, influencing how the technology is deployed and operated and the data it produces. Consideration of temporary, portable sensors that can be quickly put into place and then removed before an incident with advance notice, such as a hurricane, may also be worthwhile. There have also been demonstrations of the use of vehicles themselves, or items that they contain such as cellular telephones, which allow the vehicles to serve as probes in the traffic stream, thus relaying similarly useful information on travel speed and incident locations.

Video surveillance is an increasingly important tool in emergency transportation operations. Again, many different forms of video devices are available, not all compatible with one another, and each with possible limitations on how it can be applied to gathering the necessary understanding. Video should be viewed as a system; cameras without controllers, communications, and displays are useless. The way in which a video system is installed, for example, may limit its utility. If a camera has been installed for use in documenting red light violations, its positioning may not support the longer and broader view of traffic that is desired in assessing localized traffic flow conditions. Again, temporary, portable options may be available for uninstrumented areas.

Decision-making support systems and tools are essential to making quality decisions in a timely manner. Unfortunately, many of the current models were developed for use under nonemergency conditions and for very different objectives. Loading the models can be time-intensive, particularly if the conditions have changed significantly from the baseline. Running "what-if" scenarios, to evaluate multiple alternatives is an important capability. Information on current traffic analysis tools work by the US Department of Transportation's Federal Highway Administration (FHWA) can be found at http://www.ops.fhwa.dot.gov/trafficanalysistools/index.htm.

There is a good variety of traveler information tools. Some tools are focused on pretrip traveler information and others focus on en route information. Each type of system typically has limits, though, on the amount and type of information that it can deliver. Misusing a traveler information technology can by itself create hazardous conditions substantially. Imagine the disruption to traffic flow created by motorists traveling at 70 miles/hour trying to read four panels of text on a variable message sign. As with any tool, such systems can work well and be used effectively, or can fail to meet expectations. Early traveler information radio systems have been criticized as difficult to understand. Other challenges may exist, such as communicating effectively to drivers to whom English is not a primary language, or drivers who are unfamiliar with the area through which they are passing. Similarly, onboard navigation systems may find it difficult to develop and provide useful directions when typical routes have been limited or closed. Excellent resources from FHWA on traveler information systems and program are available at http://www.ops.fhwa.dot.gov/travelinfo/index.htm.

Traffic signals have evolved substantially since the days of Garrett Morgan and they continue to improve. Their flexibility and capacity to handle complex and numerous timing plans, and to make their own decisions based on developing flow conditions support their inclusion into emergency transportation operations plans. However, there are still many traffic signal systems in place with earlier and much more limited

technology, so the effectiveness of emergency transportation operations may be limited. More details about the work the FHWA has done on traffic signal systems are available at http://www.ops.fhwa.dot.gov/arterial_mgmt/traffic_sig.htm.

Reliable high-speed communication is fundamental to receiving the information and controlling the devices, as well as to coordinating across multiple systems, modes, and jurisdictions. Many options exist, but interoperability is key. Good design practices (such as building in redundancy and upgradeability) are essential to gain the most from a possibly significant investment. During disasters, communications systems may be overloaded or damaged, perhaps limiting the agency's ability to remotely modify the traffic control devices. The results of over a decade of work on telecommunications and transportation can be found at the website of the USDOT Intelligent Transportation Systems Joint Program Office, http://www.its.dot.gov/telecom/index.htm.

Traffic barriers, once limited to cones and barrels, now include automated gates, barriers that store below ground, and barrier systems that can be moved by specialized vehicles. These options may allow considerably a more rapid reconfiguration of traffic and roadways than would be possible manually and with greater safety as well. Even simple measures, such as having mapped out in advance where barriers will be implemented and pre-staged, the barrier materials can reduce considerably the time necessary to implement these measures, and to remove them before the arrival of tropical storm force winds.

## 6 CHALLENGES

Not surprisingly, those conducting emergency transportation operations face numerous challenges. For example, during and after the incident, transportation may need to be carried out on impact facilities; thus, they end up working under degraded conditions. Capacity may be reduced, additional hazards may exist, and devices may be impaired. Unfortunately, the transportation technology may be least functional when its assistance is most needed.

Decision quality is strongly influenced by the information that operators have, and frequently information is either imperfect or inadequate. Much of the information may be based upon models and observations, either of which may have limited fidelity. Risk is also a factor, so understanding how a risk changes with time is also important.

Coordination across jurisdictional boundaries is always challenging. For example, inland states may be hesitant to accept a free flow of evacuees who are receiving their guidance from coastal states anticipating tropical storm conditions. In other types of situations, the evacuees may, in fact, present a hazard, if for example, they have been contaminated or are contagious due to chemical/radiological and biological situations, respectively.

The political decision-making process/timeline may not work as rapidly as would be desired. There will be considerable hesitancy to make major decisions such as calling for an evacuation because of the economic impacts, and even possibly due to the impacts on resident health and safety. Evacuations are difficult particularly for persons who are hospitalized, so evacuation decisions are typicallymade very cautiously.

Resource shortages may impact the ability to conduct emergency transportation operations. If local law enforcement normally conducts traffic, but they are diverted to higher priority law enforcement missions, a major gap exists in the ability to dictate (and report) what traffic is doing.

Coordination within the overall response can be quite challenging. For example, assuring that victims picked up by search and rescue services are brought to locations from which they can be evacuated is critical. Similarly, transportation plans during an evacuation are strongly influenced by shelter availability and the knowledge of shelter availability. Poorly coordinated decisions can worsen, instead of improving, the situation.

Coordination between modes of transport is fundamental. If an evacuation by air is planned, adequacy of and coordination with transport to/from the airports are critical. Individual modes may be impacted by the disaster, not all at the same time. For example, it is important to know when airlines plan to stop flying into an airport that is in the path of a hurricane. On a smaller scale, movement of motor coaches and trucks across a bridge or a similarly exposed area may also be limited as wind speeds increase or as weather conditions worsen.

It is almost assured that, unfortunately, incidents will occur during the emergency transportation operations. Thus, incident clearance—rapid and efficient, is a vital component of emergency transportation operations. Clearance is only one component of overall incident management, which is itself an effort involving multiple agencies, each with its own priorities, objectives, technologies, and systems. Fortunately, the FHWA has been working diligently on improving traffic incident management in a comprehensive manner for a number of years. You can find more information on their work on-line at http://www.ops.fhwa.dot.gov/incidentmgmt/index.htm.

Fuel shortage, often caused by lack of electrical power, can strongly influence the process of evacuation. Impact comes not only from vehicles that run out of fuel, but from motorists who leave and reenter the traffic stream frequently attempting to obtain fuel at one station after another. Of course, fuel for the response vehicles is also a critical resource. The impact of fuel shortage may extend beyond the transportation, fire, and police department's vehicles. Fuel support to an evacuation fleet of hundreds of motor coaches and school buses is an even greater undertaking.

Unpredictability of transportation demand is a serious challenge. The first major hurricane to hit the United States after Hurricane Katrina was Hurricane Rita. With the memory of the devastation of Katrina fresh in their minds, thousands more Texans evacuated than any model predicted, resulting in impossible traffic volumes and all of the other problems that come with them.

## 7 IMPROVING THE WAY FORWARD

Clearly, technology is fundamental to successful emergency transportation operations. The technology can help resolve, but can also in some cases actually cause, some of the complex issues that transportation managers face. Several actions can help to bring progress in the area:

Continued improvement of models and simulations, particularly focusing on emergencies and disasters, will be highly beneficial.

Enhanced integration of data and of systems facilitates achieving the understanding necessary for decision making.

Lower cost systems support wider implementation.

Improved portability, through less weight and lower power consumption or alternate power sources (solar) will assist in temporary implementation for areas under construction and areas that do not have fixed systems for other reasons.

Improving the ability of the technology to withstand the rigors of disaster conditions improves the likelihood that the technology will be working when it is most needed.

Increased flexibility of technology to deal easily and rapidly with changing conditions makes it possible to "stay ahead of the curve" instead of constantly being caught behind the latest condition or forecast, or worse yet, having to supplement the technology with the very limited available manpower.

Improved representation of the data, in formats and forms focused on decision makers will help get the best decisions made as quickly as possible.

The ability of technology to support multiple modes of transport and across jurisdictional boundaries will facilitate coordination. Principles such as interoperability and the ability to share and integrate data can be major contributors to progress in this area.

# ULTRA-SCALE COMPUTING FOR EMERGENCY EVACUATION

BUDHENDRA BHADURI, JAMES NUTARO, CHENG LIU, AND THOMAS ZACHARIA
*Oak Ridge National Laboratory, Oak Ridge, Tennessee*

## 1 INTRODUCTION

Disasters impose a high level of risk on human lives within a physiographic space and evacuation is the physical movement of the population at risk to safer locations. In a broader sense of that definition which includes situations relevant to homeland and national security, emergency evacuations may occur in a variety of physiographic spaces such as passenger vessels in accidents (airplanes, trains, buses, and ships), buildings (and facilities) on fire, as well as large geographic areas (multiple counties) impacted by natural (hurricanes, floods, volcanic eruptions) or technological disasters (atmospheric dispersions of harmful gaseous agents). In all of those situations, modeling the evacuation process involves accounting for the number of people, the available evacuation routes and transportation modes (pedestrian, vehicular), and, most significantly, the behavioral characteristics of the evacuating population. High resolution databases are becoming available at an increasing rate which in turn facilitates development and incorporation of detailed behavioral processes in evacuation models. Computational complexity can originate from increasing resolutions in data (population and transportation), which increase the number of entities to be modeled, or from increasing complexity in the evacuation behavior represented in the models. Here, we focus the discussion on vehicular evacuation

of large geographic areas since this scenario potentially involves the initial complexity of large volumes of input data and consequent compounding of that complexity by the many individual and traffic behavioral processes that can be represented in the evacuation model.

The goal of this article is to provide a new perspective on the potential role of ultra-scale simulations, which require beyond single desktop processing of data, and execution of algorithms on hundreds or thousands of parallel processors in the context of existing approaches for evacuation modeling. In the subsequent sections, we propagate the use of ultra-scale computing as an enabler of new emergency evacuation models that incorporate high resolution geospatial databases and relevant human behaviors. These "use cases" are contrasted with the present state of transportation modeling to highlight the primary challenges posed by our vision.

## 2 MOTIVATION FOR ULTRA-SCALE SIMULATIONS

The use of transportation network simulation for evacuation modeling has been in practice since the mid-1980s [1]. A number of existing transportation simulation models characterize the interaction between human dynamics and transportation infrastructure and require the integration of three distinct components, namely data, models, and computation. These include detailed physical models of transportation engineering, such as is found in CORSIM [2], TRANSIMS [3–5], VISSIM [6], PARAMICS [7], and OREMS [8, 9]. Very recently, a few models have started to address the human dynamics of physical and social systems, such as Repast/Mason [10] and SEAS [11, 12].

However, none have been able to successfully integrate both the physical as well as behavioral aspects to characterize the interdependencies within the transportation systems. Progress has also been limited by data and computational challenges necessary for accommodating the required high resolution along spatial, temporal, and behavioral dimensions. With the exception of TRANSIMS [13, 14], no other model has demonstrated the aspect of ultra-scale simulations.

There are a few plausible reasons behind the apparent lack of motivation to develop beyond-desktop simulations for transportation or evacuation models. First, the lack of high resolution primary databases for transportation network and other infrastructure assets such as traffic lights and controllers; spatially explicit demographic attributes; and other critical infrastructural features such as schools, hospitals, banks, and so on, that would provide large volumes of data and therefore impose a high level of computational complexity, have only been available to the modeling community in the last decade. Moreover, evacuation modeling has traditionally been a component of emergency preparedness and planning rather than an operational tool. Estimation of evacuation time for an area given network availability, or determination of evacuation routes given available time for evacuation have been the primary applications of evacuation modeling and simulation. However, there are a couple of reasons for which evacuation modeling, even for planning purposes, can demand large-scale simulations.

First, let us consider the scenario of large-scale hurricane evacuation in the coastal states handled by divisions such as South Carolina Department of Transportation (SCDOT) [15], Louisiana Department of Transportation and Development (La DOTD) [16], and Florida Division of Emergency Management [17]. These states identify the state emergency evacuation routes that could be used for disaster situations. For the

reason of simplicity, their emergency evacuation plans only identify the state and federal highways as evacuation routes. Those plans are easy to understand and easy to follow. However, for realistic planning purposes, it would be more accurate if the street networks were also considered since the elimination of detailed street networks could lead to overestimation of the evacuation time.

For example, Figure 1 is a 3-mile distance circle around downtown Knoxville, Tennessee with only state and interstate highways. The yellow dots are the population distribution within this circle. If the evacuation plans consider only the highway networks, then there are just 36 exit points. Figure 2 is the same map with a higher resolution street network; it has 140 exit points. Therefore, many evacuees can escape from their locations within the evacuation area by utilizing local streets. However, since only the highways are designated as evacuation routes, both in models and in reality, the smaller streets remain underutilized hence adding to the total evacuation time. Another problem is that without the street network, it is difficult to estimate the local flow pattern and therefore, difficult to estimate the highway loading factor. The advantage of using only the highway network is that the data is small (it has 878 highway links in Fig. 1) and the model execution time is correspondingly diminished. On the other hand, a model using the street networks must deal with larger data (it has 7926 highway and local street links; Fig. 2); the local street network data is 10 times larger than highway data in the example above. Therefore an increased computational power is needed to solve this problem especially when the study area becomes large.

Second, the recent availability of very high resolution demographic and socioeconomic data has allowed development of detailed activity-based behavioral models that can be integrated with transportation simulations. For example, a plethora of household

**FIGURE 1** Intersection of the highway network and low resolution street data results in 36 exit points for a circular area with 3-mile radius around downtown Knoxville, Tennessee.

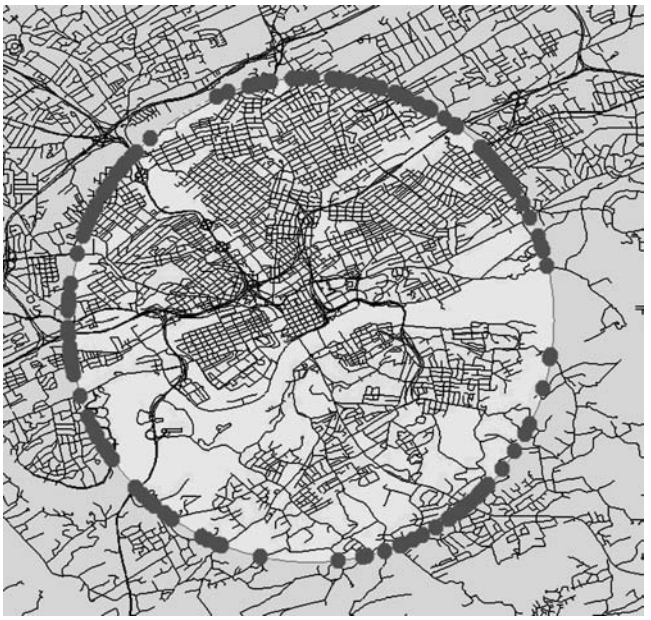


**FIGURE 2** Intersection of the highway network and a higher resolution street network data results in 140 exit points for a circular area with 3-mile radius around downtown Knoxville, Tennessee.

and microlevel data on socioeconomic and activity-based behavioral data have been collected and are disseminated primarily by the US Census Bureau and the Bureau of Transportation Statistics (www.bts.gov/data) of the US Department of Transportation. The American Community Survey (ACS) from the US Census is a new nationwide survey-based data on general demographic, social, economic, and housing characteristics. In addition, significant advancements have been made in developing very high resolution population distribution data through advanced spatial data integration and modeling through pycnophylactic [18], dasymetric [19] and smart interpolation [20] approaches. Among them, Oak Ridge National Laboratory (ORNL), as part of its LandScan Population Projects, has developed the finest resolution (1-km cell) population distribution model for the entire world [21], and an even higher resolution (90-m cell) for the United States, the latter including a time variant distribution of population [22, 23]. Such high resolution population distribution data, when combined with corresponding behavioral attributes, quickly provides a much-desired way to model individual (driver and other evacuee) behavior during evacuations and consequently adds computational complexity to large-scale simulations.

For example, explicit representation of various demographic groups in space and time provides a way to modify the simple Origin–Destination (OD) models in a transportation system. Figure 3 shows a daytime population distribution scenario of Washington, DC where some workers (parents) in downtown have their children attending schools across the river (southeast part of the figure). During an emergency, those parents are most likely to head toward their children before evacuating out in another direction. Such behavioral models become easy to formulate and integrate but add considerably to the computational complexity of evacuation scenarios. For successful emergency evacuation planning, assessing the effectiveness of possible planning strategies and discovering their

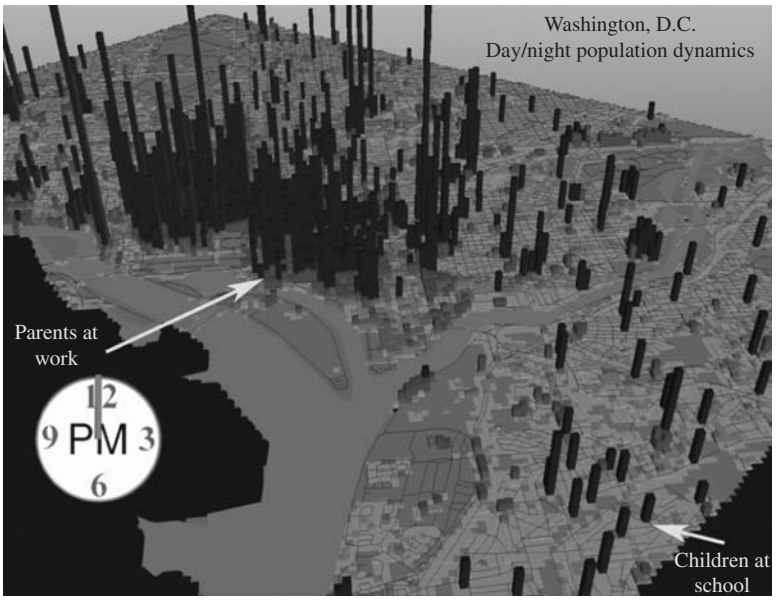



**FIGURE 3** Modeled daytime population distribution scenario for the Washington, DC area where some workers (parents) in the central business district are likely to move toward their children at school across the river (southeast part of the region) after a disaster.

unanticipated consequences can be achieved by data collection, modeling, and simulation at the finest data, process, and societal-response levels coupled with the system's behavior over large spatial and temporal scales. Modeling at this scale provides a strong impetus for ultra-scale simulations.

Finally, simulation execution time becomes a critical bottleneck when evacuation modeling needs to be implemented as an operational tool, either for short-term planning (i.e. days ahead) or to anticipate congestion quickly enough for simulation output to be used in real-time modifications of transportation network controls in order to optimize the flow of traffic. Such a modeling framework will require processing of dynamic data streams from a variety of sensor networks that can be used in description and updation of network status in real time as well as in calibration of the model outputs; in faster than real-time execution of the model to simulate emerging situations; and in evaluation of consequences of mitigation strategies to address the behavior of the system. No such modeling and simulation system exists today and it can only be developed by utilizing ultra-scale simulation frameworks.

## 3 MODELING APPROACHES FOR POPULATION MOBILITY

Evacuation models can be considered as a special situation where movement of people is expected to have certain directionality since the objective is to move the population residing inside a geographic area across and outside its boundary. This section describes and illustrates three approaches to building models of transportation systems that allow modeling of such population mobility. These approaches also represent the general methodological principles of moving vehicles along transportation networks. The

focus of this section is on microsimulations; the modeling techniques described here deal with individual vehicles. Although the approaches are presented separately, large microsimulations are unlikely to use a single approach and elements from each are frequently intermingled. For example, TRANSIMS uses both vehicle-oriented and cell-based modeling techniques in its microsimulation module [5]; MITSIM has elements of both link-based and vehicle-oriented models [24]. Nonetheless, the categories that are identified here represent three distinct elements of a transportation system: space, structure, and human behavior.

### 3.1 Spatially Oriented Models

Spatially oriented models of transportation systems focus on change as it is seen from a fixed vantage point. Cell-based models are one popular approach for constructing spatially oriented models. With this approach, the road network is divided into uniform squares called cells. Each cell has a set of attributes that describe the road type (e.g. a merging lane, freeway, surface street etc.), speed limit, direction of travel, the vehicle occupying the cell, and other items of interest. Every cell also has a set of rules that are used to change its state.

Simulation proceeds in one of two ways: time-driven or event-driven. In a time-driven simulation, the state of every cell is recomputed at regular intervals of time. This is done by sweeping through the cell space and applying each cell's transition rules. Conceptually, updates occur simultaneously at each cell; if a cell requires its neighbors' state to determine its own subsequent state then it uses the state of those neighbors at the previous instant of time.

In an event-driven simulation, the transition rules at a cell are applied only when specific event conditions are satisfied. For example, a cell that represents a freeway segment changes its state only when it, or its neighbor upstream, is occupied by a vehicle. Event-driven models have the potential for more accuracy than their time-driven counterparts; events can occur at any instant of time and are not restricted to the predetermined calculation points of a time-driven model. In principle, event-driven simulation can also reduce the amount of time that is needed to complete a simulation run by reducing the number of cells that must be updated. An event-driven simulation, however, requires considerably more supporting machinery (in the form of event-scheduling algorithms, activity scanning, event set management, etc.) than a similar time-driven simulation. Consequently, real gains in execution time or accuracy are contingent on the type of traffic problem that is being considered.

To illustrate this modeling approach, consider the single-lane road shown in Figure 4. The road is divided into uniform segments. Each segment is either occupied by a vehicle or it is not. A vehicle that occupies a cell has a speed $v$ and every cell has a maximum allowable speed $v_{\max}$. Every occupied cell also has a gap distance that is the number of cells separating the occupied cell from its next occupied neighbor, in the direction of travel. Each cell in this time-drive simulation has four rules for moving a vehicle [25]:

1. Accelerate. $v' \leftarrow \min(v + 1, v_{\max})$
2. Decelerate to avoid accidents. $v'' \leftarrow \min(v', gap)$
3. Randomize $v'' \leftarrow \max(v'' - r, 0)$ where $r$ is a random variable that yields 0 or 1 with a certain probability $p$.
4. Move. Advance the vehicle position by $v'''$ cells.

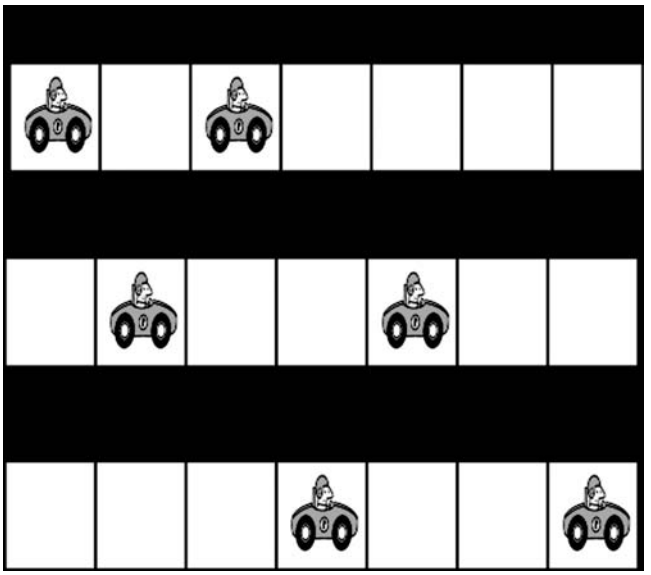


**FIGURE 4** Three time steps of a cell-based traffic model. The numbers above each vehicle indicate their individual speeds.

Figure 4 shows the motion of two vehicles over three time steps. The maximum speed in this example is two and neither vehicle undergoes random deceleration (i.e. $r$ is always zero).

### 3.2 Link-Based Models

Link-based models of transportation systems focus on the state of individual road segments within the road network. The major dynamic elements in a link-based model are road segments and intersections. Road segments are characterized by the road type, speed limit, number of lanes, occupancy limit, a speed-density function, and other attributes of interest. Interactions are characterized by control signals, permissible turning movements, and possibly other items. Vehicles move from link to link and some models also incorporate vehicle motion within a link (e.g. to permit midlink lane changes).

Links are commonly modeled as discrete event systems that act on at least two kinds of events: a vehicle arrives or a vehicle departs. Other events can be included to model congestion that crosses several links, traffic control signals, or special vehicle behaviors within a link. The queuing model developed by Gawron [26] is a good example of a link-based transportation model. Gawron's original model was designed for discrete-time simulation; a discrete event variation of it is presented here.

Every link in Gawron's model has four attributes: the free-flow speed $v_0$, the length $L$, the maximum number of vehicles per unit time $C$, the average vehicle length $l$, and the number of lanes $n_{\text{lanes}}$. When a vehicle enters a link that vehicle is assigned an earliest exit time $L/v_0$; this is the amount of time needed to cover the link distance at the best possible speed. Once the vehicle has traversed the link distance, it is placed into a queue. Vehicles in the queue are moved to the next link on their path at a maximum rate of $1/C$; the total time required for a vehicle to traverse the link is approximately $L/v_0 +$

*(Queue length)/C* where *Queue length* is the size of the queue when the vehicle enters it. A vehicle can advance to the next link when three conditions are satisfied:

1. the vehicle has advanced to the front of the queue;
2. the total number of vehicles in the next link is less than $L \cdot n_{\text{lanes}}/l$; and
3. conditions 1 and 2 have been satisfied for $1/C$ units of time while the vehicle is at the front of the queue.

Table 1 shows the first 10 iterations of a simulation of this model when applied to the traffic circle shown in Figure 5. A total of five vehicles enter the traffic circle: the first at time 2.5, the second at time 5, the third at time 7.5, the fourth at time 10, and the fifth at time 12.5. Each link has two lanes, a free-flow speed of 10 m/s, a length of 50 m, a maximum vehicle flow rate of 10 cars per second, and the average vehicle length is 7.5 m.

**TABLE 1 The First 10 Event Times in a Simulation of Five Vehicles in the Traffic Circle**

| Time | Link 1 | Link 2 | Link 3 | Link 4 | Link 5 | Link 6 |
|---|---|---|---|---|---|---|
| 2.5 | 1 | 0 | 0 | 0 | 0 | 0 |
| 5 | 2 | 0 | 0 | 0 | 0 | 0 |
| 7.5 | 3 | 0 | 0 | 0 | 0 | 0 |
| 7.6 | 2 | 1 | 0 | 0 | 0 | 0 |
| 10 | 3 | 1 | 0 | 0 | 0 | 0 |
| 10.1 | 2 | 2 | 0 | 0 | 0 | 0 |
| 12.5 | 3 | 2 | 0 | 0 | 0 | 0 |
| 12.6 | 2 | 3 | 0 | 0 | 0 | 0 |
| 12.7 | 2 | 2 | 1 | 0 | 0 | 0 |
| 15 | 2 | 2 | 1 | 0 | 0 | 0 |

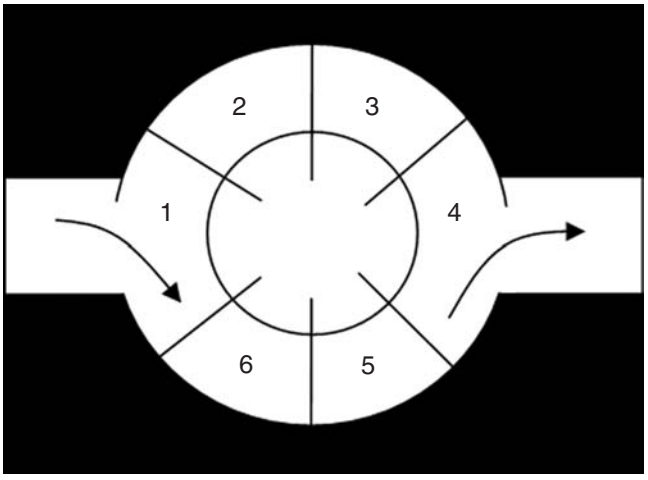



**FIGURE 5** A traffic circle that is modeled with six links.

### 3.3 Vehicle-Oriented Models

Vehicle-oriented models are constructed from the driver's point of view. The dynamic unit in a vehicle-oriented model is the vehicle itself; the driver of a simulated vehicle observes and reacts to his simulated surroundings. These types of models are attractive because they can easily incorporate models of the driver's decision-making processes and information technology that could influence driver behavior (e.g. digital maps, real-time traffic reports etc.).

The road network can be modeled just as in the link-based and spatially oriented modeling approaches. Elements of the road network, be they cells or links and intersections, have attributes that describe speed limits, road type, traffic signals, and other relevant items. It is frequently helpful to maintain a list of vehicles that occupy each part of the road network; this can simplify the calculations that are needed to model driver behavior by making nearby vehicles easy to find. The major difference between the vehicle-oriented approach and link-based or spatially oriented models is that the road network is acted on by the vehicles and not the other way round.

The car following algorithm that is used by MITSIM is a good example of a vehicle-oriented model [24]. In this model, the road network is represented as a graph with links and intersections. The simulation periodically (usually at 1-s intervals) updates the position, velocity, and acceleration of every vehicle. At each simulation update time, the driver of a vehicle observes his surroundings and changes his acceleration to either avoid a collision or reach a desired speed. In the car following regime, the acceleration is given by:

$$a = \alpha^{\pm} \frac{v_{lead}^{\beta^{\pm}}}{g^{\gamma^{\pm}}} (v_{lead} - v) \tag{1}$$

where $a$ is the acceleration, $v$ is the vehicle speed, $v_{\text{lead}}$ is the speed of the vehicle immediately ahead (i.e. leading), $g$ is the distance between this car and the leading vehicle, and the exponents $\alpha$, $\beta$, and $\gamma$ are parameters for calibrating the model ($a^+$ is an acceleration parameter and $a^-$ is used for deceleration). The vehicle speed and position at time $t + h$ is computed from its speed and position and the lead vehicle's at time $t$ by:

$$v_{t+h} = v_t + h\alpha^{\pm} \frac{v_{lead}^{\beta^{\pm}}}{g^{\gamma^{\pm}}} (v_{lead\ t} - v_t)$$

$$x_{t+1} = x_t + h v_t$$

where $x$ is the position of the vehicle relative to the start of its current link. Table 3 shows a simulation with this model of a car decelerating as it approaches the lead vehicle. The gradual approach of the following vehicle to a safe following distance is clearly apparent in the data.

The car following algorithm clearly differentiates this model from the previous cell-based and link-based models. The simulation is executed vehicle by vehicle, and individual vehicles may occupy any point on a link and perform arbitrarily complex maneuvers (e.g. MITSIM also includes lane changing, emergency breaking, and free-flow models that are influenced by the driver's perception of the current traffic conditions).

## 4 EXPERIMENTAL COMPARISON OF EXISTING MODELS

It is clear that the input data is easy to prepare and the model execution times are fast for macroscopic traffic simulations. Although the microscopic traffic simulation models take more time to prepare the data and need more simulation execution time, they generate more detailed information of the traffic flow conditions. However, microscopic models can vary, sometimes substantially, in their execution times and predictions of traffic flow even when given similar data. To illustrate this fact, we selected a macroscopic evacuation model, OREMS, and two open source microscopic traffic simulation models, MITSIM and TRANSIMS. Evacuation simulations with these models were run on a CPU (running Windows XP) with 3.79 GHz processor and 4 GB of RAM.

A set of artificial networks were generated to perform the comparison. The network was designed as a square matrix of cells. Each link was 1 mile long and the speed limit was 25 miles per hour. The horizontal nodes, the left-most and right-most were entry nodes and the vertical nodes, the top-most and bottom-most were exit nodes. The OD matrix was that each entry node had $n$ vehicles to every exit node. Figure 6 is a 10 $\times$ 10 matrix network with 100 vehicles from each entry node to every exit node. The total vehicles for each entry node is 800 vehicles because there are eight exit nodes. Figure 7 is a 16 $\times$ 16 matrix network with total 9600 vehicles for each entry node. Table 2 is the summary for all scenarios. For example, in the largest dataset scenario, 16 $\times$ 16 $\times$ 9600, there are 32 entry nodes and 14 exit nodes and the corresponding total number of vehicles that need to be evacuated is 297,200.

Though these models share several common data sets—the transportation network, an origin and destination matrix for travelers, and often a travel schedule—it is nonetheless difficult to evaluate them in a standard context. Each model incorporates particular effects

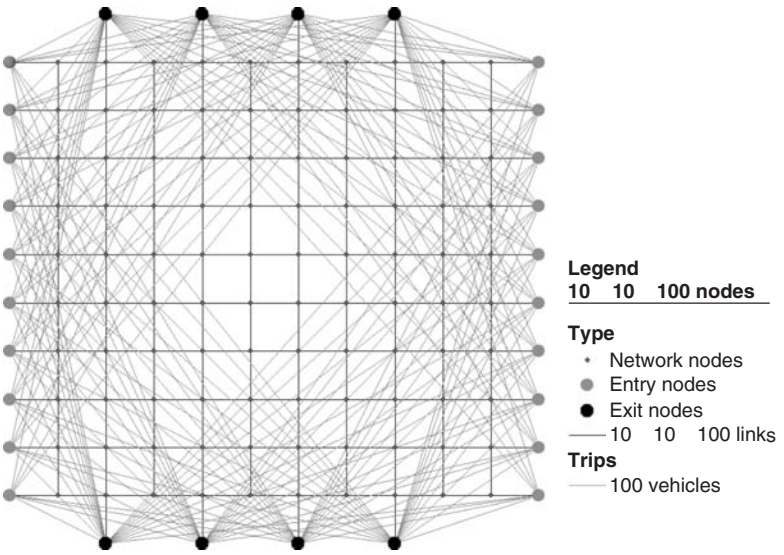



**FIGURE 6** A 10 $\times$ 10 network of nodes where the number 800 vehicles are entering each entry node.

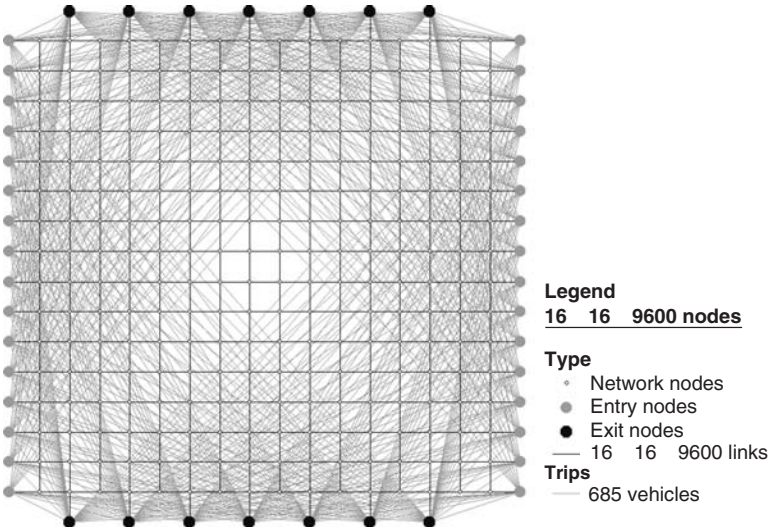



**FIGURE 7** A 16 × 16 network of nodes where the number 9600 vehicles are entering each entry node.

**TABLE 2 Characteristics of All Scenarios**

| Scenarios | No. of Entry Nodes | No. of Exit Nodes | Total Links | No. of Vehicles for Every Entry Nodes | Total No. of Vehicles |
|---|---|---|---|---|---|
| 10 × 10 × 800 | 20 | 8 | 208 | 800 | 16,000 |
| 10 × 10 × 4000 | 20 | 8 | 208 | 4000 | 80,000 |
| 10 × 10 × 8000 | 20 | 8 | 208 | 8000 | 160,000 |
| 10 × 10 × 9600 | 20 | 8 | 208 | 9600 | 192,000 |
| 12 × 12 × 800 | 24 | 10 | 298 | 800 | 19,200 |
| 12 × 12 × 4000 | 24 | 10 | 298 | 4000 | 96,000 |
| 12 × 12 × 8000 | 24 | 10 | 298 | 8000 | 192,000 |
| 12 × 12 × 9600 | 24 | 10 | 298 | 9600 | 230,400 |
| 14 × 14 × 800 | 28 | 12 | 404 | 800 | 22,400 |
| 14 × 14 × 4000 | 28 | 12 | 404 | 4000 | 56,000 |
| 14 × 14 × 8000 | 28 | 12 | 404 | 8000 | 112,000 |
| 14 × 14 × 9600 | 28 | 12 | 404 | 9600 | 268,800 |
| 16 × 16 × 800 | 32 | 14 | 526 | 800 | 25,600 |
| 16 × 16 × 4000 | 32 | 14 | 526 | 4000 | 128,000 |
| 16 × 16 × 8000 | 32 | 14 | 526 | 8000 | 256,000 |
| 16 × 16 × 9600 | 32 | 14 | 526 | 9600 | 297,200 |

and assumptions that are unique to it and, therefore, requires input data that is not common to the others. For example, TRANSIMS uses a pedestrian model to simulate the travel time from buildings (population centers) to parking lots while OREMS and MITSIM ignore the pedestrian mode. Models also vary in their representation of traffic controls

**TABLE 3 Data from a Car Following Experiment Using the MITSIM Car Following Model**

| Time | Lead Vehicle Position | Following Vehicle Position | Following Vehicle Speed |
|---|---|---|---|
| 0 | 70 | 0.0 | 30.0 |
| 1 | 90 | 30 | 26.0 |
| 2 | 110 | 56 | 23.8 |
| 3 | 130 | 80 | 22.5 |
| 4 | 150 | 102 | 21.7 |
| 5 | 170 | 124 | 21.2 |
| 6 | 190 | 145 | 20.8 |
| 7 | 210 | 166 | 20.6 |
| 8 | 230 | 187 | 20.4 |
| 9 | 250 | 207 | 20.3 |
| 10 | 270 | 227 | 20.2 |

(such as stop signs and traffic lights). Where possible, this particular study uses whatever default values are in the models to drive their unique behaviors.

Figure 8 is the egress time among the three models and Figure 9 is the execution time among the three models. For the network with fewer amounts of vehicles, all models generate almost the same egress time. When the network became congested the egress time is increased. It is predictable that OREMS and MITSIM generate the same

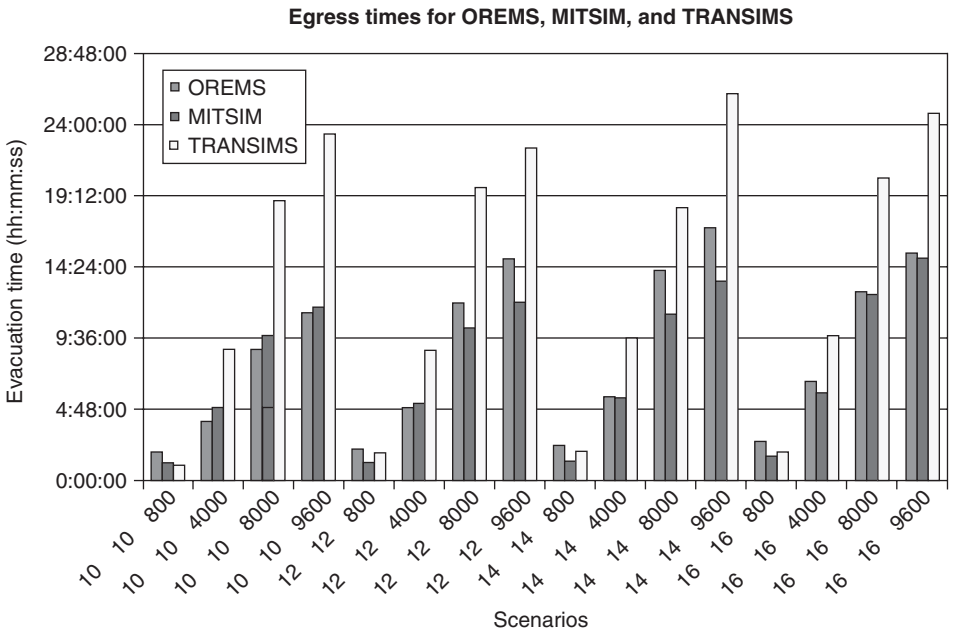



**FIGURE 8** Egress times for OREMS, MITSIM, and TRANSIMS.

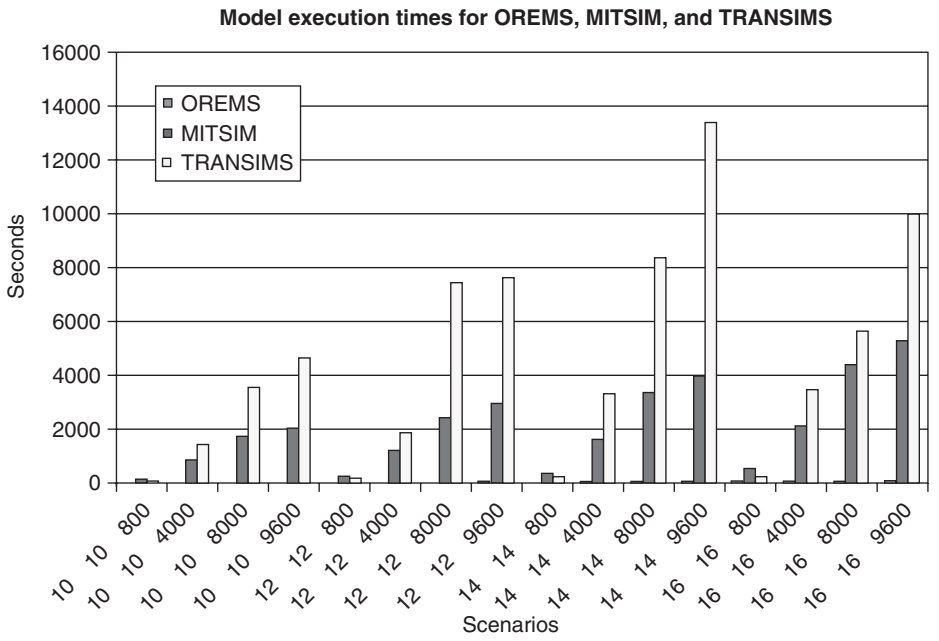



**FIGURE 9** Model execution times for OREMS, MITSIM ad TRANSIMS.

egress time because both models are based on car following, lane-switching, and human behavior models describing the between-vehicle (gap-acceptance) distance tolerance. It is worth noting that the egress time generated by TRANSIMS is different from the other two models because TRANSIMS is based on different assumptions. The reason that TRANSIMS generates longer egress time needs to be explored further. Figure 8 is the result for execution times. It is also predictable that the macroscopic model OREMS runs faster than the other two microscopic models (the range is 10–100 times faster). However in this experiment, MITSIM and TRANSIMS execution times are in the same order of magnitude, but MITSIM performs slightly better than TRANSIMS.

## 5 CHALLENGES FOR LARGE TRAFFIC SIMULATIONS

There are two major barriers to realizing our vision of high resolution multifaceted evacuation modeling. These are scalable simulations and model validation. The least onerous, but still challenging, of these are scalable simulations. The scope of the computational challenge can be estimated by extrapolating from existing simulators. For example, the Alexandria data set for TRANSIMS open source model [27] has about 240,000 vehicles that are simulated for 26 h using a time-step of 1 s. The running time of this simulation—which includes pre- and post- processing of the simulation data as well as the simulation execution itself—requires approximately 2 h. Assuming that the execution time is proportional to the number of vehicles, we can estimate that about 30 CPU hours

would be needed to simulate a Los Angeles sized area, and 140 CPU hours for an area the size of the state of Florida.

Even for a contingency plan that is constructed well in advance of the event, these execution times are too long. Modeling and simulation most effectively supports decision-making when it is used iteratively: a scenario is posed, a plan of action devised, that plan is assessed via simulation, the plan is revised in light of the assessment, and assessment and revision are done again. Assessment and revision will occur dozens of times in the course of making a decision, and sensitivity studies which are necessary to determine the robustness of a particular course of action in the face of reasonable variation, further exacerbate the computational requirement. It is not unreasonable, therefore, to expect thousands of CPU hours to be consumed by microsimulations that are used routinely and effectively for evacuation planning. To reduce thousands of CPU hours to the tens of hours that are needed to reasonably support public officials who make evacuation plans, a 100-fold speed up is needed. To support planning for near-term contingencies, such as day ahead or week ahead events, thousands of CPU hours must be reduced to single digits: a 1000-fold speed up is required.

Moreover, the decision-making process is iterative, using simulation results from earlier iterations to inform changes in a plan. The simulation tools, therefore, will be used iteratively as well with earlier simulations providing, albeit indirectly, input to later simulations. Speed up of the simulation tools themselves is therefore essential. Progress in this direction has been demonstrated with transportation models being scaled to very large parallel computers [28, 29]. But simulating the motion of vehicles is only a part of the computational problem, and the entire tool set—activity scheduling, route selection, and reporting and visualization—must be scalable to effectively support decision makers.

Model validation, however, is the most onerous, but also the most critical and least explored, aspect of transportation modeling. Lack of data about the progress of an evacuation at a suitable resolution in both time and space has been the single greatest barrier to validation, but recent advances in technology as poised to overcome this problem. Global positioning systems are becoming ubiquitous in mobile phones, personal digital assistants, and in vehicles themselves. This data, if it was available to the community of transportation modelers and could be used for validation in the context of typical, day-to-day traffic flow; fire, storm, and flood, will provide ample opportunity to acquire invaluable data on traffic flows during evacuation.

Over a period of several years, this validation activity and the consequent refinement of models will significantly reduce the discrepancies in the outcomes of different simulation tools. The relative value of microsimulations with respect to meso- and macromodels could likewise be determined; though it is widely thought that microsimulations are generally superior in their predictive power, this is still just a matter of speculation. Hard data is needed to achieve a meaningful consensus on the value of these models, and to direct the research community in the most useful directions.

## 6 FUTURE RESEARCH DIRECTIONS

High resolution, data driven simulation of urban evacuation models over large geographic areas is an emerging frontier for more efficient evacuation planning. Existing urban evacuation models are primarily at the mesoscopic scale, open source microsimulation

(traffic) models could be modified for evacuation modeling, and thus hold promise for developing large-scale simulation frameworks to support both near and long term evacuation planning. Moreover, ability to execute such simulations in real time or faster than real time opens up the new paradigm of traffic management during evacuation events. Integration of high resolution geospatial data, namely transportation network and population distribution, coupled with incorporation of finer behavioral assumptions for realistic depiction of population dynamics hold strong promise for achieving such capability [30].

Dynamic data collection and assimilation methodologies are essential to support validation efforts and for model initialization and dynamic calibration. A variety of sensor networks [31] are appearing that can actively or passively monitor traffic conditions, and this will enable accurate assessments of traffic conditions in real time. It is imperative that the exploitation of these data resources be given equal footing with the computational and visualization problems that have in the past have dominated transportation modeling and simulation.

## ACKNOWLEDGMENTS

This paper has been authored by employees of UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy. Accordingly, the US Government retains and the publisher, by accepting the article for publication acknowledges that the US Government retains, a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for US Government purposes.

## REFERENCES

1. Radwan, A. E., Hbeika, A. G., et al. (1985). A computer simulation model for rural network evacuation under natural disasters. *Inst. Transport. Eng. J.* **SS**(9), 25–30.
2. CORSIM USER'S MANUAL. (1997). *FHWA, U.S. Department of Transportation, Office of Safety and Traffic Operation R&D, Intelligent Systems and Technology Division*.
3. Smith, L., Beckman, R., Anson, D., Nagel, K., and Williams, M. E. (1995). TRANSIMS: transportation analysis and simulation system. *Proceedings Fifth National Conference on Transportation Planning Methods Transportation Research Board.* Seattle, Washington, DC.
4. Fisher, K. M. (2000). TRANSIMS is coming! *Public Roads* **63**(5), 49–51.
5. *TRANSIMS Fundamentals: Microsimulator* (2008). http://transims-opensource.org/index.php?option=com_docman&task=cat_view&gid=26&Itemid=22.
6. Bloomberg, L., and Dale, J. (2000). Comparison of VISSIM and CORSIM traffic simulation models on a congested network. *Transport. Res. Rec.* **1727/2000**, 52–60.
7. Cameron, G. D. B., and Duncan, G. I. D. (1996). PARAMICS, parallel microscopic simulation of road traffic. *J. Supercomput.* **10**(1), 25–53.
8. Bhaduri, B., Liu, C., and Franzese, O. (2006). Oak Ridge Evacuation Modeling System (OREMS): a PC-based computer tool for emergency evacuation planning. *Proceedings Symposium on GIS for Transportation*.
9. Franzese, O., and Han, L. (2002). Using traffic simulation for emergency and disaster evacuation planning. *Proceedings 81st Annual Meeting of the Transportation Research Board*.

10. North, M. J., et al. (2006). Experiences creating three implementations of the repast agent modeling toolkit. *ACM Trans. Model. Comput. Simul.* **16**(1), 1–25.
11. Chaturvedi, A., et al. (2005). Bridging kinetic and non-kinetic interactions over time and space continua. *Proceedings Interservice/Industry Training, Simulation and Education Conference, Orlando, FL.*
12. Chaturvedi, A., Gupta, M., Mehta, S. R., and Yue, W. T. (2000). Agent-based simulation approach to information warfare in the SEAS environment. *Proceedings 33rd Hawaii International Conference on System Sciences*. hicss 2:2005.
13. Nagel, K., and Rickert, M. (2001). Parallel implementation of the TRANSIMS microsimulation. *Parallel Comput.* **27**(12), 1611–1639.
14. Rickert, M., and Nagel, K. (2001). Dynamic traffic assignment on parallel computers in TRANSIMS. *Future Gener. Comput. Syst.* **17**(5), 637–648.
15. South Carolina Department of Transportation. (2008). *Coastal evacuation directions, route maps and reversal plans*, (http://www.dot.state.sc.us/getting/evacuation.shtml).
16. Louisiana Department of Transportation. (2006). *2006 evacuation route map*, (http://www.dotd.louisiana.gov/maps/).
17. Florida Division of Emergency Management. (2008). *Regional evacuation studies update*, (http://www.floridadisaster.org/gis/res/).
18. Tobler, W. R., et al. (1997). World population in a grid of spherical quadrilaterals. *Int. J. Popul. Geogr.* **3**, 203–205.
19. Mennis, J. (2003). Generating surface models of population using dasymetric mapping. *Prof. Geogr.* **55**, 31–42.
20. Dobson, J., et al. (2000). LandScan: a global population database for estimating populations at risk. *Photogramm. Eng. Remote Sens.* **66**(7), 849–857.
21. Budhendra, B., Bright, E., Coleman, P., and Dobson, J. (2002). LandScan: locating people is what matters. *Geoinfomatics* **5**(2), 34–37.
22. Bhaduri, B., Bright, E., Coleman, P., and Urban, M. (2007). LandScan USA: a high-resolution geospatial and temporal modeling approach for population distribution and dynamics. *GeoJournal* **69**, 103–117.
23. Bhaduri, B. (2008). Population distribution during the day. In *Encyclopedia of GIS*, S. Shekhar, and H. Xiong, Eds. Springer-Verlag, New York, NY, p. 1377.
24. Yang, Q., and Koutsopoulos, H. N. (1996). A microscopic traffic simulator for evaluation of dynamic traffic management systems. *Transport. Res. Part C* **4**(3), 113–129.
25. Whale, J., Neubert, L., Esser, J., and Schreckenberg, M. (2001). A cellular automaton traffic flow model for online simulation of traffic. *Parallel Comput.* **27**(5), 719–735.
26. Gawron, C. (1998). An iterative algorithm to determine the dynamic user equilibrium in a traffic simulation model. *Int. J. Mod. Phys. C (IJMPC)* **9**(3), 393–407.
27. TRANSIMS Open Source. (2008). http://transims-opensource.net.
28. Cetin, N., Burri, A., and Nagel, K. (2003). A large-scale agent-based traffic microsimulation. *Proceedings 3rd Swiss Transportation Research Conference*.
29. Perumalla, K. S. (2006). A systems approach to scalable transportation network modeling. *Proceedings Winter Simulation Conference*, IEEE.
30. Perumalla, K. S., and Bhaduri, B. (2006). On accounting for the interplay of kinetic and non-kinetic aspects in population mobility models. *Proceedings European Modeling and Simulation Symposium*.
31. Shankar, M., Bhaduri, B., and Liu, C. (2005). From static to dynamic models: enabling real-time geocomputation infrastructures. *Proceedings Geocomputation*.

# HARDEN SECURITY OF HIGH-RISK AND CRITICAL SUPPLY CHAINS

GLEN HARRISON

*Transportation Policy and Planning Group, Center for Transportation Analysis, Energy and Transportation Science Division, Oak Ridge National Laboratory, Knoxville, Tennessee*

## 1 INTRODUCTION

Container transportation forms the circulatory system of the world economy. Over 48 million cargo containers move between major seaports each year. More than 16 million containers arrive in the United States each year by ship, truck, and rail. Ninety percent of the world's nonbulk cargo moves through container supply chains. A supply chain is defined as a "linked set of resources and processesthat begins with the sourcing of raw materials and extends through the delivery of products or services to the end user across the modes of transport [1]". Supply chains include the infrastructure of raw materials and parts suppliers, manufacturers, containers, transport vehicles (sea vessels, rail cars, and motor carriers), intermodal facilities (ports, rail yards, and truck terminals), distribution centers, and retail centers. The financial and logistics support organizations facilitate the movement of containers through the supply chain. There is no single government regulatory system that governs the movement of container shipments through the international supply chain. In fact, there is a mosaic of international and national regulations that govern container shipments. The regulatory framework that is applicable to a specific container shipment is determined by its origin and destination, contents, and the mode of shipment [2].

In the post-September 11 era, there is a greater focus on ensuring the security of goods, people, information, and facilities involved in global supply chains. Container transport is vulnerable to terrorists through (i) interception of a legitimate shipment and tampering with the contents of the container by introducing a chemical, biological, radiological, or nuclear weapon or by contaminating the contents in some way or (ii) obtaining control of a legitimate shipping company, and placing a container with dangerous or illegitimate cargo into the supply chain. The major vulnerability points for the container are in its initial loading, rail yards, truck stops, and intermodal terminals. US Coast Guard officials estimate that the closure of a single major port for a month because of a terrorist attack could cost the US' economy $60 billion in losses [3]. The impact of such a port closing in the United States would also have a domino effect on the economy of many of its trading partners and on the flow of world trade.

Actions taken to reduce the threat of terrorism in the container supply chain include scanning, ensuring the integrity, controlling access, tracking, background checks on personnel, and risk assessment [2]. Rather than inspecting all containers and goods as they

enter a port, there is more reliance on security measures implemented throughout the product supply chain. Governments are investing in enhanced inspection technologies and staffing not only at their own borders and ports but also at overseas production, distribution, and port locations. Companies are reconfiguring their business processes, security systems, information systems, and staffing practices to increase security. Many companies also require their business and supply chain partners to implement compatible security measures. These changes result in increased costs of doing business, but at the same time can also enhance efficiencies in the supply chain and reduce losses due to theft and pilferage [4].

## 2 WORK TO IMPLEMENT A SECURE SUPPLY CHAIN

There is work at several different levels to increase security in the container supply chain, including introduction of processes and procedures, as well as technologies. The following section will discuss increased security measures that have been introduced for the containers, at port facilities, and in the container supply chain.

### 2.1 Containers

Smart containers incorporate electronic systems in the shipping container, which include an electronic seal requiring a code to open the container door, tracking to provide location information, and communications technology that transmits a signal to provide information on the location of the container and any breach of container integrity. After the container is loaded, an electronic data key is used to lock the door of the container at the point of origin. When the container is locked, the security tag sends a signal with status information to other supply chain partners and any authorized government agency requiring the information. The data transfer can occur by mobile telephone or satellite communications. The smart container can be tracked at points along the supply chain. Geo-fencing can be incorporated into the system so that if the container is moved outside of the normal supply chain flow, a signal is sent to the supply chain partners and governmental authorities. A signal is also sent if an unauthorized breach or opening of the container occurs along the supply chain. When the container arrives at the consignee's location, an electronic data key is used to open the container. This generates a signal that results in termination of the container tracking. Future smart containers will include sensors that can detect chemical, biological, radiological, or nuclear weapon devices. They will also include cameras to allow for remote viewing of the container interior [5].

The Container Security Initiative (CSI) places US Customs and Border Protection (CBP) inspectors at foreign ports of embarkation to target containers for inspection. Currently, CSI inspectors are assigned to 54 global ports. CSI requires that the manifest for a container be sent to CBP for review at least 24 h before the container is loaded on a vessel bound for the United States. The CBP's Automated Targeting System rule-based mathematical decision support tool assesses the information and assigns a risk value to each container. If the risk value is high, the container is selected for inspection. All questions must be resolved before the shipment is allowed to be loaded on a vessel bound for a US port [3].

The Secure Freight Initiative began in 2007 at six overseas ports (Port Qasim, Pakistan; Puerto Cortes, Honduras; Southampton, United Kingdom; Port Salalah, Oman; Singapore;

and Busan, South Korea). The program uses local port staff to inspect containers bound for the United States for nuclear and radiological materials. The scanned container images are sent to a CBP operations center for analysis. Containers judged suspect, require physical inspection before being allowed to be loaded on the vessel [6].

## 2.2 Port Security

Port security is an ongoing challenge. It involves ensuring that the cargo containers transiting the port are safe and secure, there is no tampering with the cargo containers while they are in the port, and that the personnel working at the port (dock workers, maritime workers, and transportation workers) are secure. A number of international and US initiatives address these security concerns.

***2.2.1 Scanning Equipment at Ports.*** Two types of scanning equipment are used at ports for container inspection. Radiation portal monitors are used to detect the presence of nuclear and radiological materials in the container. Each container is driven through the portal for a reading. Nonintrusive inspection imaging systems use x rays or y rays to penetrate containers and produce an image of the contents. The image is then reviewed to identify dense areas within the container that could be shielding radioactive material. If there is an alarm generated by either of these systems, then the container is subject to physical inspection [7]. These scanning systems will not detect chemical or biological agents.

***2.2.2 International Ship and Port Facility Security (ISPS) Code.*** The International Maritime Organization (IMO)'s International Ship and Port Facility Security (ISPS) Code provides a common international framework to assess security vulnerabilities and threats, implement security measures, respond to security incidents, and facilitate international cooperation. It was adopted in 2002 as a part of the International Convention for the Safety of Life at Sea (SOLAS). An assessment of the risks must be made to determine the security measures that are appropriate for each ship and port facility. The code provides a standard framework for evaluating risk, so that appropriate response actions can be taken to ensure that security measures correspond with the threat level for ships and port facilities [8].

The code requires that ports conduct a security assessment that includes three components. The first step is to identify and evaluate important assets and infrastructures that are critical to the port facility, as well as those areas or structures that, if damaged, could cause significant loss of life or damage to the port facility's economy or environment. Secondly, the actual threats to those critical assets and infrastructure must be identified in order to prioritize security measures. Finally, vulnerabilities of the port facility must be addressed by identifying its weaknesses in physical security, structural integrity, protection systems, procedural policies, communications systems, transportation infrastructure, utilities, and other areas that may be a likely target. Upon completion of this assessment, the risk level of the port can be determined. Security requirements for ports include the implementation of a port facility security plan based on the risk assessment, the designation of a port security officer, and the acquisition of certain security equipment. The port must change its level of security activities based on the level of risk at any time. Each ship entering the port is also required to have a security plan, designated security officer, and security equipment [9].

***2.2.3 United States Maritime Transportation Security Act of 2002.*** The Maritime Transportation Security Act of 2002 requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle, and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment. The Act also requires the establishment Area Maritime Security Committees at US ports. The purpose of the Committee is to coordinate plans and information exchange to ensure the security of the port. This includes determining the best use of resources that would be used to deter, prevent, respond to, and recover from terror threats or attacks.

***2.2.4 United States Transportation Worker Identification Credential (TWIC).*** The Transportation Worker Identification Credential (TWIC) is a tamper-resistant biometric credential for workers who require unescorted access to secure areas of ports, vessels, outer continental shelf facilities, and all credentialed merchant mariners. An estimated 750,000 workers including longshoremen, truckers, port employees, and mariners are required to obtain a TWIC. TWIC enrollment began in October 2007, and will be phased in through 2008 [10].

***2.2.5 Prenotification.*** Section 343 of the Trade Act of 2002 requires prenotification for cargo entering or leaving the United States by air, land, or sea. The prenotification includes detailed descriptions of the contents of containers. This allows CBP officers to analyze the content information of the container, and identify potential terrorist threats before the US-bound container arrives by highway or rail or is loaded onto a vessel at the foreign seaport. The specific prenotification times are shown in Table 1 [11].

"Do-Not-Load" messages, which forbid the loading, are issued to vessels that violate the 24-h rule. Vessels that disregard the "Do-Not-Load" messages (and load the cited container) are denied permission to unload the container at any US port [12].

All vessels over 300 gross tons must contact the US Coast Guard 96 h before scheduled arrival at a US port. The vessel must provide information on destination, scheduled arrival time, cargo, and crew roster to the Coast Guard. This information and associated information from intelligence agencies are reviewed to identify "high-interest" vessels and are used to determine if the vessel should be boarded, inspected, escorted, or denied entry [13].

**TABLE 1 Prenotification Times**

| Mode | Prenotification Time (h) Import | Export |
|---|---|---|
| Air | 4 h prior to arrival at the border | 2 h prior to departure |
| Rail | 2 h prior to arrival at the border | 2 h prior to arrival at the border |
| Truck | 1 h prior to arrival at the border | 1 h prior to arrival at the border |
| Vessel | 24 h prior to loading on the vessel in the foreign port | 24 h prior to departure from US port where cargo is loaded |

### 2.3 Supply Chain Security

Supply chain security programs apply to the movement of goods and information in commerce. Standards for supply chain security have been developed and implemented at the international, national, and commercial sector levels.

***2.3.1 International Standards Organization's Supply Chain Security Management Standards.*** The International Standards Organization (ISO) has developed security management standards for supply chains [1]. The ISO standards provide a means for organizations to review the security environment of their supply chain, and determine if it is adequate. If inadequacies are found, the standards recommend mechanisms and processes to enhance supply chain security. The finance, manufacturing, information management, and facilities for packing, storing, intermodal transfers, and transporting freight are considered in the security standards. The process for implementing the organization's security management system based on the Plan-Do-Check-Act methodology involves the following steps:

- The organization develops an overall security management policy based on its needs.
- A security risk assessment mechanism is implemented to determine security threats, and target security goals and implementation programs to achieve these security targets are established.
- The organization establishes the structure, provides the resources, and staffs the security management system operation. This includes awareness training, information security, physical security, emergency preparedness, and recovery planning.
- There is continuous monitoring of the security management system and the changing security threat environment. The supply chain changes as technology improves, threat conditions change, and lessons are learned. The security management system is adjusted to ensure that appropriate security measures are in place as changes occur.
- Management performs periodic reviews of the security management system to ensure that it continues to meet overall security objectives.

***2.3.2 Smart and Secure Trade (SST) Lanes Initiative.*** The smart and secure trade (SST) lanes initiative, initiated by the Strategic Council on Security Technology, is an industry-based initiative to improve supply chain security and efficiency. The initiative has four major objectives. Objective 1 is to rapidly deploy a baseline functional infrastructure to secure, track, and manage containers and leverage proven technology and the global networks of the major port operations companies, such as Hutchinson Port Holdings, PSA, P&O Ports, SSA Marine, and China Merchants Holdings Company Limited. Objective 2 is to collaborate with international shippers and their supply chain partners to implement end-to-end container security. Objective 3 is to synchronize and ensure compatibility with existing government freight security initiatives, such as the CSI, Customs Trade Partnership against Terrorism (C-TPAT), Operation Safe Commerce, and ISPS Code. Objective 4 is to demonstrate operational efficiencies through real-time in-transit visibility for supply chain partners [14].

The ports of Singapore, Hong Kong, Kaohsiung (Taiwan), Bangkok, Walvis Bay (Namibia), Cape Town, Tacoma, Seattle, Los Angles, Long Beach, New York/New Jersey, Rotterdam, Antwerp, and Felixstowe (United Kingdom) are currently integrated into the SST system. The Strategic Council on Security Technology's goal is to expand to additional ports, inland distribution centers, and intermodal terminals in the future.

***2.3.3 World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework).*** The World Customs Organization's SAFE Framework of Standards to Secure and Facilitate Global Trade facilitates the implementation of standard and best practices between the customs services of different countries. The goal is to move toward one set of inspection standards that would not duplicate or overlap others [15].

***2.3.4 Secure Trade in the Asia-Pacific Economic Cooperation (APEC) Region (STAR).*** Asia-Pacific Economic Cooperation (APEC) is an organization of Pacific Rim nations working together to promote trade and investment liberalization, business facilitation, and economic and technical cooperation. In 2002, APEC formed the Secure Trade in the Asia-Pacific Economic Cooperation Region (STAR) initiative to accelerate action on screening people and cargo for security before transit; increasing security on ships and airplanes while en route; and enhancing security in airports and seaports. The STAR plan of action for cargo security included (i) identifying and examining high-risk containers, assuring in-transit integrity, and providing advance electronic information on containers to customs, port, and shipping officials as early as possible in the supply chain; (ii) implementing common standards for electronic customs reporting; and (iii) promoting private-sector adoption of high standards of supply chain security. The plan of action for vessel operations involved (i) promoting ship and port security plans and installation of automatic identification systems on certain ships and (ii) cooperating to fight piracy in the region [16]. APEC Private Sector Supply Chain Security Guidelines were also developed to recommend actions on physical security, access control, personnel security, education and training awareness, procedural security, documentation processing security, trading partner security, conveyance security, and crisis management and disaster recovery [17].

***2.3.5 United States Customs Trade Partnership against Terrorism (C-TPAT).*** The C-TPAT is a joint US CBP and business voluntary initiative to enhance security procedures along supply chains. The program provides a trade-off between enhanced security measures along the supply chain for expedited cargo processing at the US border. This program enables CBP to reduce screening efforts for C-TPAT partners who have adequate supply chain security procedures and controls in place for their imported cargo. This enables CBP to focus its screening efforts on unknown or high-risk import cargo transactions [18].

The initiative is based on five overall goals. Goal 1 is to ensure that C-TPAT partners improve the security of their supply chains on the basis of C-TPAT security criteria. When a company joins the C-TPAT partnership, it works with CBP to implement a review of its supply chain, identify security gaps, and implement security measures and best practices to enhance the security of the total supply chain. The areas covered in the review include personnel security; physical security; procedural security; access controls; education, training, and awareness; manifest procedures; conveyance security; threat awareness;

document processing; business partners and relationships; vendors; and suppliers. Upon certification of a company's supply chain, CBP and the company validate the supply chain processes to ensure that the implemented security procedures are effective, efficient, and accurate, which helps ensure that best security practices are in place. The security review and validation process are iterative, recurring on an ongoing basis.

Goal 2 is to provide incentives and benefits to include expedited processing of C-TPAT shipments to C-TPAT partners. This activity involves seminars for sharing information on best practices for securing supply chains. C-TPAT partners receive expedited border crossing procedures that reduce processing time for goods entering the United States. Corollary benefits from the C-TPAT program have been more efficient supply chain operations and reduced inventory loss due to theft and diversion of cargo.

Goal 3 is to internationalize the core principles of C-TPAT through cooperation and coordination with the international community. C-TPAT membership has a multiplier effect. C-TPAT companies require supply chain partners, including foreign manufacturers, shippers, and distribution operations to comply with C-TPAT security measures, which results in the impact of C-TPAT going far beyond the C-TPAT partners to other members of their supply chain operations.

Goal 4 is to support other CBP security and facilitation initiatives. These include the Free and Secure Trade (FAST) program between the United States, Mexico, and Canada, Operation Safe Commerce, the Advanced Container Security Device program, the CSI, and the Industry Partnership Program.

Goal 5 is to improve administration of the C-TPAT program. This involves increases in CBP Supply Chain Specialists, expanded training of staff, and enhanced data collection and information management capabilities.

***2.3.6 United States Operation Safe Commerce.*** Operation Safe Commerce is a federal grant program under the Department of Homeland Security (DHS) that established partnerships with the three largest US container ports (Seattle-Tacoma, Port Authority of New York and New Jersey, and the Ports of Los Angeles and Long Beach) to develop, test, and share best practices to improve the security of container supply chain movements. Specific objectives of the program are (i) validating security at the point of origin, (ii) securing the supply chain from the point of origin to final destination, (iii) enhancing accuracy and communication of cargo information used by Federal agencies, carriers, and shippers, and (iv) monitoring movement and integrity of cargo in transit. Eighteen separate supply chains moving containers through one or more of these ports were evaluated [19].

## 3 MAJOR CONCERNS

Cargo containers may be used to smuggle chemical, biological, radiological, or nuclear weapons into a country. Assuring container supply chain security is a major priority of governments and private sector trade partners around the world.

Efforts to strengthen supply chain security face a number of institutional challenges that include (i) developing a comprehensive risk management approach, (ii) ensuring that funding needs are identified and prioritized and that costs are controlled, (iii) establishing effective coordination among the many responsible public and private entities, (iv) ensuring adequate workforce competence and staffing levels, and (v) implementing security standards for transportation facilities, workers, and security equipment [13].

For the United States and internationally, funding is a major issue in implementing security measures. Individual ports in the United States require funding for security upgrades for basic security measures, as well as the implementation of changes required by legislation or technology enhancements. Funds are also required for ongoing security activities, exercises, and training of staff. Funding is required by the different government regulatory agencies that are involved with port and supply chain security. Funding for agencies in DHS includes the Coast Guard, which is responsible for port security, CBP, which is responsible for the inspection of cargo and passengers entering the United States, and the Transportation Security Agency, which is responsible for cargo and passenger security within the United States. As the security threat has increased, additional legislation has been passed that has expanded the responsibilities for each of these agencies. The Coast Guard and CBP have roles to play at ports in the United States, as well as overseas. Budget allocations for security upgrades in US ports and for the additional DHS staff to enforce these security requirements have not always kept up with the increased requirements mandated by legislation or the potential of increased threats from terrorists. The question that has also not been resolved is the funding of increased security requirements in overseas ports. If an overseas port does not have adequate security infrastructure and staff in place based on international standards, who pays for it?

There are a multitude of national government, international government, international business, and corporate initiatives to increase supply chain security. There is no one overall coordinating agency to eliminate the overlaps or conflicts between these different entities. Some of the programs initiated by the US government involve actions in foreign countries. This includes the installation of imaging systems and inspection of containers at foreign ports by Customs and Border Protection (CBP) staff, inspection of port security measures by the US Coast Guard, and the inspection of the security of international supply chains that can include the manufacturer, transportation, distribution, and ports in a foreign nation. All of these issues involve the negotiation of agreements with these nations to allow US government officials to be involved in these security activities in their country.

There is a major need for the ability of government security agencies to share proprietary business sensitive information on cargo container movements in a secure manner. This would include the manifest, shipping papers, detailed description of the cargo, seller and purchaser, origin and destination of the goods, origin of the container loading operation, transport companies, and freight forwarders [20]. Currently, there is no system to do this. A worst case scenario for international cargo inspections would be that a multitude of countries will want to station inspectors at foreign ports that ship goods to their country. In this case, each port would need to provide information on the shipments and meet the security requirements of these different national security interests. Currently, the United States shares the data on its foreign port security operations only with the host country. Yet, a container ship will make stops in a number of countries as it moves cargo around the world. A better way to share this data with other nations needs to be developed.

Container shipments that are bound for a specific port in the United States are thoroughly reviewed by CBP. But, in-bond container shipments transit an arrival US port to another domestic port location without officially entering US commerce. The purpose of in-bond cargo is to facilitate trade that moves between ports in the United States. For instance, an in-bond container shipment from Asia to Europe could be off-loaded from a ship on the west coast of the United States, be transferred to a railcar, and taken to

an east coast port for transfer to a ship bound for Europe. This in-bond cargo is not as thoroughly screened as normal containers shipments bound for a single port in the United States. Also, CBP does not track the arrival of the in-bond cargo at the second destination US port. Diversion of this cargo could lead to reduced duty collection on imports and increased security vulnerabilities. More attention needs to be given to inspection and tracking of in-bond cargo [21].

Legislation introduced in Congress in 2007 to require 100% screening for all containers entering the United States failed in the Senate [22]. The requirement for 100% screening of containers would change the current process that uses intelligence and information on the cargo shipment analyzed with the use of a rule-based algorithm to determine the need for inspection of individual containers. This process reduces the need for equipment and staffing for inspections of containers, and facilitates the flow of containers through ports. The requirement for 100% screening of containers would require a substantial increase in funding for equipment and staff, training of this staff in the operation of the equipment, and the agreement of overseas governments to allow for the installation of inspection equipment and expanded inspection activities at their port facilities. There is also the need to transmit the data on the screened cargo for review and analysis to an operations center that may be at a location thousands of miles from the actual port. This would result in greater delays in the movement of containers through port facilities [23].

Improved technologies are required to enhance the security of the container supply chain. The Directorate for Science and Technology (S&T Directorate) is the primary research and development arm of DHS. The Domestic Nuclear Detection Office is responsible for implementing research, development, testing, evaluation, and implementation of radiation detection equipment that can be used to monitor containers. Issues that require additional technology development include imaging systems with enhanced patter recognition capabilities; sensors that detect explosives and biological or chemical hazards in containers; and radiation detection systems with improved signature detection systems to identify specific hazards. The development of Advanced Spectroscopic Portals enables users to both detect and identify the type of radioactive material in a container. These portals are now being deployed at ports around the United States [23].

## 4 SUMMARY AND CONCLUSIONS

Significant improvements have been made in the security of containers, ports, and supply chains since the 11 September 2001 attack. Still, there is more to be done. The 2006 “Global Survey of Supply Chain Progress” performed by the Computer Sciences Corporation and Supply Chain Management Review surveyed 134 supply chain organizations. On the question of supply chain disruptions, only 40% of the respondents said they had contingency plans for significant disruptions [24].

There is also a need for greater coordination and consistency among the security programs initiated by the private sector, government, international governments and international organizations. Each of these sectors is initiating programs that improve security, but in many cases there is overlap and inconsistency. One of the greatest needs is the ability to share business sensitive information between international government security agencies. Security initiatives that are initiated need to be funded at an adequate level for the equipment, staffing, training, maintenance, and regulatory supervision. Funding is a crucial issue as technical advances result in better container tracking, container security

systems, screening equipment, communications systems, and risk assessment systems that will need to be deployed at ports around the world.

## REFERENCES


1. International Standards Organization/Publicly Available Specification 28000 (2005). *Specification for Security Management Systems for the Supply Chain*, 15 November 2005.
2. *Organization for Economic Co-operation and Development* (2005). *Container Transport Security across Modes*, 19 April 2005. http://www.oecd.org/dataoecd/29/8/31839546.pdf.
3. PriceWaterhouseCoopers (2005), *Cargo Security White Paper, Independent Verification of C-TPAT Cargo Security Controls*, 26 May 2005. http://www.pwc.com/extweb/pwcpublications.nsf/docid/36261E03158608EB8525705A006C6DCF.
4. Eggers, W. (2004). *Prospering in the Secure Economy*. http://www.deloitte.com/dtt/article/0,1002,sid%253D5628%2526cid%253D80288,00.html.
5. Giermanski, J. (2007), *Smart Containers and the Chain of Custody*, 12 February 2007. Traffic World Commonwealth Business Media, Newark, NJ, p. 6.
6. Keane, A. G. (2006). *DH'S Boxes In Security*, 18 December 2006. Traffic World Commonwealth Business Media, Newark, NJ, pp. 10–12.
7. U.S. Department of Homeland Security (2007), *Customs and Border Protection Service, Secure Freight Inspection Technology*, October 2007. http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/sfi/sfi_technology.ctt/sfi_technology.pdf.
8. Lyndon B. Johnson School of Public Affairs (2006). *Port and Supply-Chain Security Initiatives in the United States and Abroad*. The University of Texas, Austin. http://www.trb.org/news/blurb_detail.asp?id=6804.
9. International Maritime Organization (2002). *The International Ship and Port Facility Security Code*. http://www.imo.org/About/mainframe.asp?topic_id=583&doc_id=2689.
10. U.S. Department of Homeland Security, Transportation Security Administration (2007). *Transportation Worker Identification Credential*. http://www.tsa.gov/what_we_do/layers/twic/index.shtm.
11. U.S. Department of Homeland Security, Customs and Border Protection Service (2002), Table 2—Summary of Rule By Mode, Section 343, Trade Act of 2002, *Advance Electronic Cargo Information*. http://www.cbp.gov/linkhandler/cgov/import/communications_to_trade/advance_info/transport_matrix.ctt/transport_matrix.xls.
12. U.S. Department of Homeland Security, Customs and Border Protection Service (2003). *Enforcement of 24-Hour Rule Begins February 2*, 30 January 2003. http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/cbp_press_releases/012003/01302003.xml.
13. U. S. General Accounting Office (2003). *Transportation Security, Post-September 11th Initiatives and Long-Term Challenges*, GAO-03-616T, 1 April 2003. http://www.gao.gov/new.items/d03616t.pdf.
14. Strategic Council on Security Technology (2003), *Smart and Secure Tradelanes*, May 2003. http://www.savi.com/products/casestudies/wp.sst_initiative.pdf.
15. World Customs Organization (2005). *Framework of Standards to Secure and Facilitate Global Trade*, June 2005. http://www.cbp.gov/linkhandler/cgov/border_security/international_activities/international_agreements/wco/wco_framework.ctt/wco_framework.pdf.
16. The White House (2002). *Fact Sheet: Secure Trade in the APEC Region ("STAR")*, 26 October 2002. http://www.whitehouse.gov/news/releases/2002/10/print/20021026-8.html.
17. Asia-Pacific Economic Cooperation (2007). *APEC Private Sector Supply Chain Security Guidelines*, http://www.apec.org/apec/apec_groups/som_special_task_groups/counter_terrorism/secure_trade_in_the.html#.

18. U.S. Department of Homeland Security, Customs and Border Protection Service (2004). *Customs-Trade Partnership against Terrorism (C-TPAT) Strategic Plan*, November 2004. http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ctpat/ctpat_strategicplan.ctt/ctpat_strategicplan.pdf.
19. U.S. Department of Homeland Security, Office of Domestic Preparedness (2005). *Operation Safe Commerce Phase III*. http://www.ojp.usdoj.gov/odp/docs/FY05_OSC_revised.pdf.
20. Coalition for Secure Ports. *Enhance the Government's Security Targeting and Screening of Containerized Cargo Shipments*. http://www.secureports.org/improving_security/factsheet_screening.html.
21. U. S. General Accounting Office (2007). *Persistent Weaknesses in the In-Bond Cargo System Impede Customs and Border Protection's Ability to Address Revenue, Trade, and Security Concerns*, GAO-07-561, April 2007. http://www.gao.gov/new.items/d07561.pdf.
22. SecurityInfoWatch (2007). *Lloyds List, Senate Nixes Container Screening Bill, 6 March 2007.http://www.securityinfowatch.com/article/printer.jsp?id=10652.*
23. U. S. General Accounting Office (2007). *Maritime Security, One Year Later: A Progress Report on the SAFE Port Act*, GAO-08-171T, October 16, 2007. http://www.gao.gov/new.items/d08171t.pdf.
24. Poirier, C. C. and Quinn F. J (2006). *Survey of Supply Chain Progress: Still Waiting for the Breakthrough Supply Chain Management Review. 1 November 2006*. http://www.scmr.com/article/CA6399959.html?industryid=48314.

# TRANSPORTATION SECURITY PERFORMANCE MEASURES

RUSSELL LEE
*Oak Ridge National Laboratory, Oak Ridge, Tennessee*

## 1 INTRODUCTION

Transportation security organizations—both public and private—face difficult challenges in deciding which security systems to deploy. Advances in science and engineering continue to offer a wide range of new technologies and systems that might reduce the risks of natural and terrorist threats. Although it is impossible to precisely predict the effectiveness of these systems, it is important to assess how well they are likely to perform prior to commercializing or deploying them. In this regard, it is useful to define a concise set of measures that can be systematically and uniformly used to assess the value of alternative technologies and systems under different scenarios. This article defines a

framework for defining these performance measures, suggests specific metrics within this framework, and provides illustrations from previous studies. These metrics are primarily intended for use in science, technology, and R&D organizations in homeland security agencies and offices, such as the US Department of Homeland Security, to assess the value of candidate technologies and systems prior to their commercialization or deployment (i.e. the purchase, installation, and operation of a system).

## 2 PERFORMANCE MEASURE CONCEPTS

"Measures" in this article refer to ways of gauging how well a system will perform. A broadly defined measure could have one or more specific measures under that general category. For example, a general measure is the "benefits" of a system; and under benefits, a specific measure is "reduced harm to human health." *Metrics* refer to one or more quantitative indicators for a given measure. For example, the "estimated reduction in lives lost due to a terrorist attack" is a metric for "reduced harm to human health."

In this article, the term, *performance measures*, differs from another common application that defines criteria to *retrospectively* evaluate the *management* or *programs* of an organization [1, 2]. Whereas, this article uses performance measures to *prospectively* assess the *value* of transportation security *technologies and systems*.

Another important distinction is that these measures focus on the expected value of these systems *in practice*, rather than solely on their technical specifications or performance under controlled *laboratory* conditions, as commonly stipulated in American National Standards Institute and other similar standards (e.g. [3, 4]). The latter are an important consideration, but the performance of the systems and their benefits and impacts, in the *field* are ultimately more important in gauging their value.

## 3 FRAMEWORK TO DEFINE PERFORMANCE MEASURES FOR TRANSPORTATION SECURITY SYSTEMS

This section defines a framework for defining performance measures to assess the value of transportation security technologies, systems, and operations (other related work includes [5, 6]). The framework is applicable to assessments of systems that are to monitor for, prevent, respond to, mitigate, or recover from natural disasters, terrorist attacks, or other threats to transportation systems and to the activities and economies that depend on them.

### 3.1 Elements in a Risk-Based Approach

We use the following terms to describe the basic elements in a risk-based approach for considering transportation security:

1. *Threats.* The nature and quantity or magnitude of an event, material, or substance that does harm (e.g. explosives, biological, or chemical weapons of mass destruction, illicit radiological material).
2. *Transportation systems.* Transportation networks, nodes, corridors or other infrastructure; the flow of vehicles, trains, ships, ferries, containers, goods, or people who use that infrastructure. There are parts of a transportation system that can be used

to deliver a threatening agent (e.g. airplanes used as weapons), or they can be the target of a threat (e.g. a bridge with high traffic volume).

3. *Targets.* The infrastructure, population, or other entities that are at risk from a threat (e.g. a critical bridge, transit facility, or airport terminal).
4. *Vulnerability.* Aspects of targets that are at risk of damage from threats, the probabilities of damage, and factors affecting these probabilities.
5. *Damages.* The adverse effects of an attack on, or catastrophic disruption to, a target (e.g. physical damage, economic costs).
6. *Transportation security systems.* Technologies, operations, and systems whose function is to detect, identify, reduce, or respond to a threat (e.g. video surveillance systems, automated biological, and chemical threat detection systems).

These elements help frame the problem at hand, the associated risks and the transportation security systems that might be deployed to address these risks.

### 3.2 Performance Measures Framework

The performance measures framework provides a consistent and systematic means of assessing transportation security systems for different scenarios, threats, and targets. There are four major categories of performance measures: (i) system performance, (ii) benefits, (iii) resources, and (iv) impacts. Each is discussed in turn.

1. *System performance* refers to the technical and operational performance of the transportation security system under actual field conditions. It is worth emphasizing that the measures of system performance address both technical *and* operational considerations.
   - *Technical* performance measures gauge the technical capabilities of the system in terms of the number of vehicles, or items it can process, the system's effectiveness, and its reliability (e.g. throughput of baggage scanning systems).
   - *Operational* performance measures gauge whether the system, including the operational and response protocols, is easy to deploy and operate and provides information that helps personnel to perform their tasks (e.g. ease of operating a scanner).
2. *Benefits* refer to the ultimate reasons for deploying such systems—ensuring the safe movement of people and goods on our nation's transportation systems, and the safety of other affected parties, by efficiently detecting and responding to threats. Usually, the reasons for deploying a transportation security system are to reduce the risk of loss of life or injury, or the economic costs of damages, or disruptions to the operation of a transportation system. Thus, "benefits" are the *ultimate*, underlying reasons for deploying these systems. In many situations, however, it is difficult to estimate these outcomes. Thus, in practice, system performance metrics such as the percentage of false negatives, can be used as surrogates for some of the benefits of a system.
3. *Resources* are the technologies, supplies, equipment, space, personnel, and other resources needed to deploy, maintain, and operate these systems, including the cost of training personnel. Initial, capital costs of purchasing equipment, one-time

setup and training costs, and periodic maintenance and operating costs are resource requirements that should be taken into account as well.

4. *Impacts* are effects associated with the operation of the system, such as possible delays to freight and other traffic, safety or discomfort issues, and the economic cost of delays. Another impact could be interference with activities normally carried out at the site, for example, interfering with truck weigh-station staff and their routine responsibilities.

Collectively, these measures comprise a comprehensive set of considerations for assessing systems and ultimately for helping decide which to deploy.

## 4 DEFINITIONS AND ESTIMATION OF PERFORMANCE METRICS

This section suggests specific metrics for each of the measures and describes how to estimate the values of these metrics in practice.

### 4.1 Metrics for System Performance

The first set of performance measures summarizes key technical and operational aspects of the system. These measures are subdivided as follows:

Technical performance
- throughput
- effectiveness
- reliability

Operational performance
- ease of operations
- usefulness of the information from the transportation security system for operators

Other technical or operational performance measures could be used, but the ones listed above are a basic set to consider. We discuss each in turn.

***4.1.1 Throughput Metrics.*** *Throughput* refers to the number of items, such as vehicles, rail cars, or passengers who can be processed through the security system per unit time. For example, a metric for throughput would be the number of vehicles per minute that can be scanned for explosives before driving onto a ferry. Assessments of system throughput can be compared to throughput without any security system in place.

***4.1.2 Effectiveness Metrics.*** The effectiveness of a system is a key measure of its value. For systems that provide domain awareness and prevention, their effectiveness can be characterized by their ability to accurately predict the presence of threatening material or activity. For technologies that detect the presence of radiological, chemical, or biological threats, the standard metrics to use are the "false negative" and "false positive" rates. For medical diagnostic technologies, "sensitivity" and "specificity" are commonly used

**TABLE 1 Sensitivity, Specificity, False Positive Rate, False Negative Rate, Positive Predictive Value and Negative Predictive Value are Common Metrics for the Effectiveness of a Transportation Security System**

| | Predicted | |
|---|---|---|
| Actual | Positive | Negative |
| Positive | a = True Positive | d = False Negative |
| Negative | c = False Positive | b = True Negative |

[a]Definitions of metrics of system effectiveness:
[b]Sensitivity = a / (a + d)
[c]Specificity = b / (b + c)
[d]False Negative Rate = d / (d + b)
[e]False Positive Rate = c / (c + a)
[f]Positive Predictive Value = a / (a + c)
[g]Negative Predictive Value = b / (b + d)

metrics to gauge their ability to identify the presence of a threatening health condition. Table 1 and the notes accompanying the table define these terms. Illustration 1 is an example of the use of these metrics for a system that detects the transportation of illicit radiological material.

In other situations, the effectiveness of a system can be assessed by its ability to reduce a certain threat or damaging condition. Illustration 2 discusses this situation in the context of screening airline passengers for pandemic influenza. Other systems might be geared more toward protection (e.g. enhanced shielding), response or recovery. Similar principles for defining system performance measures apply to these types of systems as well.

In assessing the effectiveness of systems, it is also important to study the reasons for their technical and operational performance. For example, certain environmental conditions might affect the operation of an instrument or limit its ability to detect or identify certain types of material (e.g. specific radionuclides, or specific types of explosives). Such assessments help identify vulnerabilities and the need to develop ways of addressing them.

***4.1.3 Reliability.*** The concept of reliability refers to a system's long-term ability to perform with little variability in effectiveness, in the face of disturbances that could affect performance. Thus, a reliable system is one whose performance is predictable. Suitable metrics for reliability include:

- frequency or rate of system outages or malfunction, per day
- variability of technical performance, from day to day, or under different conditions.

***4.1.4 Ease of Operations.*** In practice, the ease of operating a system is important to its performance. A system could be technically superior but if it is difficult to operate then its overall performance in the field suffers. Metrics to gauge the ease of operations can be based on either the operators' direct assessments or on the frequency of operator errors observed in a field operational test.

***4.1.5 Usefulness to Operators.*** Some systems provide useful data, information, or other insight to help system operators to carry out their responsibilities better. A metric for this measure would likely depend on input from the operators in a field operational test.

**TABLE 2 Metrics to Gauge System Performance**

| Type of System Performance | Metrics | Estimation Methods |
|---|---|---|
| Throughput | Quantity or number of units processed per unit time (e.g. number of vehicles screened per minute) | Observations from a field operational test.<br>Simulation model of the process |
| Effectiveness | Sensitivity.<br>Specificity.<br>False negative rate.<br>False positive rate.<br>Positive predictive value.<br>Negative predictive value | Compilation of data from a field operational test.<br>Subject matter experts' estimates.<br>Vendors' specifications provide preliminary estimates, under laboratory conditions |
| Reliability | Rate of system malfunction per unit time (e.g. number per week) | Data from a field operational test.<br>Subject matter experts' estimates.<br>Vendors' specifications or estimates provide an initial estimate |
| Ease of operation | Assessment of ease of operation on, say, a five-point scale.<br>Operator error (e.g. number per week) | Survey of system operators in a field operational test.<br>Data from a field operational test |
| Usefulness to operators | Assessment of usefulness, to system personnel, of the information or other outputs from the system on, say, a five-point scale | Survey of operators who participate in a field operational test |

Table 2 summarizes different metrics for system performance and methods to estimate them.

### 4.2 Metrics for the *Benefits* of Transportation Security Systems

By the "benefit" of a transportation security system, we refer to desirable outcomes. The concept, "outcome," implies some ultimate, end result that relates to human health, economic or social well-being, or the state of the environment. It is important to distinguish between these *ultimate* outcomes and capabilities. Outcomes are the fundamental reason for having a system, for example, to save lives. Whereas, capabilities are an enabling attribute such as a system's ability to, for example, detect a threat.

The benefits of interest vary depending on the threats and the possible damages. In practice, it might not be possible to estimate the benefits, *per se*, and in these instances, we use metrics that are surrogates for more direct measures of benefits. For instance, in Illustration 1, it is difficult to estimate the human health repercussions if the transport of illicit radiological material is not interceded. In this example, the false negative rate, which is a metric of technical performance, is also used as one of the metrics for the benefits of the system. Table 3 lists important types of benefits, specific metrics for these benefits, and ways of estimating them.

**TABLE 3 Metrics for the Benefits of a System**

| Type of Benefits | Metrics | Estimation Methods |
|---|---|---|
| Health and safety | Expected reduction in loss of life and injury or illness | Field operational tests (e.g. "Red-Team" exercises with role playing to gauge operator performance and the likelihood of system failure).<br>Simulation modeling (e.g. using plume models and geographic information systems to simulate the spread of a chemical and exposure to population).<br>Subject matter experts' assessments of reduced vulnerability and effectiveness of a system |
| Economic | Expected reduction in direct financial loss.<br>Expected reduction in economic damage due to indirect impacts (e.g. industries that depend on businesses that are directly impacted by an attack) | Econometric model.<br>Financial analysis.<br>Subject matter experts' estimates based on estimates of technical performance (e.g. estimate of economic impact from a terrorist attack at a certain location) |
| Social | Expected reduction in damage to social well being in the region or country | Previous studies of similar situations.<br>Subject matter experts' assessments |
| Value to stakeholders | Assistance or support to stakeholders to help them carry out their responsibilities more efficiently or more effectively, as measured on a five-point scale, say | Survey of stakeholders involved in a field operational test of the system |

### 4.3 Metrics for the *Resources* Needed for a Deployment

Resources include technologies, supplies, equipment, space, personnel, and items needed to deploy, maintain, and operate a transportation security system. Table 4 lists key resources needed in most deployments, and ways of defining and estimating the amount of resources.

### 4.4 Metrics for the *Impacts* of Transportation Security Systems

Deployment of transportation security systems often result in impacts on the people or vehicles monitored, or on activities in the area. Such impacts are an indirect consequence of deploying a system. Table 5 lists potentially important impacts, specific metrics for these impacts and ways of estimating them.

## 5 ILLUSTRATIONS OF THE USE OF PERFORMANCE MEASURES

This section gives two illustrations of the application of the performance measures framework and the definition of specific metrics. Each illustration describes the threat,

**TABLE 4 Metrics for Resource Needs**

| Type of Resources | Metrics | Estimation Methods |
|---|---|---|
| Personnel: type, number and cost | Number of personnel, by type | Estimates from simulation model.<br>Subject matter experts to estimate number of personnel needed.<br>Labor cost estimates (including fringe benefits, overhead) |
| Supplies: type, amount and cost | Quantity of supplies, by type | Simulation model to estimate amount of activity and supplies.<br>Subject matter experts' estimates of amount of supplies needed per unit of deployment activity |
| Capital costs: type and amount of equipment; cost of equipment, installation and supplies | Quantity, size or amount.<br>Cost (dollars) | Calculations of quantities required.<br>Subject matter experts' and planners' estimates of types and amount of equipment and supplies.<br>Survey vendors' quotes, or literature or information on cost estimates |
| Annual operations and maintenance costs | Cost | Engineering cost estimates |

**TABLE 5 Metrics for the Impacts of a System**

| Type of Impacts | Metrics | Estimation Methods |
|---|---|---|
| Delays | Average delay time per unit, e.g. seconds of additional transit time per passenger | Estimate from a field operational test.<br>Estimate from a simulation model |
| Economic effects | Cost of delays to commerce, e.g. in dollars per week.<br>Value of time delays to individuals, e.g. in dollars per week | Calculated based on estimated time delay and on the dollar value of a unit of time delay.<br>Survey information from affected party |
| Safety | Assessment of risk to operators or those being monitored, assessed on a five-point scale, say.<br>Predicted accident rate | Survey of people impacted.<br>Subject matter experts' assessment |
| Social or psychological | Assessment of social or psychological impact on those monitored, on operators, or the public in general, assessed on a five-point scale, say | Survey of people impacted.<br>Estimate of some indicator based on the scientific literature |
| Changes in operations | Assessment of either adverse or desirable change in operations or other processes, assessed on a five-point scale, say | Survey of people in organizations impacted |

transportation system, targets, vulnerability, possible damages, and the transportation security system under consideration. Specific metrics are defined, based on the general framework. Since the illustrations are from studies whose results are For Official Use Only (FOUO), we do not list the actual values for the performance metrics. Any numbers presented in this article these illustrations are for illustrative purposes only.

### 5.1 Illustration 1: Assessing Performance of a Transportable Radiation Monitoring System

The first illustration of the use of the performance measures framework is an operational test of a transportable radiation monitoring system (TRMS) [7–9]. The technologies in this system detect and identify $\gamma$ and neutron radiation. They monitor the possible, illicit transport of radiological material in vehicles along highways, or in containers at rail and port facilities. The transportable system is similar to stationary portal monitors found at land border crossings, which detect radiological material in vehicles crossing the border into the country. A distinguishing feature of the transportable systems is that they can be deployed virtually anywhere along a transportation network or at special events that might be targets of terrorists, such as high-profile political, sports or entertainment events.

In this illustration, the risk-related aspects for considering the transportation security system are as follows:

*Threat.* Illicit transportation of radiological material.

*Transportation system.* Interstate or other major highways, or rail or port facilities.

*Target.* Any people exposed to the illicit radiological material.

*Vulnerability.* Radiological material sources are easily concealed; releases will affect population exposed; likelihood is low but general impact could be significant.

*Damages.* Human health effects of exposure to radiation and, more generally, the panic and fear inflicted on the country.

*Transportation security system being assessed.* Deployment of TRMS that detects and identifies materials emitting $\gamma$ or neutron radiation from packages in vehicles or containers.

Field operational tests on actual roads (not test facilities) were used to compile data to calculate the metrics. The first test monitored vehicles on roads entering and exiting a US Department of Energy facility [8]. The facility's security personnel controlled vehicle entry and exit from the facility; other conditions of the test replicated field conditions. The second test involved local and state responders, Red Teams, and reachback to the Joint Analysis Center in the Domestic Nuclear Detection Office of the US Department of Homeland Security. The system was deployed at a rest area on an interstate highway [9]. Key metrics were defined and estimated as follows. The first set was the system performance metrics.

#### *5.1.1 System Performance Metrics*

*5.1.1.1 Metric—Throughput.* The counts of the number of vehicles monitored each hour were recorded each day in the field operational tests. This estimate provides a lower-bound estimate of the throughput because field experience showed that the system

is capable of monitoring at least this number of vehicles. An upper-bound estimate was calculated based in the maximum speed that vehicles can drive past the monitoring system without affecting its operation.

*5.1.1.2 Metric—Effectiveness of Detection System.* The effectiveness of the system was gauged by its ability to correctly detect $\gamma$ and neutron radiation from packages in vehicles. In Table 6, the predicted attribute is whether "Radioactive Material (is) Detected" by the system. The actual attribute is whether the "Vehicle (is) Carrying Radioactive Material." The ability of the system to detect vehicles carrying radiological material was assessed using data from shipping manifests and other documentation, which were used to verify the contents of each vehicle. The top number in each cell in Table 6 is the number of vehicles in the category:

- carrying radioactive material that was detected (true positives—cell "a"),
- without radioactive material and which were appropriately released with minimal delay (true negatives—cell "b"),
- carrying radioactive material that the system did not detect (false negatives—cell "c"), and
- without radioactive material, but which were detained because the vehicle triggered an alarm in the system, indicating presence of radioactive emissions (false positives—cell "d").

These metrics were compared to percentages established in technical standards for accuracy under controlled laboratory conditions [3, 4]. Incidentally, these standards were used as a frame of reference, not as a formal basis for evaluating these systems because the test conditions differed from the controlled conditions used in setting the standards.

Several other metrics were used in the study, such as the number and types of radionuclides the system was able to correctly identify, and which radionuclides it was unable to identify [8, 9].

**TABLE 6 Data to Calculate the Effectiveness of a Detection System**

Number of Vehicles and *Percentage of Total Vehicles*
(Percentages in parentheses are the standard for accuracy under controlled laboratory conditions, per ANSI N42.43-2005 and ANSI N42.35-2004)

| | Vehicle Carrying Gamma or Neutron Emitting Radioactive Material? | |
|---|---|---|
| Radioactive Material Detected? | Yes | No |
| Yes | 381<br>*a*%<br>(98.3%) | x<br>*d*%<br>(0.1%) |
| No | y<br>*c*%<br>(1.67%) | 42,058<br>*b*%<br>(99.9%) |

*5.1.1.3 Metric—Reliability of Detection System.* The reliability of the system was assessed on the basis of the number of hours the system was not in operation due to equipment failure or other cause, during the field operational tests. Table 7 is taken from the study (the actual results of the study are not listed because they are FOUO).

*5.1.1.4 Metric—Ease of Operating the Detection System.* The operators who manned the system during field operational tests were asked about the ease of operating the system. Nine questions were asked, with the responses given on a five-point scale. An example of one of the questions is: "The inspection procedures were easy to carry out." Individual operators' responses were either strongly agree = 5, agree = 4, somewhat agree = 3, disagree = 2 or strongly disagree = 1. Responses were averaged to produce overall scores.

*5.1.1.5 Metric—Usefulness of Detection System to Operators.* In the field operational tests, operators were asked seven questions about the usefulness of the system; responses were on a five-point scale. An example of one of the questions is: "Information/data from the system at the primary inspection location helped me decide what action(s) to take with each vehicle at the secondary inspection location."

***5.1.2 Metrics for the Benefits of the Detection System.*** The performance measures for the benefits of the system were detector accuracy and the value of the system to stakeholders.

*5.1.2.1 Metric—Detector Accuracy.* It is extremely difficult to estimate the ultimate benefits of the system, in terms of its expected ability to reduce morbidity or mortality from exposure to radionuclides. Thus, the technical performance metrics used for "effectiveness" were used as surrogates for the benefits of the system. In this example,

**TABLE 7 Reliability of Transportable Radiation Monitoring System as Measured by Frequency and Duration of System Downtime**

| | Sites | | | |
|---|---|---|---|---|
| | In-bound East | In-bound West | Out- bound | All |
| Number of days system deployed | | | | |
| Number of times out of service | | | | |
| Total amount of time out of service (hours) | | | | |
| Total hours that system should have been in service during the deployment period | | | | |
| Average number of shutdowns/hour | | | | |
| Cumulative hours system shut down/total hours | | | | |
| Average time spent out of service (minutes) | | | | |

the purpose of the system is to detect vehicles carrying radiological material with an acceptable degree of accuracy, and without nuisance alarms. Among the metrics used, then, were the system's false negative and false positive rates. These rates depend on the operators' interpretations of the data, which the system provides, and the operators' responses to alarms.

*5.1.2.2 Metric—Value to Stakeholders.* The value to stakeholders is an "enabling" benefit. By assisting stakeholders, the system enables them to reduce risk or damage. This metric was gauged by asking stakeholders questions about the use and usefulness of information the system provides. For example, one of the questions is: "*Specific* information/data from the TRMS, or from a TRMS operator, would greatly aid my organization in our response to the incident." Respondents answered these questions on a five-point scale.

***5.1.3 Metrics for Resource Needs and Costs of the Detection System.*** The primary resources needed, in this example, are the system itself and trained personnel to operate it. The cost estimate for the system was based on the actual cost of purchasing it from the vendor, who assembled the system using commercial off-the-shelf components, based on a set of technical specifications [7]. The total number of personnel was estimated based on the number needed to operate the system at any one time, the number of shifts per day, and the number of backup personnel needed. The estimates were verified in the field operational tests.

***5.1.4 Metrics for Impacts of the Detection System.*** The impacts of the detection system were assessed on the basis of:

- the length of inspection delays (which were recorded, in minutes);
- observations of the operation in the field in terms of the extent to which normal traffic and activities were disrupted; the operators' impressions were supplemented by their evaluations on a five-point scale; and
- operators' responses to questions about whether operating the system led to safety concerns, either to operators or others in the area.

## 5.2 Illustration 2: Assessing Performance of Airport Entry Screening of Passengers during a Pandemic

The second illustration of the definition and use of performance measures is a study of the usefulness and impacts of airport passenger screening during a global influenza pandemic [10, 11]. Once the World Health Organization recognizes human-to-human transmission of a problematic subtype of influenza, the organization elevates the situation to a Phase 4 pandemic condition. At this point, many countries plan to screen passengers and crew on inbound international flights.

In this second illustration, the risk-related aspects of the transportation security system are as follows:

*Threat.* Human-to-human transmission of pandemic influenza virus.

*Transportation system.* International air travel.

*Target.* Any people potentially exposed to the virus.

*Vulnerability.* New strain of virus could cause high incidence of infection; daily human activities and contacts mean that spread is likely once the pandemic is "seeded."

*Damages.* Illnesses and deaths, and associated economic losses.

*Transportation security system being assessed.* Deployment of multilayered screening protocol to screen international passengers entering the country at airports to identify those infected with the pandemic influenza virus.

Performance metrics calculated in this study were based largely on results from simulation models of the passenger screening process and the spread of the epidemic in the country. The performance metrics were defined as follows.

### *5.2.1 System Performance of Screening System Metrics*

*5.2.1.1 Metric—Throughput of Passenger Screening System.* The throughput of the screening system was estimated by assessing the specific activities in different phases of the screening process. Subject-matter experts estimated the time needed by the screening station to complete each activity for a passenger, assuming that there is no one waiting in line.

*5.2.1.2 Metric—Effectiveness of Passenger Screening System.* The effectiveness of the system was assessed by considering the number and percentage of false negatives and false positives (false negatives are undetected infected passengers who enter the country; false positives are uninfected passengers who are significantly detained because they are thought to be infected). These estimates were tied to:

- the number and type of personnel needed to man the screening stations at the primary and secondary screening areas (the effectiveness of the system can be improved by devoting greater resources to it), and
- passenger waiting times (the effectiveness of the screening system is inherently tied to its impacts).

A passenger screening simulation model was used to calculate these metrics.

No metrics were calculated in the study for the reliability of the screening system, the ease of operating it or its usefulness to screeners.

***5.2.2 Metrics for the Benefits of Passenger Screening System.*** The overarching purpose of having airport entry screening of international passengers is to reduce the ultimate incidence and associated mortality of pandemic influenza in the country. Thus, the measures of benefits are the estimated reduction in cumulative incidence and associated number of deaths in the country, which are averted by having entry screening at the airport.

In the study cited, the incidence and number of deaths were estimated using simulation models. The major steps in that analysis are illustrated in Figure 1. The numbers in the figure are keyed to the steps in the simulation analysis:

1. Assumptions were made about the prevalence of the epidemic (i.e. the rate of illness in the population) in foreign regions from where passengers travel on international

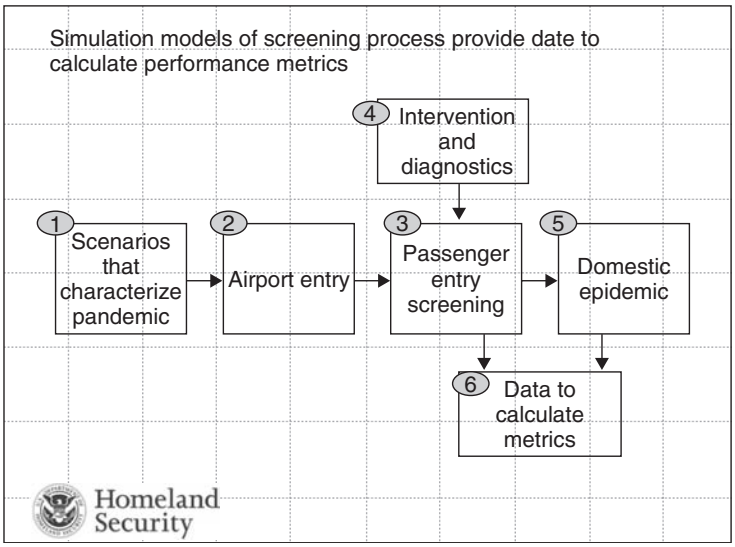



**FIGURE 1** Steps in simulation to develop data inputs to calculate performance metrics.

flights into the United States; these assumptions were made by subject-matter experts on the basis of past pandemics and their assessments of the severity of a future pandemic.

2. The volume of inbound international air traffic was estimated using data on individual flights, regions of origin, numbers of passengers on each flight and arrival times of flights, growth in future traffic, and the likely reduction in traffic volumes as a result of the pandemic.
3. A passenger screening simulation model was developed based on the passenger screening Concept of Operations (ConOps); it simulates the processing of each passenger at each stage of the screening process.
4. Estimates of the effectiveness of selected screening methods and screening processing times (if there is no waiting) were used in the passenger screening simulation model.
5. The key prediction of the passenger screening model is the number of false negatives, that is, the number of infected passengers who are not detected and who thus enter the country and soon infect others; the numbers of false negatives at each airport on each day were used as input data for a detailed agent-based epidemic simulation model that predicts the spread of the epidemic in the country.
6. The epidemic model computed the incidence each day, depending on the likelihood of an infected individual spreading the illness (based on evidence from other influenza epidemics) and mitigative measures implemented within communities such as vaccination, prophylaxis, and social distancing (e.g. closing schools and other activities); mortality was estimated using an assumed ratio of fatalities to cases.

***5.2.3 Metrics for Resource Needs and Costs of Passenger Screening System.*** Various resource needs were estimated using the passenger screening simulation model. For example, the ConOps calls for the possible use of antiviral prophylaxis at the airport, for passengers who might be exposed to the virus. Based on this protocol, the simulation model estimated the quantity of antiviral supplies needed. The quantity was based on the predicted number of suspected cases the screening system culls out.

***5.2.4 Metrics for Impacts of Screening System.*** One of the main impacts of passenger screening is that it causes delays. The passenger screening simulation model estimated the delay experienced by each passenger. The calculations were based on queuing principles that account for the number and timing of passenger arrivals at the airport, the prevalence of symptomatic passengers, the methods used in each screening layer to identify ill passengers, the effectiveness of these methods and the staff resources available for the screening activities.

The key metrics of the impacts were as follows:

- passengers' average delay time;
- passengers' maximum delay time.

The US government is using these metrics to help plan for the personnel needed for entry screening and to reduce these delays.

## 6 KEY CONCEPTS AND RECOMMENDATIONS ON FUTURE DIRECTIONS

Performance measures, and specific metrics for quantitatively evaluating these measures, are important means of gauging the value of alternative transportation security systems. Consistent definition and systematic use of performance measures are at a relatively early stage of development in terms of their application for *prospectively* assessing the *operational* performance of transportation security systems.

The focus of this article is on "prospectively" assessing their value, prior to making an investment and deploying a system. Testing under actual field conditions is the best means of developing the data needed to calculate performance metrics; computer models that simulate the system's operation in the field are an alternative means of compiling data, though not as good as actual field data. We emphasize that systems should be assessed by how they will perform *in practice*, after they are tested under controlled conditions.

## ACKNOWLEDGMENTS

Oak Ridge National Laboratory is a US Department of Energy facility managed and operated by UT-Battelle, LLC under contract number DE-AC-05-00OR22725. Some of the research referenced in this article was funded by the Transportation Security Administration of the US Department of Homeland Security and by the Office of Health Affairs

and the Science and Technology Directorate of the US Department of Homeland Security. All opinions in the article are solely those of the author and do not necessarily reflect the views of any of these institutions. The author is grateful to Jeffrey Western, Principal, Western Management and Consulting, for his review and comments on a preliminary draft of this article.

## REFERENCES

1. ExpectMore.gov (2008). *Expect Federal Programs to Perform Well, and Better Every Year*, Office of Management and Budget, Washington, DC, accessed June 10, 2008. http://www.whitehouse.gov/omb/expectmore/.
2. U.S. Government Accountability Office (2006). *Homeland Security: Guidance and Standards are Needed for Measuring the Effectiveness of Agencies' Facility Protection Efforts*, Report 06-612, GAO, Washington, DC, accessed June 10, 2008. http://www.gao.gov/new.items/d06612.pdf.
3. ANSI. (2004). *American National Standard for Evaluation and Performance of Radiation Detection Portal Monitors for Use in Homeland Security*, ANSI N42.35-2004 Institute of Electrical and Electronic Engineers, New York.
4. ANSI. (2004). *American National Standard for Evaluation and Performance of Transportable and Mobile Portal Monitors for Use in Homeland Security*, ANSI N42.43-2005. Institute of Electrical and Electronic Engineers, New York.
5. Krugler, P., Walden, M. N., Hoover, B., Lin, Y. D., and Tucker, S. (2006). *Performance Measurement Tool Box and Reporting System for Research Programs and Projects*, NCHRP 20-63, National Academies, Washington, DC, accessed June 10, 2008. http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_w127.pdf.
6. Jacobson, S. H., Bowman, J. M., and Kobza, J. E. (2001). Modeling and analyzing the performance of aviation security systems using baggage value performance measures. *IMA J. Manag. Math.* **12**(1), 3–22.
7. Chiaro, P. J. Jr. (2007). *Transportable Radiation Monitoring Systems (TRMS)–Volume 1: Technical Specifications*, prepared for the Transportation Security Administration, U.S. Department of Homeland Security, Oak Ridge National Laboratory, Oak Ridge, TN.
8. Lee, R., Chiaro, P. H. Jr., and Hu, P. (2007). *Transportable Radiation Monitoring System (TRMS) –Volume 5: Phase I Performance Evaluation*. in *a Controlled Environment*, prepared for the Transportation Security Administration, U.S. Department of Homeland Security, Oak Ridge National Laboratory, Oak Ridge, TN.
9. Lee, R., Hu, P., and Chiaro, P. J. Jr. (2007). *Transportable Radiation Monitoring System (TRMS) –Volume 6: Performance Evaluation*. in *a Field Operational Test*, prepared for the Transportation Security Administration, U.S. Department of Homeland Security, Oak Ridge National Laboratory, Oak Ridge, TN.
10. Lawrence Berkeley National Laboratory, Los Alamos National Laboratory, Oak Ridge National Laboratory and Pacific Northwest National Laboratory (2008). *U.S. Airport Entry Screening in Response to Pandemic Influenza: Modeling and Analysis*, prepared for the U.S. Department of Homeland Security, Oak Ridge National Laboratory, Oak Ridge, TN.
11. Brigantic, R. T., Malone, J. D., Muller, G., Lee, R., Kulesz, J., Delp, W., and McMahon, B. H. Simulation to assess the efficacy of U.S. airport entry screening of passengers for pandemic influenza. *Int. J. Risk Assess. Manag.* Invited paper for special issue on Biosecurity Assurance in a Threatening World: Challenges, Explorations, and Breakthroughs, forthcoming.

# INTELLIGENCE SYSTEMS

# FILE FORENSICS AND CONVERSION

Brian D. Carrier
*Basis Technology, Cambridge, Massachusetts*

## 1 INTRODUCTION

File forensics is the analysis of digital files to answer some form of question. For example, the question could be "which files contain the keyword X." This type of question is frequently asked in law enforcement and intelligence gathering contexts and the answer can identify if someone is guilty or innocent or identify people or places that are a threat or that are threatened. Files contain user-created content and are therefore crucial to learning about the actions of the computer's user. This article focuses on the state of the art and the challenges associated with file forensics. The other areas of digital forensics are outlined in other articles of this book. The first section outlines the general process of file forensics and the second section outlines the technology areas used. The third section describes the unique need areas that exist and the fourth section provides requirements for future file forensics efforts.

## 2 PROCESS OVERVIEW

### 2.1 Digital Investigation Process

File forensics fits into the larger area of digital investigations, which is also called digital forensics or media exploitation [1]. Digital investigations analyze digital data to answer questions about the current or previous state of the data or about previous digital events. The full process is similar to a physical crime scene investigation [2]. At a physical crime scene, the state is preserved by limiting access and taking pictures. Next, the scene is searched for evidence and the evidence is analyzed. Lastly, events are reconstructed based on the evidence at the scene to determine who did what and when.

At a "digital crime scene," the state of the digital media is preserved by making a copy of the data. Next, tools are used to analyze the data and the investigator searches for files or fragments of deleted files that could be relevant. In the physical world, evidence can typically be seen by the naked eye, but specialized tools are needed in the digital world to process and display the digital evidence. These tools can process various types of file systems, file formats, and network protocols. After the evidence has been identified, the

investigator tries to put them into context. Which user and program created them, when were they created, or what do they mean?

Because of the design of storage media, there are several layers of data analysis that occur [3]. When analyzing a hard drive, first the volume system and partition tables must be analyzed to identify how a hard drive was partitioned. Next, the file systems in each volume are analyzed to identify the files and to recover deleted content [4]. The next step, which is file forensics, is to analyze the contents of each file. Similar layers exist for network and memory data.

### 2.2 File Forensics Process

The file forensics process starts with a file or some other discrete amount of data. The file could be from a hard drive, a network trace, or extracted from memory. Because files are used to store data ranging from text to video, there is no single analysis process. For the sake of this article, we will start with the high-level process, which has two steps: file type identification and analysis.

The first step in the high-level process is to identify the file type, such as JPEG or PDF. The most reliable method for doing this is to look for signatures in the file content. For example, Adobe PDF files start with the bytes 0x25, 0x50, 0x44, and 0x46, which represent the letters "%PDF" in ASCII. JPEG files start with the bytes 0xffd8 and end with the bytes 0xffd9.

Signatures are not guaranteed to be unique and because a file has a sequence of bytes that matches a signature does not mean that it is that file type. Therefore, it is important to validate other data in the file after a signature is found and to look for all known file type signatures instead of stopping after the first match.

Some programs, such as Microsoft Windows, use file name extensions to identify the file type, but this is not reliable because the user could have changed the extension to avoid detection. Also, some deleted files do not have names.

After the file type is identified, the second step in the high-level process is to analyze the data using knowledge about that file type. This step allows tools and analysts to access the user created content. Although there are many tools that can open files, it is often best to use specialized tools that can display deleted and hidden content and that do not modify the file.

## 3 RESEARCH AREAS USED

File forensics can encounter any type of file and therefore its needs are diverse. The process of identifying file types is well understood, but the analysis process has many challenges. Specifically, the challenges include having a single tool that supports all file formats and being able to process large amounts of data. Fortunately, these challenges are not unique to digital forensics and are shared by the information retrieval, natural language processing, and graphics communities. In this section, we will outline the research areas that are used in file forensics. Because of space limitations, the high-level concepts and areas will be identified, but detailed approaches are not given.

### 3.1 File Formats

One of the largest challenges with digital investigations is dealing with the vast number of different file formats. The breadth of file types that are relevant to investigations is increasing and no single analysis tool supports them all. A computer intrusion

investigation will need to analyze executable files to detect malware and rootkits [5] and will need to analyze log files to look for suspicious activity. An investigation about downloading contraband images (i.e. child pornography) from the Internet will need to analyze web history files and graphic file formats [6]. Terrorism cases may focus on web histories, e-mails, chat sessions, and videos.

The extraction of text or multimedia data from files is largely an engineering problem. Each file format is created using a specification and if the specification is known then a program is created to support it. If the format is not known, then reverse engineering techniques are typically used to identify the data structures and algorithms used.

The unique need for file forensics is that deleted content and change histories, if they exist, need to be recovered. For example, there are many tools that can extract messages from PST Outlook files, but they do not return the deleted messages that are still in the file.

### 3.2 Metadata Extraction

A general forensics concept that applies to all file formats is metadata extraction. In general, file formats are created to store a specific type of data, such as image data or text. Many formats also have metadata, which is data about the data.

Metadata typically contains information such as which application or user created the file content and the date the file content was created. The metadata may also contain information about the computer or digital device that was used to create the content. For example, JPEG files frequently contain metadata about the camera and settings used to take a picture.

The amount of metadata varies by file type and not all programs that create the files will fill in all metadata. For example, PDF and Microsoft Office files allow the user to save metadata about the author and title of the documents, but they are not required to be entered.

Metadata can be used by an investigator to determine who created the file and on what computer. It can also be used to correlate documents that may have been created by the same person.

### 3.3 Documents

Documents store text by mapping the characters in the text to numbers. Those numbers are saved in the file and are remapped to the characters when the file is read. Over the years, many character to number mappings have been defined and many are script-specific. The exception is the Unicode specification, which supports nearly all scripts [7].

Documents come in many forms, which can be organized into two basic categories. At the most basic, there are raw text files that contain only the encoded text with no markup for sections, fonts, or styles. These files have no file type signature. To process these types of files, a program must identify the text encoding, which can be done using statistical techniques.

The second category of documents has structure that describes the font and style of the text and may contain embedded data, such as images and tables. Common examples of this category include HTML, XML, Microsoft Office files, PDF, e-mails, and chat logs. Most documents fit into this category. To process these types of files, a program must know the internal structure of the file format and process it accordingly. In many cases, the file stores the text encoding that was used.

Once the files have been processed and the text has been decoded, there are many analysis techniques that are conducted. The most basic technique is that the text is

displayed to the investigator so he/she can read it. However, the text in each file could be long and the investigator may not have enough time to read all files. This problem has also been researched by the Information Retrieval community.

To reduce the number of files to look at, the documents are typically searched for keywords. While this is a technique that we all use to find documents on internal servers and websites, the requirements for doing a search during a digital investigation can be stricter. The document that contains incriminating or exculpatory evidence may have a typo or spelling variation of the keyword. To deal with this situation, searches can be conducted using "fuzzy" matching [8] or text normalization. With text normalization, words are reduced to a normal form using text analytics. For example, the British word "colour" could be normalized to "color".

There are several techniques that can be used to reduce the time required to analyze each document. If names are important, then information and named entity extraction techniques can be used to statistically analyze the text and highlight or extract the people and places that are mentioned [9]. Another approach is to use automated text summarization techniques to create a summary of the key ideas in the document [10].

Clustering and classification can be used to reduce the number of files that need to be looked at [11]. Clustering takes the search results and groups them together based on concepts. This allows the investigator to examine one of the files in the cluster and then move on to another cluster if its topic is not relevant. Classification will organize the search results based on specified categories, such as topics or file types.

When investigations deal with text in languages that the investigator does not speak, then machine translation becomes a needed technology. Machine translation automatically translates text from one language to another. Because machine translation is difficult and the result of the process can be difficult to read, name translation [12] is an alternative middle step. In this approach, names in the text are identified and transliterated from the native script to Latin script (i.e. A to Z) so that the phonetic sound of the names can be determined.

### 3.4 Multimedia Files

Multimedia files are also of interest during digital investigations. Picture and video files may contain images of relevant people or locations. Audio files may contain relevant messages or instructions.

Digital image processing techniques [13] can be used to identify similar images, to identify which images contain skin tones, and to perform object or face recognition. Images are also frequently analyzed to detect if messages are hidden in them using steganography [14].

Like documents, multimedia files also have challenges with search and summarization. Multimedia files cannot be easily searched to identify ones with content on a specific topic. Also, it is time consuming to review long movies and audio. Summarization techniques can help to show summaries of the data when major things change, such as when the scene in a video changes or when the audio profile changes. These summarization techniques could help to find data that is hidden among other data. For example, a movie could start off with scenes from a family vacation, but could then have a message from a terrorist leader a few minutes into the movie.

### 3.5 Executable Files

Some investigations require the analysis of executable files. This can occur when unknown programs are installed during a computer intrusion or found on a suspect's

computer. Analysis techniques for executables include static analysis where the executable file is analyzed and dynamic analysis where the file is run and monitored [15].

Static analysis can provide basic information by identifying what libraries and system functions the file uses. Text from the file can also be extracted to provide insight about what messages are displayed to the user.

Dynamic analysis is more dangerous, but can provide more insight because the file and network traffic can be observed. However, the program could damage the local computer, spread to other computers on the investigator's network, or send a message that would alert someone that the program was run from the investigator's network. Virtual machines are commonly used for dynamic analysis because they can be easily restored to a clean state. However, some malware can detect when it is being run in a virtual machine and will stop running to prevent dynamic analysis.

### 3.6 Correlation

The previous sections outlined high-level techniques for extracting information from different file types, but sometimes it is useful to correlate data among the different file types. From a time perspective, it could be useful to correlate log entries, web browser histories, e-mail messages, and file modification times so that a timeline of activity can be created. Similarly, it could be useful to correlate IP and e-mail addresses found in log messages, e-mails, and executables. Social networks can be created by the analysis of e-mail messages and chat logs. The ability to correlate results may identify new systems or people on which to focus.

## 4 CRITICAL NEEDS ANALYSIS

As described in the previous section, much of the nonengineering file forensics challenges are not unique to digital forensics. They are challenges common to information retrieval, text analytics, digital image processing, and software engineering.

Advances in machine translation, video and audio search, object recognition in images, and multimedia and text summarization will all have a positive impact on file forensics. These advances will help to sift through the growing amount of data that investigators encounter and their needs are outlined in other sections of this book. In this section, we will outline some of the unique needs of file forensics.

### 4.1 Plug-in Infrastructure

While many of the need areas are not unique to file forensics and research is underway, it is unique that file forensics needs to leverage all of these areas at the same time. Currently, no single tool supports all of the techniques needed for file forensics, including the ability to extract text from all document formats, process multimedia files, and reverse engineer executables. There is a need for an open plug-in infrastructure that allows multiple file forensics modules to be used in a single analysis tool. This infrastructure would allow an investigator to use a single interface to analyze all of the file types that they would encounter instead of needing to export and import files between multiple tools.

A plug-in infrastructure could also allow the investigator to use modules from competing vendors and have them vote on the result. It is best practice in digital forensics to verify the results of one tool with another tool. This process could be automated with a plug-in infrastructure.

### 4.2 File Carving

A unique requirement of file forensics is the need to extract files from a blob of data. This scenario can occur when you have a large amount of unallocated space in a hard drive. A file could be inside of this data, but the file system structures that identified the file layout have been overwritten.

The traditional method of recovering these files, [16], is to scan for file type signatures. When a byte sequence is found, which matches the header signature, it is assumed that the file starts at that location and the algorithm then searches for the end of the file. Some files have a footer signature, but others do not. If a footer signature exists, then the basic algorithm is to assume that everything in between the header and footer is part of the file. If the file type does not have a footer signature and there is no value for the size of the file in the header, then a default length is assumed and all data between the header and the default length is extracted.

The problem with this approach is that files are not always contiguous on the disk. Files are broken up into blocks, typically from 4 to 16 KB, which can be stored in any order in any part of the disk. Files that have noncontiguous blocks cannot be recovered by this simple carving method.

Initiated by the DFRWS 2006 and 2007 Forensics Challenges [17, 18], new carving algorithms have been developed that take more of the file structure into account so that fragments can be detected. See [19] and the challenge submissions for more details. Additional work into this area is needed to improve the algorithms and expand the file formats that are supported.

### 4.3 Non-English Text Extraction

During a digital investigation, an unknown file format may be encountered or a blob of data may exist that cannot be carved any further. In this situation, it is common to analyze the data to look for possible text.

For English text, this approach will search for four or more consecutive 1- or 2-byte values that could be printable ASCII or Unicode characters. This is the approach used by the Unix strings command. In general, this approach is successful at extracting text and it has a low false positive rate. With ASCII, 37% of the 1-byte values are printable characters and the probability of finding four consecutive printable values in random data would be 1.8%.

When non-English text is considered, the false positive count dramatically increases because the probability of finding four or more printable Unicode characters is much higher. With Unicode, 80% of the 2-byte values are printable characters and the probability of finding four or more consecutive printable values in random data would be 41%. New approaches that reduce the false positive rate are needed to extract non-English text.

## 5 RESEARCH DIRECTIONS

The requirements for the research areas previously mentioned are as follows:

- Accuracy
- Speed
- Scalability

- Modular with plug-in support
- Multilingual

Accuracy is needed to ensure that investigators can state that data does not exist when searches do not find it. Similarly, it is needed so that an investigator can state that something existed because it was observed.

Speed is a requirement because some incidents will require quick results. There could be a time limit on the duration that a suspect can be held and his computer needs to be analyzed in that time frame. In the battlefield, a soldier may want to quickly scan a computer to extract intelligence about where threats and targets are located.

As hard drives increase in size and more portable devices are used, scalability is a requirement so that systems can handle the data. Distributed systems, central databases, and analysis interfaces that encourage collaboration are needed to sort through the massive amounts of data.

Because the needs of file forensics are diverse, systems should be modular with plug-in support so that a single system can be used to handle the diverse set of scenarios that can be encountered. The need to export data from one tool to import it into another can introduce errors and prevents the systems from being more fully automated.

Lastly, digital forensics has historically focused on searching English text. As investigations involve computers in multiple languages and as the military and intelligence increasingly focus on non-English systems, the tools need to better handle searching non-English text. When analyzing systems that contain text in languages that the analyst does not understand, the tools need to help with translating keywords and text. The tools also need to help with identifying spelling variations of a word.

## REFERENCES

1. Garfinkel, S. L. (2007). *Document & Media Exploitation*. ACM Queue. November 2007.
2. Carrier, B. D. and Spafford, E. H. (2003). Getting physical with the digital investigation process. *Int. J. Digit. Evid.* **2**(2), 2.
3. Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. *Int. J. Digit. Evid.* **1**(4).
4. Carrier, B. (2005). *File System Forensic Analysis*, Addison Wesley, NJ.
5. Hoglund, G. and Butler, J. (2005). *Rootkits: Subverting the Windows Kernel*, Addison Wesley, NJ.
6. Casey, E. (2004). *Digital Evidence and Computer Crime*, 2nd ed., Elsevier Academic Press, CA.
7. Unicode Consortium (2007). *The Unicode 5.0 Standard*, Addison Wesley, NJ.
8. Navarro, G. (2001). A guided tour to approximate string matching. *ACM Comput. Surv.* **33**(1), 31–88.
9. Cardie, C. (1997). Empirical methods in information extraction. *AI Mag.* **18**(4), 65–79.
10. Mani, I. and Maybury, M. T. (1999). *Advances in Automatic Text Summarization*, MIT Press, MA.
11. Manning, C. D. and Schuetze, H. (1999). *Foundations of Statistical Natural Language Processing*, MIT Press, MA.
12. Knight, K. and Graehl, J. (1997). Machine transliteration. *Proceedings of the Thirty-Fifth Annual Meeting of the Association for Computational Linguistics*, Madrid Spain.

13. Gonzalez, R. C. and Woods, R. E. (2008). *Digital Image Processing*, 3rd ed., Pearson Prentice Hall, NJ.
14. Wayner, P. (2002). *Disappearing Cryptography*, 2nd ed., Morgan Kaufmann, CA.
15. Skoudis, E. and Zeltser, L. (2004). *Malware: Fighting Malicious Code*, Prentice Hall, NJ.
16. Richard, G. G. and Roussev, V. (2005). Scalpel: a frugal, high performance file carver. *Proceedings of the Fifth Annual Digital Forensic Research Workshop*, New Orleans, LA.
17. Carrier B, Eoghan C, and Venema W. *Digital Forensic Research Workshop* (2006). File Carving Forensic Challenge. Available at: http://www.dfrws.org/2006/challenge/.
18. Carrier B, Eoghan C, and Venema W. *Digital Forensic Research Workshop* (2007). File Carving Forensic Challenge. Available at: http://www.dfrws.org/2007/challenge/.
19. Garfinkel, S. L. (2007). Carving Contiguous and Fragmented Files with Object Validation. *Proceedings of the Seventh Annual Digital Forensic Research Workshop* Pittsburgh, PA.

## FURTHER READING

Manning, C.D., Raghavan, P., and Schutze, H. (2008). *Introduction to Information Retrieval*, Cambridge University Press, NY.

Witten, I.H. and Frank, E. (2005). *Data Mining*, 2nd ed., Morgan Kaufmann, CA.

Witten, I.H., Moffat, A., Bell, and T.C. (1999). *Managing Gigabytes: Compressing and Indexing Documents and Images*, 2nd ed., Morgan Kaufmann, CA.

# CRANIOFACIAL AGING

KARL RICANEK JR, AMRUTHA SETHURAM, AND ERIC K. PATTERSON

*Computer Science Department, University of North Carolina Wilmington, Wilmington, North Carolina*

ARLENE M. ALBERT

*Anthropology Department, University of North Carolina Wilmington, Wilmington, North Carolina*

EDWARD J. BOONE

*Statistics Department, Virginia Commonwealth University, Richmond, Virginia*

## 1 SCIENTIFIC OVERVIEW

Medical and forensic studies have been conducted for quite some time on various aspects of human aging and its relation to changes in the face [1–4], but few studies have

addressed the effects of aging on face biometric technologies. There have been a few studies conducted recently with regards to modeling the effects of growth and development (i.e. the stage from birth to maturation) for application to face recognition technologies [5–10]. Although similar approaches to studying growth and development and adult aging may yield improvements in biometric technologies, the two processes are distinct, and therefore, should be studied separately for more accurate modeling of the underlying processes [3, 4].

Some work has been conducted concerning simulation of aging in facial images or models, considering a few different approaches. One approach is biomechanical simulation, and work in this area has included a layered facial simulation model for skin aging with wrinkles [11], an analysis–synthesis approach to aging the orbicularis muscle in virtual faces [12], and a flaccidity-deformation approach [13]. Anthropometric deformation approaches have also been attempted for both adult aging [14] and growth and development [15]. In one of recent works [16], a twofold approach toward modeling facial aging in adults is proposed. In this work, a shape transformation model that is formulated as a physically based parametric muscle model that captures the subtle deformations facial features undergo with age is developed. Next, an image gradient–based texture transformation function that characterizes facial wrinkles and other skin artifacts often observed during different ages is developed. Other approaches have also simulated aging through direct image manipulation of shape and texture, mainly for testing human perception [17, 18]. A summary of existing research on craniofacial aging, age-progression, and face biometric techniques that address the effects of aging directly are presented in the following sections.

### 1.1 Craniofacial Aging: Findings in Anthropology and Forensics

The craniofacial region of a human is where, effects of aging that would significantly impact human or computer recognition of individuals occurs. These changes include both the bony portion of the head as well as the overlying soft tissues that produce the external appearance of one's face. There is a large body of literature concerning this facial morphology due to aging that may be referenced to learn aspects that should be considered for face recognition technologies [4, 19, 20].

Our modern approach to studying age-related changes to the craniofacial complex can be traced back to D'Arcy Thompson's now classic work, first published in 1917—*On Growth and Form*—in which he explained shapes in the biological world in part through mathematics [21]. Contemporary studies indeed suggest that cardioidal strain transformation, a nonlinear topographical transformation, may be a reasonable mathematical model through which to observe major changes in craniofacial shape affected by growth [22, 23]. However, cardioidal strain transformations cannot account for other aging features such as hair, skin elasticity and texture, adipose tissue, nose, ears, eyes, and lips [24]; therefore, its importance in recognizing faces as they age should not be overestimated [25]. While three-dimensional shape changes may affect perceptions of aging, there is also evidence to suggest that age perception is highly dependent on internal facial features as well—eyes, lips, nose, and ears [26]. Indeed, the distinction between feature-based and configurational information is one of the ultimate challenges in face recognition [26]. Key features changing with adult age are noted below.

Degenerative soft tissue changes and small shifts in skeletal form ultimately affect the appearance of the face during aging. The skeletal changes include cranial expansion,

anterior face-height increase, and jaw shrinkage [20]. Soft tissue appearance is affected by decreasing muscle tone or atrophy, diminishing collagen and elastin, and skin wrinkling and sagging. Along with these natural changes that occur with aging, there are other aspects that affect facial appearance over time. Of these, photoaging is one of the most significant—largely impacting fair-skinned individuals and those residing in sunny regions [4]. Other major factors include ancestry, gender, health and disease, tobacco and drug use, diet, stress-related sleep deprivation, biomechanical factors, gravity, and hyperdynamic facial expressions [4, 20]. In addition, there are factors that can exacerbate age-related changes such as weight loss due to illness, drug use, and/or some medications [4, 19].

These changes are not consistent but vary in rate over adulthood. As expected, fewer changes generally occur in the twenties, accelerating a little in the thirties, and increasing even more in the forties and fifties—typically the period of greatest change. This period of greater morphology is fairly consistent across race and gender. Past the fifties, the changes that have begun increase significantly and other associated degenerative affects may appear.

Figure 1 illustrates the changes in an aged female with annotated points. Changes to note beginning in the twenties and thirties include horizontal creases in the forehead (areas 1 and 2), slight drooping of the eyelids (area 6 and 9), nasolabial lines or "laugh lines" (areas 16 and 17), lateral orbital lines or "crow's feet" (area 7), circumoral striae (which are lines around the mouth) (areas 18 and 20), hollowing of the cheek (around area 15), decrease in upper lip size (area 21), and retrusion (which is a backward movement of the upper lip that is more apparent in females) [4, 19, 20].

Through the adult aging process these changes become more noticeable, and by or around the age of 50, there are other changes that have begun including the appearance of fine lines, and thinning and sagging of skin as shown in Figure 2. Skin also becomes rougher, drier, and shows loss of tone and elasticity. This combined with atrophy in corrugator and orbicularis muscles can affect facial appearance greatly. Wrinkles appear on the neck, and discolorations in skin may begin to appear. Loss of hair and depigmentation may occur. Hair may also grow in areas that previously had little or no growth [4, 20].

In general, trends occur that affect facial size as well. Small skeletal changes in height and width affect the outer appearance of the soft tissue. Nose height and length increases, and ear length increases. Mouth width also increases. In very aged people, faces may appear smaller due to overall degeneration of the boney substructure (craniofacial complex) and tissue degeneration.

Table 1 summarizes the soft tissue and hard tissue changes that occur at various age spans [3].

## 2 CRITICAL NEEDS ANALYSIS

Face recognition has been a key biometric research area for more than a decade. This technology has had mixed, almost disappointing, results when applied in commercial venues [27–29]. Nonetheless, robust face recognition systems are needed to meet the demands of intelligence agencies, military, and, more broadly, homeland security. Face recognition systems used for identification or watch lists require enrollment, which is the process of learning known faces. The performance of these systems deteriorates after a


**FIGURE 1** Annotated diagram of craniofacial morphology.

few years unless the system is updated with current faces of the known subjects. The degradation of performance of these systems has been demonstrated, but not studied in depth, as far back as the original Face Recognition Technology (FERET) evaluations [30]. They were also further highlighted in face recognition vendor test (FRVT) 2002 [31]. The paucity of research on this topic can be summarized as (i) the algorithm developers had little to no understanding of the complete biomechanical processes that affect facial aging and (ii) there are only a few publicly available longitudinal face databases. The following section details the known longitudinal databases and summarizes the results of recent work in quantifying the effects of age-progression and automatic synthesis of adult aging in facial images.

### 2.1 Longitudinal Face Databases

The FERET, FRVT, and face recognition grand challenge (FRGC) are programs sponsored by Defense Advanced Research Projects Agency (DARPA)/National Institute of Standards and Technology (NIST)/Central Intelligence Agency (CIA) to further biometrics research and each has created vast data corpora to facilitate the analysis and evaluation of various biometrics. Furthermore, each program contains face databases designed to meet the mandate of each challenge. The FERET face database (1994), which continues to be used by researchers worldwide, contains a set of longitudinal images in its Duplicate I and Duplicate II data sets. The Duplicate I probe set holds 722 images whose matches were taken between 0 and 2.8 years after the match. The median is 2 months

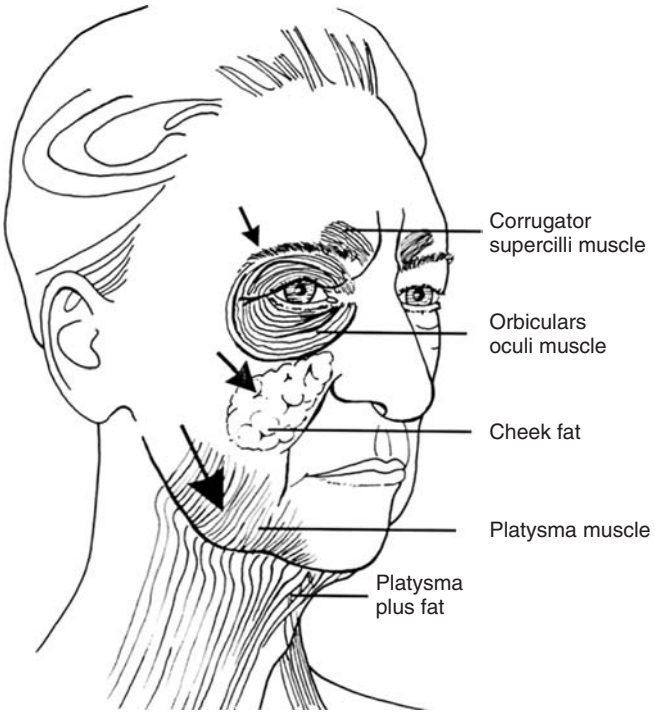



**FIGURE 2** Illustration of aging: impacts on soft tissue (musculature and skin) demonstrating wrinkling and muscle sagging.

and the mean is 8.25 months. The Duplicate II probe set contains 234 images from subjects whose match was taken between 540 and 1031 days beforehand. The median is 1.5 years and the mean is 1.7 years. The challenge of using FERET is sparseness of subjects, unknown ages, and diversity of gender and ethnicity. The FRVT 2002 database was comprised of longitudinal images of subjects with some ethnic diversity, but this was not released for general public research as was the FERET. Additional information can be obtained on this database from the website (www.frvt.org). The FRGC primary objectives did not include the problem of age-progression or gallery-probe acquisition differences.

The Face and Gesture Recognition Research Network (FG-NET) Aging Database [32] constructed by Andreas Lanitis at Cyprus College, is constructed from scanned photographs provided by volunteers. The photographs range from childhood to senescence of 82 subjects under various pose and facial expressions. The database does not provide researchers with important parameters like ethnicity, height, or weight.

The Craniofacial Morphological Face Database, MORPH, is a longitudinal face database developed for researchers investigating all facets of adult age-progression [33]. The MORPH database includes metadata on the face images within the database: subject's ethnicity, height, weight, gender, and age. Figure 4 is a sample of two subjects from the database highlighting appearance changes of adult faces. The database is partitioned into two albums, Album 1 and Album 2. Album 1 consists of 1690 images of 628 subjects that were scanned from photographs taken as far back as the 1960s. Album 2 has over 55,608 digital images of 13,673 subjects which consist of males

**TABLE 1 Adult Hard and Soft Tissue Age-related Changes**

| Approximate Age Range (years) | Likely Bony Change | Probable Soft Tissue or Facial Appearance Effect |
|---|---|---|
| 20–30 | Slight craniofacial skeletal growth | Upper eyelid drooping begins |
| | Slight anterior (mostly lower) face height *increase* | Eyes appear smaller |
| | | *Nasolabial* lines begin to form |
| | *Mandibular* length increase | Lateral orbital lines begin to form |
| | | Upper lip *retrusion* begins in females |
| 30–40 | *Dentoalveolar* regression suggesting eruptive movement of teeth | *Circumoral striae* begin to form |
| | | Lines begin to form from lateral edges of nose *to* lateral edges of mouth. |
| | Maxillary *retrusion* progressing, contributing to *nasolabial* folds | |
| | *Mandibular* length increase | Upper lip thickness decreasing |
| 40–50 | Craniofacial skeletal remodeling progresses | Facial lines and folds continue to increase in depth |
| | Dental alveolar regression and dental eruption progressing | Nose and chin positioning affected as dental arch lengths decrease |
| | Maxillary and *mandibular* dental arch lengths decreasing | Most profound morphological changes of the head, face, and neck are evident |
| 50–60 | Craniofacial remodeling continues | Facial lines and folds continue to increase in depth. |
| | Cranial thickness likely unchanging | |
| | Alveolar bone remodeling | Protuberance of nose and ears due to greater craniofacial convexity |
| | Possible dental attrition affecting vertical face height | |
| <60 | Decrease in craniofacial size | Protuberance of nose and ears continues |
| | Greater craniofacial convexity (excluding maxilla and mandible) | Concave appearance in cheek hollows due to alveolar bone remodeling |
| | Possible *temporomandibular* joint arthritis and joint flattening | |
| | Alveolar bone remodeling continues | Diminished jaws |

and females of the Caucasian, Asian, Hispanic, and African ethnic groups; however, there are very few Asian and Hispanic samples. Detailed statistics are shown in Tables 2 and 3. The MORPH database is an ongoing project in the Computer Science Department at the University of North Carolina Wilmington and can be requested from www.faceaginggroup.com.

### 2.2 Effect of Adult Aging on a Standard Face Recognition Technique

The work of Ricanek and Boone 2005 [34] was an early attempt to quantify the effects of normal adult aging, age-progression, on a face recognition technique. In this work, the

**TABLE 2 Statistics for Morph Album 1**

| General | | Age Statistics (yr) | | | | |
|---|---|---|---|---|---|---|
| Number of Subjects | Number of Images | Minimum | Maximum | Average | Median | SD |
| 515 | 1690 | 16 | 68 | 27.28 | 26 | 8.65 |

Morph Album 1: Number of Facial Images by Gender and Ancestry

| | Americans of African Descent | Americans of European Descent | Americans of "Other" Descent | Total |
|---|---|---|---|---|
| Male | 1037 | 365 | 3 | 1405 |
| Female | 216 | 69 | 0 | 285 |
| Total | 1253 | 434 | 3 | 1690 |

Morph Album 1: Number of Facial Images by Decade of Life Categories (yr)

| | <18 | 18–29 | 30–39 | 40–49 | 50+ | Total |
|---|---|---|---|---|---|---|
| Male | 142 | 803 | 345 | 93 | 22 | 1405 |
| Female | 15 | 182 | 70 | 18 | 0 | 285 |
| Total | 157 | 985 | 415 | 111 | 22 | 1690 |

authors sought to quantify the impacts of aging against the standard principal components analysis (PCA)-face recognizer as implemented in the Colorado State University's Face Identification and Evaluation System (FIES). The FERET and MORPH databases were used for the evaluation. MORPH album 1 was used which contained large longitudinal images of more than 500 subjects whose images were scanned from photographs. The largest span was 20.3 years and the average was 6.45 years.

The work concluded that there was a statistically significant degradation in rank-N performance as evaluated as a function of age difference between enrolled and probe. To this end, the researchers were able to generate a function of performance loss using logistic regression. Table 4 shows the results of the logistic regression on correct classification on the time-differenced images. The table illustrates that the time difference is an important factor in determining the recognition rate with a p value $<0.0001$. Table 4 also shows the odds ratio associated with a 1 year increase in time between the enrolled image and the test (probe) image such that a 1 year increase would result in a rank-N performance decay of 0.6707. Figure 3 shows a graph of this relationship across time for rank 1 and Figure 4 illustrates the relationship for rank 5.

### 2.3 Face Recognition Using Synthetic Facial Aging

One of the several reasons that make testing variation in human faces due to aging, a difficult task, is data collection. Current face databases suffer from small number of subjects, less than a few hundred, and/or small number of or inconsistent age spans for subjects. There has been indication, though, that face recognition technologies are not well suited to perform invariantly across images of the same individual at different ages [6, 8]. As discussed in the previous section, the MORPH database has been developed to

**TABLE 3 Statistics for Morph Album 2**

| General | | Age Statistics (yr) | | | | |
|---|---|---|---|---|---|---|
| Number of Subjects | Number of Images | Minimum | Maximum | Average | Median | SD |
| 13,673 | 55,608 | 18 | 77 | 32.69 | 33 | 10.9 |

Morph Album 2: Number of Facial Images by Gender and Ancestry

| | Americans of African Descent | Americans of European Descent | Americans of "Other" Descent | Total |
|---|---|---|---|---|
| Male | 37,093 | 8119 | 1845 | 47,057 |
| Female | 5803 | 2617 | 131 | 8551 |
| Total | 42,896 | 10,736 | 1976 | 55,608 |

Morph Album 2: Number of Facial Images by Decade of Life Categories (yr)

| | <18 | 18–29 | 30–39 | 40–49 | 50+ | Total |
|---|---|---|---|---|---|---|
| Male | 2964 | 17,728 | 12,587 | 10,248 | 3530 | 47,057 |
| Female | 373 | 2783 | 2924 | 2017 | 454 | 8551 |
| Total | 3337 | 20,511 | 15,511 | 12,265 | 3984 | 55,608 |

**TABLE 4 Logistic Regression Parameters: Longitudinal Difference MORPH Training and FERET Training**

| Rank | Training | Time Difference | Standard Error | $p$ value | Odds Ratio |
|---|---|---|---|---|---|
| 1 | MORPH | −0.39941 | 0.07429 | <0.0001 | 0.6707 |
| | FERET | −0.36261 | 0.06714 | <0.0001 | 0.6958 |
| 5 | MORPH | −0.35702 | 0.05291 | <0.0001 | 0.6997 |
| | FERET | −0.33250 | 0.04983 | <0.0001 | 0.7171 |

help research improvements for face technologies across a wide span of age with this in mind. It has been used to make some initial tests of face recognition performance across wide spans of age samples [8]. A few other studies have also begun to investigate the possible effects of age and aging-related variation in the human face-to-face recognition technologies [5–10]. All of these initial studies have concluded that there is the possibility of significant degradation on the methods tested. Further study will need to expand these tests to very recent developments in face recognition technology that have shown significant performance increases in areas other than aging. Although it is still not known completely to what extent aging affects face-based biometric technologies, it is certain that it does have a strong impact on the appearance of the face and likely on most face recognizers.

Although the overarching theme is to develop robust, and to this end insensitive, face-based biometrics to the problem of age-progression the practical approach appears to be the development of synthesized imagery for enhancement of current methods.

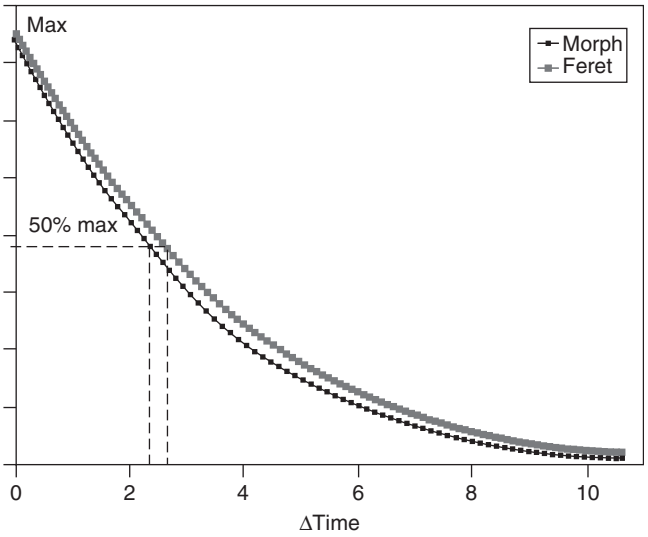



**FIGURE 3** Probability of rank 1 recognition performance against time span (years) between enrolled and probe image. Logistic regression was used to formulate the model and projected over a time span of 10 years (FERET projection used both Duplicate I and Duplicate II partitions).

Intelligently crafted synthetic images may be used to augment training galleries or be used to manipulate current test images to improve performance in a variety of areas. This approach is broadly known as *template aging* via generative synthetic templates.

Orlans et al. demonstrated augmenting FRVT 2000 findings for pose and temporal experiments by support with synthetic face image galleries using Singular Inversions' FaceGen software [35] and the Viisage [36] FaceTools commercial face recognition packages. They achieved a performance increase across pose variation tests by use of the synthetic images, and they demonstrated the individuality of the images in the synthetic gallery, but they also mentioned that it may be difficult to validate large galleries of synthetic faces. Also, 50 random faces were used and "aged" from 20 to 60 in 5-year increments with FaceGen [6]. FaceGen builds 3D faces synthetically using methods similar to those in [37] and allows for a gradient-based shifting of facial features, including age, but the statistical validity of these is not confirmed. With 128 principal components computed from 300 face scans, there may not be enough representation of aging among the population scanned, particularly across individuals to indicate idiosyncratic modes of aging [38]. Orlans et al. did mention that the statistical significance of this approach may be light but that recognition results degraded over "time" as represented by the synthesized test images.

Zhang et al. attempted to use a texture synthesis approach to correct for pose and illumination effects that degrade face recognition performance. Combined with a generic 3D face model and single frontal views, virtual views under different poses and illumination conditions were synthesized and used to augment the training gallery in a PCA-based recognizer and achieved a significant improvement in recognition accuracy across pose and illumination variations [39].

Lanitis and Taylor as well as Wang et al. have both conducted tests over the use of aging functions to improve recognition performance. Both of these cases, however,

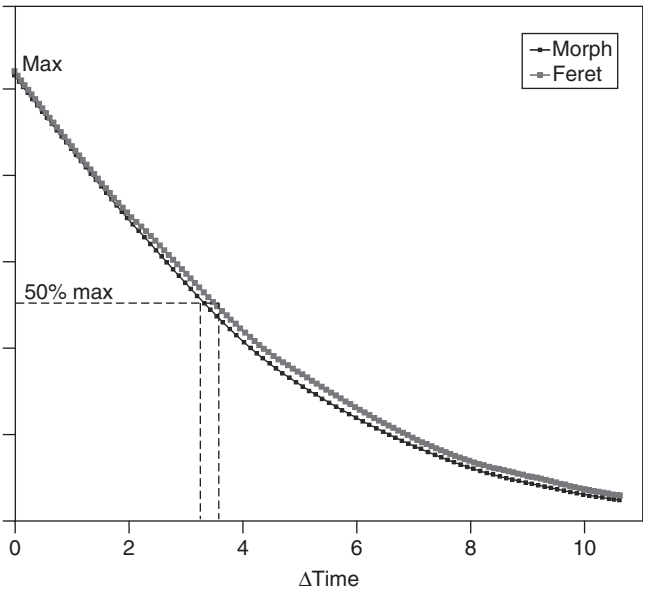



**FIGURE 4** Probability of rank 5 recognition performance against time span (years) between enrolled and probe image. Logistic regression was used to formulate the model and projected over a time span of 10 years (FERET projection used both Duplicate I and Duplicate II partitions).

considered images from human growth and development (birth to 18, 19–30 in the first case, and unknown in the second case), not specifically adult aging—a different period with different aspects and rates of change as represented in the anthropological literature. Growth and development has larger scale changes of structure as bones shift during growth. Adult aging in general has smaller structural shifts for a long period of time marked by larger changes of textural information in images. The system used by Lanitis and Taylor estimates the age of a test image and parametrically shifts it to the mean age of those represented in training [5]. Wang et al. appear to have used images from both growth and development and adult aging (a mean of 15-year age representation over 60 individuals, although the exact range of ages is not specified) and generate feature vectors of test faces at different ages [40]. Both cite improved performance in recognition, the first using an active-appearance-model (AAM)-based recognizer and the second a PCA-based recognizer. We have conducted brief initial tests indicating similar results. On a small subset of the MORPH database, with individual ages ranging from 18 to 40, PCA-based recognition was tested by augmenting the training gallery with "aged" images to match the current age of a test subject. Also, current test images were "de-aged" to match the range of ages of the individuals when gallery photos were taken. Although it was a very small test, the "de-aging" of the test images appeared to perform best for the given setup [9]. All of these initial studies have indicated a potential in some use of synthesized face information to improve biometric techniques.

We have recently conducted two initial studies using AAM-based approaches to synthetically age progressing and regressing images to represent adult aging effects to the face [41]. The first contained a small subset of the MORPH database [33]. Such is necessary to consider constructing individual or idiosyncratic models of face aging versus

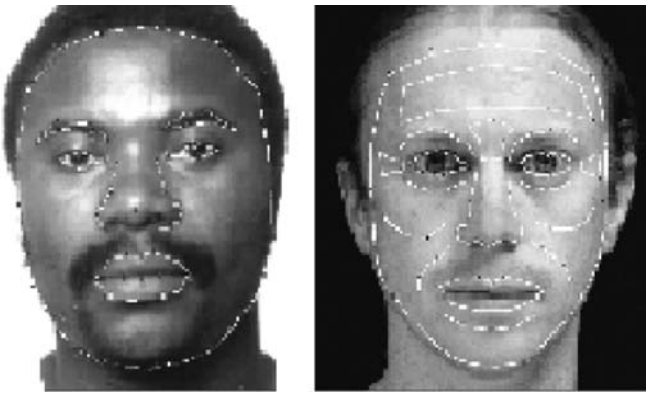


**FIGURE 5** Landmarks used in first and second setups.

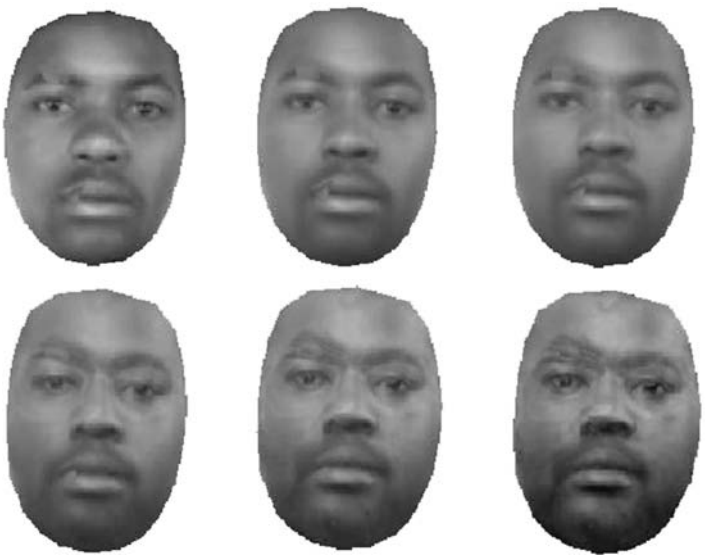


**FIGURE 6** Average faces over age-progression with first setup, from age 18 to 40.

generalized models which could be based on large databases of individuals of a variety of ages.

In the first setup, images from 9 individuals over a roughly 20-year period were used along with a set of 65 landmarks (which were mostly a superset of the anthropometric landmarks made popular by Farkas), shown in Figure 5, to construct an AAM with 30 parameters and representations of an aging estimation function and aging-lookup table similar to that presented in [42] but geared specifically toward adult aging. More details concerning the first tests are presented in [9]. A new image that will be progressed or regressed has its AAM parameters shifted by a difference of parameters taken from the difference of the average age parameters in the lookup table generated by Monte Carlo simulation [9, 42]. Examples of the average age-progression as represented by the lookup table are shown in Figure 6.

**FIGURE 7** Average faces over age-progression with second setup, from 20 to 70.

The second setup was designed to emulate a forensic sketch artist's approach to age-progression and was built with 99 images from a family, including young images of an individual along with images of parents and grandparents from the same family. One hundred and sixty one landmarks, also shown in Figure 5, were used to attempt to better track specific regions of aging in the face, and 55 AAM parameters were used, retaining 98% of the combined shape and texture variation. The desire was to present a better case study with improved image quality and texture resolution before continuing efforts on labeling and modeling the entire MORPH database.

A forensic sketch artist was employed to render sketches to be compared to the synthetic images. Examples of the average age-progression as represented in the second study are shown in Figure 7. Figure 8 demonstrates the loss of visual information and model construction as fewer parameters are chosen. The second setup uses 99 images but relatively few people, five individuals, to build a model, but it is in a sense a "family face space" that should and was proven to perform a reasonable representation of an individual and aging based on a wide representation of family images. It also represents one of the widest age ranges attempted so far, from approximately 20 to 70.

Age progressions generated with this setup and technique are shown in Figure 9. Similar experiments were likewise conducted in de-aging the family members, as shown in Figure 10. Also shown here is the difference image between the reconstructed AAM image of the individual at age 50 and the AAM image age regressed to 30. Although it may be difficult perceptually to notice changes depending upon presentation, and changes may be mild, the difference image demonstrates changes in both shape and texture and in probable regions as discussed henceforth. Parallels may be drawn about the regions in the face where rhytids, ptosis, loss of elasticity, and atrophy occur. Differences around

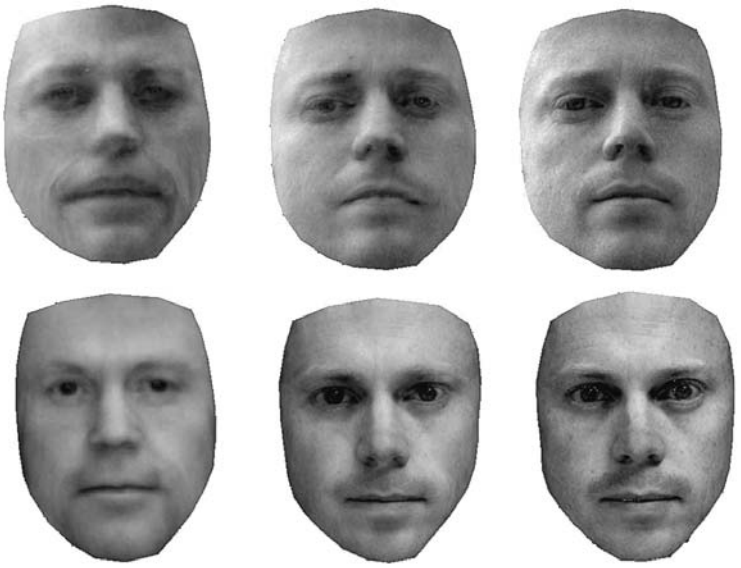


**FIGURE 8** Parameter variation with 10, 30, and 50 parameters.

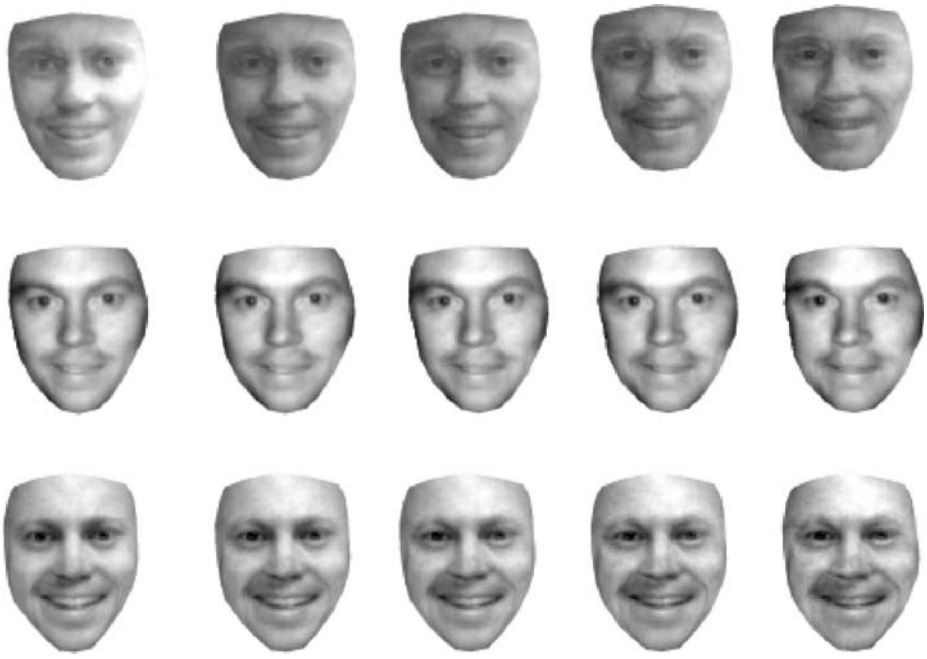


**FIGURE 9** Different images of an individual synthetically progressed from ages 23, 25, and 34 (top to bottom) to 40, 50, 60, and 70 (left to right).

**FIGURE 10** De-aging example from 50 to 30. Top images include original reconstruction, de-aged image, and difference image of reconstructed and de-aged. Bottom images are original and composite.

the outer edge of shape may correspond to suggested small changes in the face length and shape due to skeletal remodeling as well [3]. The difference image presented in Figure 11 demonstrates changes from 34 to 70 in an individual. Regions of change include the center forehead where documented rhytids and ptosis occur. Just inside of the orbital regions, changes are indicated, such as are present in the glabellar rhytidosis that occurs there. Regions above, below, and around the eyes also indicate change represented by the aging model that correspond to the areas where lid ptosis and rhytidosis and lateral

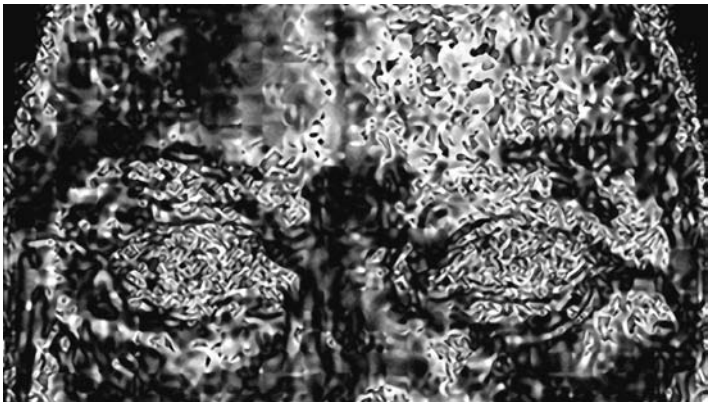


**FIGURE 11** Aging effects, upper facial region, as demonstrated by difference of progression.

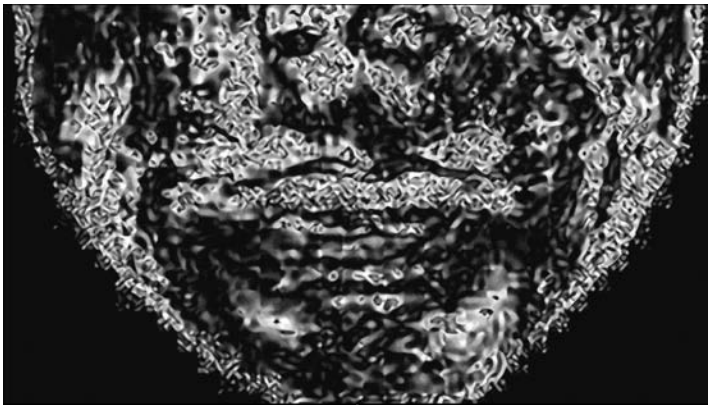


**FIGURE 12** Aging effects, lower region, as demonstrated by difference of progression.

canthal rhytidosis occur. In Figure 12, the lower region, similar comparisons may be made. Change is evident in the nasolabial regions that typically develop creases in older age; change is also apparent in the lip regions where thinning and atrophy often occurs; and some change is evident in the chin region where ptosis and retraction occurs [3, 4].

## 3 RESEARCH DIRECTIONS

The temporal results of FRVT 2000 show that recognizing faces from images taken more than a year apart remains an active area of research. Given the inadequacy of the existing databases, emphasis should be laid on significant data collection—both in breadth and depth of individuals which is the approach being sought by the developers of MORPH [33] and the collection work by Notre Dame's Kevin Bowyer and Patrick Flynn.

Some previous work in the area of growth and development centered on the deformations of bony changes as modeled with cardioidal strain maps, [43, 44] are arising for the study and modeling of adult age-progression. Cardioidal strain transformations can be described as geometric transformations of the face. Although this approach has been predominately used to model cranioskeletal changes of the face due to growth and development, researchers are applying this method to soft tissue (texture) deformation [7].

Fundamentally, the objective is to create face recognition (FR) systems that are resilient to adult age-progression by exploiting a feature space that is invariant over time; however, there has been a paucity of work in this area. Therefore, work in developing aggregate systems as in synthetic templates must continue. To this end, research should be directed toward quantifying the performance of FR systems on existing databases, generating metrics to judge synthesized age-progressed likeness, investigating and authenticating various aging techniques, and modeling age-progression with more input from metadata. From this work, a deeper understanding of aging will drive the development of age-robust FR systems.

To encourage more work in this critical area, more attention should be directed to this problem via workshops, symposia, and grand challenges. Finally, more funding should be made available in this active area of research (US and European Union funding of

this problem has dwindled whereas corporate research dollars are on the rise in many Asian countries).

## REFERENCES


1. Zhao, W., Chellappa, R., Phillips, P. J., and Rosenfeld, A. (2003). Face recognition: a literature survey. *Acm Comput. Surv*. **35**(4), 399–458.
2. Phillips, P. J., Flynn, P. J., Scruggs, T., Bowyer, K. W., Chang, J., Hoffman, K., Marques, J., Min, J., and Worek, W. (2005). Overview of the face recognition grand challenge. *In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. (CVPR 2005), San Diego, CA, June 2005, Vol. 2, pp. 947–954.
3. Albert, A. M., Ricanek, K., and Patterson, E. (2007). A review of the literature on the aging adult skull and face: implications for forensic science research and applications. *Forensic Sci. Int*. In Press, available online April 2007 Vol. 172(1), pp. 1–9.
4. Behrents, R. G. (1985). *Growth in the Aging Craniofacial Skeleton*, University of Michigan, Ann Arbor, Michigan. Center for Human Growth and Development, University of Michigan, Ann Arbor, Mich.
5. Lanitis, A., and Taylor, C. J. (2000). Towards automatic face identification robust to ageing variation. *In Proceedings of the Fourth IEEE International Conference on Automatic Face and Gesture Recognition*, Grenoble, France, pp. 391–396.
6. Orlans, N. M., Piszcz, A. T., and Chavez, R. J. (2003). Parametrically controlled synthetic imagery experiment for face recognition testing. *In Proceedings of the 2003 ACM SIGMM workshop on Biometrics Methods and Applications (WMBA '03)*, 2003, Berkeley, CA, 58–64.
7. Ramanathan, N., and Chellapa, R. (2005). Face verification across age progression. *In IEEE Conference Computer Vision and Pattern Recognition*. (CVPR 2005), San Diego, CA, June 2005, Vol. 2, pp. 462–469.
8. Ricanek, K., Boone, E., and Patterson, E. (2006). Craniofacial aging impacts on the eigenface face biometric. *In Proceedings of the Sixth IASTED International Conference on Visualization, Imaging, and Image Processing*. Palma de Mallorca, Spain, 249–253, August.
9. Patterson, E., Ricanek, K., Albert, A. M., and Boone, E. (2006). Automatic representation of adult aging in facial images. *In Proceedings of the Sixth IASTED International Conference on Visualization, Imaging, and Image Processing*. Palma de Mallorca, Spain, August.
10. Wang, J., Shang, Y., Su, G., and Lin, X. (2006). Age simulation for face recognition. *In 18th International Conference on Pattern Recognition*, Hong Kong, China. Vol. 3, pp. 913–916.
11. Wu, Y., Beylot, P., and Thalmann, N. (1999). Skin aging estimation by facial simulation. In *Computer Animation*, IEEE Computer Society, Washington, DC.
12. Berg, A. C., and Justo, S. C. (2003). Aging of orbicularis muscle in virtual human faces. *In Proceedings of the Seventh International Conference on Information Visualization*, London, England, UK, pp. 164–168.
13. Berg, A. C., Lopez, F. J. P., and Gonzalez, M. (2006). A facial aging simulation method: using flaccidity deformation criteria. In *Proceedings of Information Visualization*, IEEE Computer Society, Washington, DC.
14. Bastanfard, A., Takahashi, H., and Nakajima, M. (2004). Toward e-appearance of human face and hair by age, expression, and rejuvenation. *In Proceedings of the 2004 International Conference on Cyberworlds*, Tokyo, Japan, pp. 306–311.
15. Ramanathan, N., and Chellapa, R. (2006). Modeling age progression in young faces. *In Proceedings of the 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, New York, Vol. 1, pp. 387–394.

16. Ramanathan, N., and Chellappa, R. Modeling shape and textural variations in faces. *To appear in 8th IEEE Int'l Conference on Automatic Face and Gesture Recognition*, Amsterdam, The Netherlands.
17. Tiddeman, B., Burt, M., and Perrett, D. (2001). Prototyping and transforming facial textures for perception research. *IEEE Comput. Graph. Appl.* **21**(5), 42–50.
18. Burt, D. M., and Perrett, D. I. (1995). Perception of age in adult Caucasian male faces: computer graphics manipulation of shape and color information. *Proc. Biol. Sci.*, **259**(1355), pp. 137–143.
19. Taylor, K. T. (2001). *Forensic Art and Illustration*, CRC Press, Boca Raton, FL.
20. Zimbler, M. S., Kokoska, M. S., and Thomas, J. (2001). Anatomy and pathophysiology of facial aging. *Facial Plast. Surg. Clin. North Am*. **9**(2), 179–187.
21. Thompson, D. W. (1961). *On Growth and Form*, Cambridge University Press, Cambridge, UK,
22. Pittenger, J. B., and Shaw, R. E. (1975). Aging faces as viscal-elastic events: implications for a theory of nonrigid shape perception. *J. Exp. Psychol. Hum. Percept. Perform*. **1**(4), 374–382.
23. George, P. A., and Hole, G. J. (1995). Factors influencing the accuracy of age estimates of unfamiliar faces. *Perception* **24**(9), 1059–1073.
24. Pittenger, J. B., Shaw, R. E., and Mark, L. S. (1979). Perceptual information for the age level of faces as a higher order invariant of growth. *J. Exp. Psychol. Hum. Percept. Perform*. **5**(3), 478–493.
25. Burt, D. M., and Perett, D. I. (1995). Perception of age in adult Caucasian male faces: computer graphic manipulation of shape and colour information. *Proceedings: Biological Sciences, The Royal Society* **259**(1355), 137–143.
26. George, P. A., and Hole, G. J. (1998). The influence of feature-based information in the age processing of unfamiliar faces. *Perception* **27**, 295–312.
27. Security Management (2002). *Tampa Facial Recognition a Failure, ACLU Claims*, March.
28. Security Management (2002). *Face Recognition Blasted Again*, August.
29. Turk, M., and Pentland, A. (1991). Face recognition using eigenfaces. *Proc. Int. Conf on Pattern Recognition* 586–591.
30. Phillips, P. J., Rauss, P. J., and Der, S. Z. (1996). *FERET (Face Recognition Technology), Recognition Algorithm Development and Test Results*, Technical Report 995,Army Research Lab.
31. The Facial Recognition Technology (2006). *(FERET) Database*, June 22, 2006. http://www.itl.nist.gov/iad/humanid/feret/feret_master.html.
32. FGNET. *Aging Database*, http://www.fgnet.rsunit.com/, 2007.
33. Ricanek, K., Boone, E., and Patterson, E. (2005). *"MORPH:A Craniofacial Morphological Database"*, UNCW-TR03.
34. Ricanek, K., and Boone, E. (2005). The effect of normal adult aging on standard PCA face recognition accuracy rates. *Proceedings of IEEE International Joint Conference on Neural Networks*, *2005*. *IJCNN*. Montreal, Canada, Aug. 2005. Vol. 4, pp. 2018–2023.
35. *FaceGen*, http://www.facegen.com/, 2007.
36. *Viisage Facetools*, http://www.l1id.com/, 2007.
37. Blanz, V., and Vetter, T. (1999). A morphable model for the synthesis of 3d faces. *In SIGGRAPH International Conference on Computer Graphics and Interactive Techniques*, Los Angeles, CA pp. 187–194.
38. Chen, T.-P. G., and Fels, S. (2004). Exploring gradient-based face navigation interfaces. *In Proceedings of the 2004 Conference on Graphics Interface*, Ontario, Canada, pp. 65–72.

39. Zhang, X., Gao, Y., and Leung, M. K. H. (2006). Automatic texture synthesis for face recognition from single views. *In The 18th International Conference on Pattern Recognition*, Hong-Kong, China, **3**, 1151–1154.
40. Pitanguy, I., Leta, F., Pamplona, D., and Weber, H. I. (1996). Defining and measuring aging parameters. *Appl. Math. Comput*. **78**, 217–227.
41. Patterson, E., Sethuram, A., Albert, M., Ricanek, K., and King, M. (2007). Aspects of age variation in facial morphology affecting biometrics. *First IEEE International Conference on Biometrics: Theory, Applications, and Systems, BTAS 2007*. Washington, DC, 1–6, 27-29 Sep 2007.
42. Lanitis, A., Taylor, C. J., and Cootes, T. F. (2002). Toward automatic simulation of aging effects on face images. *IEEE Trans. Pattern Anal. Mach. Intell*. **24**(4), 442–455.
43. Mark, L. S., Pittenger, J. B., Hines, H., Carello, C., Shaw, R. E., and Todd, J. T. (1980). Wrinkling and head shape as coordinated sources of age level information. *Perception and Psychophysics* **27**, 117–124.
44. Mark, L. S., Todd, J. T., and Shaw, R. E. (1981). Perceptions of growth: a geometric analysis of how different styles of change are distinguished. *J. Exp. Psychol. Hum. Percept. Perform*. **7**, 855–868.

# NEW APPROACHES TO IRIS RECOGNITION: ONE-DIMENSIONAL ALGORITHMS

YINGZI DU
*Indiana University-Purdue University Indianapolis, Indianapolis, Indiana*
ROBERT W. IVES
*United States Naval Academy, Annapolis, Maryland*
DELORES M. ETTER
*Southern Methodist University, Dallas, Texas*

## 1 INTRODUCTION

The key step in many current iris pattern recognition algorithms is to transform the iris pattern into a two-dimensional code [1–3]. To eliminate the effect of eye tilt, circular rotation or area-based image registration of the iris pattern is usually necessary in iris matching and identification algorithms [1–3]. Generally, iris recognition systems require

a cooperative subject [3] who willingly stares into a camera for a few seconds. The performance range (from subject to camera) of commercially available iris recognition systems is usually less than 2 ft [4]. Recently, Matey [5] from the Sarnoff Corporation has developed a remote iris recognition system, which can perform iris recognition up to 10 ft. As with other iris cameras, the user must look at the camera while moving toward it. The current functional speed is 1 m/s. Under these conditions, the iris image is obtained with the maximum amount of iris information. On the other hand, for a noncooperative subject, who may be facing away from the camera, only a portion of the iris information may be captured (a partial iris). Partial iris recognition algorithms would be very important in surveillance applications where capturing the entire iris may not be feasible. Little research has been performed in this area. The one-dimensional approach is different. The grayscale invariant local texture pattern (LTP) is developed to extract the local iris features. The one-dimensional (1D) signature is then generated for each iris image. The Du measure is used to evaluate the similarity between a test iris signature and those signatures in the database. The system will output the top $n$ closest matches. This method enables partial iris recognition and is more tolerant of the noise (such as eyelids, eye lashes, and glare), since the system only needs local information for processing instead of global information. In addition, no circular rotation is needed.

## 2 SCIENTIFIC OVERVIEW

Figure 1 shows a general iris recognition system, which is composed of four main modules:

1. Image acquisition. This module captures one or multiple iris image(s) from the subject using an iris camera [1–5]. Typically this is a near-infrared (NIR) camera.
2. Preprocessing. In this step, the image is first enhanced if needed, and then eyelashes, eyelids, pupil, and sclera are detected. With this information, the iris patterns are then extracted from the iris image. Usually, normalization is performed in this step to reduce the effect of pupil contraction or dilation [6–16].
3. Template generation. In this step, feature extraction of the iris is performed. A mathematical model is used to generate the template from the extracted iris patterns. In the literature, there are various approaches to generate the templates [1–16].
4. Pattern recognition. The newly generated iris template is compared with the iris templates in the database using some similarity measure. If a match is found, the iris will be identified.

In 1987, ophthalmologists Flom and Safir first patented an iris recognition system using a manual approach [17], in which the light intensity is manually adjusted to get

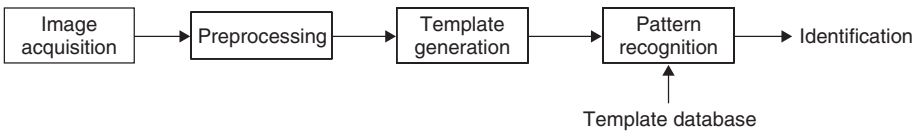



**FIGURE 1** Block diagram of typical iris recognition system.

the same pupil size iris images for iris pattern comparison. In 1994, Daugman invented the first automatic iris recognition system. Since then, various algorithms have been proposed for iris recognition using a waveform that is bounded in both frequency and duration to extract information. Daugman used the phase measure of 2D Gabor wavelets as the iris code. The phase is quantized to four values (2 bits) and the iris code is 256 bytes long. This method has been adopted by Iridian Technologies [1] and is currently used in commercial iris recognition systems. Masek and Kovesi used the Log-Gabor wavelet for iris recognition and made their MATLAB code available [6]. Boles and Boashash [7] used 1D zero-crossing wavelets for encoding iris patterns. Sanchez-Avila et al. [8] used a similar approach. Lim et al. [9] also used the wavelet transform to extract features from the iris region. Both the Gabor wavelet and the Haar wavelet are used as the mother wavelet. Muron et al. [10] have analyzed iris patterns in the frequency domain using the Fourier transform. Wildes et al. decomposed the iris region by constructing a Laplacian pyramid from an iris image [11]. Ma et al. [12] have designed a series of Gabor-wavelet-like spatial domain filters to analyze and extract iris pattern information. This was later followed by their iris recognition algorithms based on local intensity variation [13]. Recently, the authors designed a local texture analysis algorithm to calculate the LTP of iris images to generate a 1D iris template [14]. This approach relaxed the requirement of a significant portion of the iris for identification and recognition [15]. Some researchers have used independent component analysis (ICA) or principle component analysis (PCA) [16].

The methods used to perform template matching can be grouped into two categories: binary matching and nonbinary matching. Daugman [1] encodes the iris patterns into binary numbers. Then the Hamming distance [1] is calculated between the input iris template and iris templates in the database. Many other methods also encode the iris patterns into binary numbers. Hamming distance and Euclidean distance methods are the popularly used binary matching methods. Wildes et al. [11] used the Laplacian pyramids to represent the iris patterns, and the normalized correlation method is used for template matching [11]. In 1D method, Du measure is developed to calculate the similarities between two iris templates.

In terms of the number of dimensions of iris template, these algorithms can be grouped into multidimensional methods [11], two-dimensional (2D) methods [1, 12], and 1D methods [7, 14]. For the 1D cases, both methods [7, 14] transform the iris images to polar coordinates; however, their ways [7] of generating the 1D iris templates are very different. Ma et al. [12] generated the 1D iris signals from successive horizontal scan lines in the polar axis image and concatenated them to constitute an ordered 1D binary vector. The circular rotation would be needed at template matching stage. Du et al. [14] have a different approach. They used normalized image to compute the LTP values, which results in a 2D array of values with the same dimensions as the polar image. Each row of this LTP array becomes an element in the 1D template vector. In this way, the 1D template generated is rotation invariant [14].

## 3 ONE-DIMENSIONAL IRIS RECOGNITION SYSTEM ARCHITECTURE

The 1D system is composed of the following modules: iris acquisition, preprocessing, mask generation, LTP, iris signature generation, enrollment, iris identification, and iris signature database. The system architecture is depicted in Figure 2, and is described in the following sections.

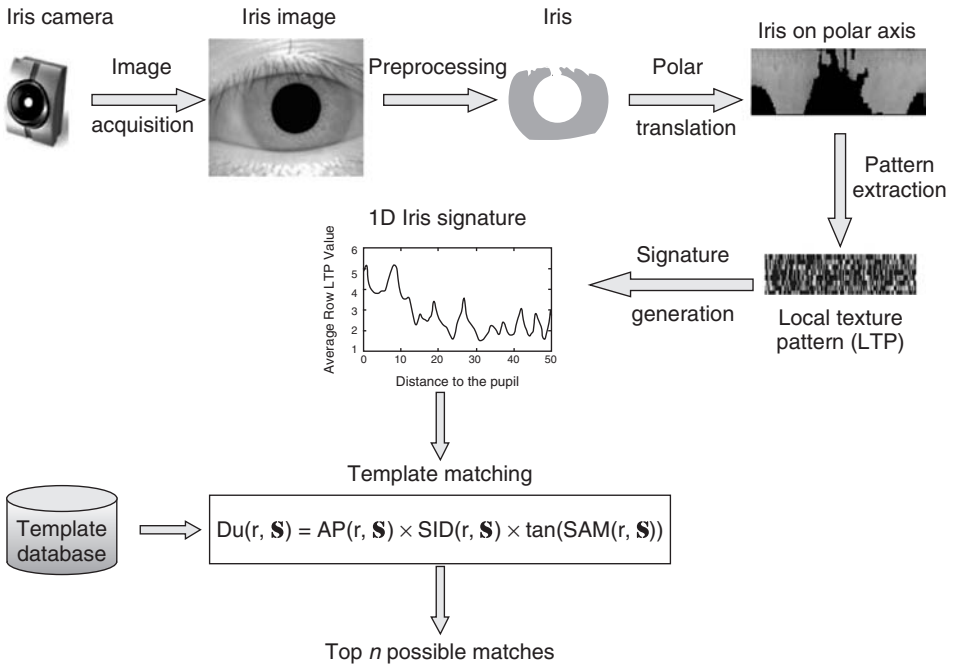



**FIGURE 2** The 1D iris identification system architecture.

### 3.1 Image Acquisition and Preprocessing

***3.1.1 Image Acquisition.*** The iris acquisition module uses an NIR camera to acquire an image of the eye. An NIR camera is used in most iris recognition systems to better capture the underlying features of the iris. The NIR range is especially useful for individuals with dark irises, or with contacts or glasses.

***3.1.2 Image Preprocessing.*** The preprocessing module locates the various components of the iris boundary. In particular, it is to find the inner and outer boundaries of the iris, the eyelids, and eyelashes.

Edge detection method is used to detect the rough inner and outer boundaries of the iris. Sometimes, the edges are not perfect, which may have broken points, spurious edges, and various thicknesses. The curve fitting or model based fitting is used to detect the fine boundaries. Usually, for cooperative users with frontal iris patterns, the pupillary and limbic boundaries are assumed to be circular. In such a case, circular Hough transform could be used. Some researchers have found that even for frontal irises, it could be noncircular. In such cases, ellipse fitting or general curve fitting method is used to solve the problem.

The edges above and below the circle are the edges of eyelids and eyelashes, which are usually identified after the detection of inner and outer boundaries of iris.

As a result of changes in the camera-to-face distance, the size of the same iris taken at different times may vary in the image [1, 14]. Because of stimulation by light or other reasons (such as hippus, the natural continuous movement of the pupil) the pupil may be constricted or dilated [14]. These factors will change the iris resolution, and the actual

distance between the pupillary and the limbic boundary. Normalization is necessary to reduce the effect of these problems. Usually, the distance between the pupillary and limbic boundary should be normalized in all iris images.

The iris area is then transformed using resolution invariant polar coordinates (which are different from the standard polar coordinates used below) to address the potential iris size difference [14]. For each pixel in the original iris image located at rectangular coordinates $(x_i, y_i)$, its polar coordinates $(r_i, \theta_i)$ are calculated as follows:

$$r_i = \frac{\tilde{L}}{L}\left(\sqrt{(x_i - x_0)^2 + (y_i - y_0)^2} - r_0\right) \tag{1}$$

$$\theta_i = \begin{cases} \arcsin\left(\dfrac{y_i - y_0}{x_i - x_0}\right), & y_i \geq y_0 \\ \pi + \arcsin\left(\dfrac{y_i - y_0}{x_i - x_0}\right), & y_i < y_0 \end{cases} \tag{2}$$

Here, $(x_0, y_0)$ is the center of the pupil, $r_0$ is the radius of the pupil, $L$ is the actual distance between the pupillary and limbic boundary in the original image, and $\tilde{L}$ is the normalized distance between the inner and outer boundaries of the iris. Here, it is assumed that the inner and outer boundaries are circular and they share same center. If they share a different center, the calculation principle will be similar to this approach, but it will be a little more complex. Usually, the center difference between the inner and outer boundaries for a frontal iris is very small. For a nonfrontal iris, it could be very different. In that case, their shape would not be circular and the transfer function could be much more complicated.

The location of the boundaries of eyelids and eyelashes is transformed to the respective polar coordinates. In this way, a mask for the iris in polar coordinates is generated.

### 3.2 Computation of Local Texture Patterns (LTP)

Analyzing iris patterns is a key step in iris pattern recognition and verification. A major problem in analyzing iris pattern (iris texture) images is that they are often not uniform due to variations in orientation, scale, contrast, and/or illumination. To solve the problem of illumination (grayscale) variations, the grayscale invariant LTP is developed.

The LTP computation begins with the definition of two windows. Let $T$ be a set of pixels inside a window and let $B$ be the center subset of pixels in window $T$. The grayscale value of the window $T$ is subtracted from the grayscale values of the pixels in the window $B$ to form the LTP for the pixels of set $B$.

Window $T$ is selected slightly larger than window $B$ so that the local mean be can be a better approximation to the true mean value and is less affected by noise. The $T$ windows overlap to reduce any edge effects of windowing. In addition, by computing LTPs using an overlapping $T$ window, the effects of noise on the LTP function is reduced.

After applying the mask to the iris pattern in the invariant resolution polar coordinates, the LTP module generates the local iris patterns. Note that the left-most column of the iris image in polar coordinates wraps around to the right-most column, so there are no actual left or right edges that would introduce artifacts.

### 3.3 1D Iris Signature Generation Module

After local iris patterns are calculated by the LTP module, the iris signature generation module will generate a 1D signature for each iris image by averaging the LTP values of each row. The generated 1D iris signatures are rotation invariant.

This is very different from any other iris templates or signatures, which are rotation dependent. Circular rotation or special registration is needed for traditional approaches in the pattern matching/identification step. Usually, this registration will pose a limitation for the angle of the eye tilt. For example, Daugman's method [1] requires an eye tilt less than $45^{\circ}$ in both directions.

For an iris pattern to be recognizable in the system, it should be enrolled in the database. Enrollment usually takes multiple iris images of the same iris to register and generate the enrollment iris patterns. It could be single or multiple iris images. In general, the iris signature generated from multiple iris images would be more robust than that generated from single iris image. But, it could take longer time to enroll if multiple iris images were used.

### 3.4 Template Matching

The spectral angle mapper (SAM) [17] has been widely used as a spectral similarity measure for multi/hyperspectral signals. The SAM measures the angle between the spectral vectors $\mathbf{r} = (r_1, r_2, \ldots, r_L)^{\mathrm{T}}$ and $\mathbf{s} = (\mathrm{s}_1, \mathrm{s}_2, \ldots, \mathrm{s}_{\mathrm{L}})^{\mathrm{T}}$ and is given as

$$\mathrm{SAM}(\mathbf{r}, \mathbf{s}) = \cos^{-1}\left(\frac{\langle \mathbf{r}, \mathbf{s} \rangle}{||\mathbf{r}||_2 \times ||\mathbf{s}||_2}\right) \tag{3}$$

Here, $\langle \mathbf{r}, \mathbf{s} \rangle$ is the inner product of vectors $\mathbf{r}$ and $\mathbf{s}$,

$$\langle \mathbf{r}, \mathbf{s} \rangle = \sum\nolimits_{i=1}^{L} r_i s_i \tag{4}$$

$||\mathbf{r}||_2$ and $||\mathbf{s}||_2$ are two norms of vectors $\mathbf{r}$ and $\mathbf{s}$. The two norm is defined as

$$||\mathbf{x}||_2 = \sqrt{\langle \mathbf{x}, \mathbf{x} \rangle} \tag{5}$$

Let $\mathbf{p} = (p_1, p_2, \ldots, p_L)^{\mathrm{T}}$ and $\mathbf{q} = (q_1, q_2, \ldots, q_L)^{\mathrm{T}}$ be the two probability mass functions generated by vectors $\mathbf{r}$ and $\mathbf{s}$. The spectral information divergence (SID) [14, 16] between vectors $\mathbf{r}$ and $\mathbf{s}$ is defined as

$$\mathrm{SID}(\mathbf{r}, \mathbf{s}) = D(\mathbf{p}||\mathbf{q}) + D(\mathbf{q}||\mathbf{p}) \tag{6}$$

Here, $D(\mathbf{p}||\mathbf{q})$ is the relative entropy (also known as *Kullback–Leibler information measure*) [14, 16] of $\mathbf{q}$ with respect to $\mathbf{p}$, where

$$D(\mathbf{p}||\mathbf{q}) = \sum\nolimits_{j=1}^{L} p_j \log(p_j/q_j) \tag{7}$$

Also, $D(\mathbf{q}||\mathbf{p})$ is the relative entropy of $\mathbf{p}$ with respect to $\mathbf{q}$, where

$$D(\mathbf{q}||\mathbf{p}) = \sum\nolimits_{j=1}^{L} q_j \log(q_j/p_j) \tag{8}$$

Note that $D(\mathbf{p}||\mathbf{q})$ is usually different from $D(\mathbf{q}||\mathbf{p})$. From information theory, we know that $D(\mathbf{q}||\mathbf{p})$ and $D(\mathbf{p}||\mathbf{q})$ are always nonnegative.

Recently, Du et al. [14] developed the (SID,SAM)-mixed measure. It is defined as

$$\text{mixed measure} = \left[D(\mathbf{q}||\mathbf{p}) + D(\mathbf{p}||\mathbf{q})\right] \times \tan\left[\cos^{-1}\left(\frac{\langle \mathbf{r}, \mathbf{s}\rangle}{||\mathbf{r}|| \times ||\mathbf{s}||}\right)\right] \tag{9}$$

The spectral discriminability of such a mixed measure is greatly enhanced by multiplexing the spectral abilities of the two measures [18]. However, it does not consider the energy difference. A better measure of similarity is given by the *Du* measure, which is defined as

$$\text{Du}(\mathbf{r},\mathbf{s}) = \text{APD}(\mathbf{r}, \mathbf{s}) \times \text{mixed measure} \tag{10}$$

where APD is the average power difference. Here instead of using the two norm, we use the single norm. In this way, the effect of the noise in some dimensions relative to the overall noise will be reduced. The APD is found as follows:

$$\text{APD}(\mathbf{r}, \mathbf{s}) = \frac{1}{N}||\mathbf{r} - \mathbf{s}||_1 \tag{11}$$

where $||\mathbf{x}||_1$ is the single norm defined by: $||\mathbf{x}||_1 = \sum_i |x_i|$. In this equation, $N$ is the total number of nonzero pairs of $r_i$ and $s_i$. In this way, the Du measure is defined as

$$\text{Du(r,s)} = \frac{1}{N} \times ||\mathbf{r} - \mathbf{s}||_1 \times \left[D(\mathbf{q}||\mathbf{p}) + D(\mathbf{p}||\mathbf{q})\right] \times \tan\left[\cos^{-1}\left(\frac{\langle \mathbf{r}, \mathbf{s}\rangle}{||\mathbf{r}|| \times ||\mathbf{s}||}\right)\right] \tag{12}$$

The Du measure is shown to be an effective measure of the similarity between two iris signatures because it takes three important perspectives of signature similarities into consideration: energy, angle, and information.

When an iris image is presented for identification, its iris signature is generated by the iris signature generation module, and it is compared with the enrolled iris signatures in the database using Du measurement. Each iris signature is a vector. Let us assume that two signatures to be compared are vectors $\mathbf{r}$ and $\mathbf{s}$ with same dimensions. Du measurement score is the result of product of three scores: *SAM*, *SID*, and *APD*.

The smaller the Du measurement score is, the closer the two signatures would be. In this way, this module outputs the $n$ closest matches from the database, where $n$ is selected by the user.

## 4 PARTIAL IRIS ANALYSIS USING 1D IRIS RECOGNITION METHOD

Generally, iris recognition systems require a cooperative subject [1–3] who willingly stares into a camera for a few seconds. Recently, Matey et al. from the Sarnoff Corporation developed a remote iris recognition system, which can perform iris recognition up to 10 ft. Different from conventional iris cameras, their iris camera is mounted with a telescope-like lens and stronger IR illuminator. As with other iris cameras, the user must look at the camera while moving toward it. The current functional speed is 1 m/s. Under these conditions, the iris image is obtained with the maximum amount of iris information. On the other hand, for a noncooperative subject who may be facing away

from the camera, only a portion of the iris information may be captured (a partial iris). Partial iris recognition algorithms would be very important in surveillance applications where capturing the entire iris may not be feasible.

In a partial iris image, depending on the percentage of the iris image available, it could be very difficult or even impossible to detect the pupil, the limbic boundary, the eyelids and eyelashes. The partial iris segmentation itself could be a challenging research topic. The purpose is to analyze the use of partial iris patterns. Therefore, a full iris image is used to generate the partial iris image as follows:

- Tear duct-to-outside: The "tear duct-to-outside" model gradually exposes the iris beginning at the near tear duct side and ending at the outside part of the eye. For the subject's left eye, this corresponds to the "left-to-right" model and for the subject's right eye, it would be the "right-to-left" model.
- Outside-to-tear duct: The reverse direction of the "tear duct-to-outside" model.
- Radial outside-to-inside.
- Radial inside-to-outside.

It is important to distinguish between left and right eye, and tear duct-to-outside and outside-to-tear duct because the eyelids tend to cover most of the iris on the side closer to the tear duct.

In this system, we first preprocess the full iris image to identify the iris area and determine pupil center, pupil radius, and limbic radius. In addition, eyelids and eyelashes are detected. These parameters are combined with the information available in the partial iris image to extract the partial iris pattern and to normalize the iris. The pupil may be contracted or dilated due to stimulation by light or other reasons (such as hippus, the natural continuous movement of the pupil). Accordingly, the distance between the pupillary and the limbic boundary would vary. As a result, the resolution of the same iris would change when taken at different times. To solve this problem, the partial iris must be normalized. The parameters such as the center and the radius of the pupil and the radius of the limbic boundary are obtained a priori from the full iris image. After these parameters are determined, the location of occluded iris patterns are zeroed and would not be used neither when generating the template nor for matching.

The experimental results show that a more distinguishable and individually unique features are found in the inner rings of the iris. As expected, the experimental results also show that the eyelids and eyelashes detrimentally affect the iris recognition results. There are minor differences between races, but this difference does not largely impact the iris recognition accuracy.

It is also observed that with the exploring of more percentage of the iris patterns, the increase in speed of the accuracy rate has been reduced. Especially, when the exploring of 45% iris patterns (from tear duct-to-outside), we can achieve very decent accuracy compared to full iris patterns (in rank 5 or rank 10 cases).

For surveillance, it is more likely that the eye away from the tear duct would be captured. This is the more challenging scenario, but the results show that it is still possible. The results show that a partial iris image can be used for human recognition when providing a ranked output, such as rank 5 or rank 10 system. Finally, the experimental results show that a partial iris image could be used for human identification (rank 1) with limited accuracy.

## 5 RESEARCH DIRECTIONS

The 1D iris recognition method differs from current approaches to iris recognition in several ways. First, it generates a 1D iris signature that is translation, rotation, and illumination invariant. The iris patterns or signatures generated by traditional methods are rotation dependent [6–13]. Circular rotation or special registrations are necessary for pattern matching/identification, and usually there is a limit regarding the angle of the eye tilt [1]. However, this method will relax this limitation since the signatures are rotation invariant. Since the generated iris signature does not have all the feature information, the recognition accuracy is not very high. In the future, the improvement to have more feature information in the signature could help to improve the recognition accuracy. In general, the recognition accuracy could be largely affected by the quality of iris images. Incorporating the quality measures in the iris recognition system could help to improve the accuracy.

## REFERENCES

1. Daugman, J. (1993). High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. Pattern Anal. Mach. Intell.* **15**(11), 1148–1161.
2. Du, Y., Ives, R. W., and Etter, D. M. (2005). Iris recognition, *The Electrical Engineering Handbook*, 3rd Edition, CRC Press, Boca Raton, FL.
3. Wilds, R. (2005). Iris recognition. In *Biometric Systems*, J. Wayman, A. Jain, D. Maltoni, and D. Maio, Eds. Springer, London, pp. 63–95.
4. Woodward, J. D., Orlans, N. M., and Higgins, P. T. (2002). *Biometrics*, The McGraw-Hill Company, Berkeley, CA.
5. Matey, J. (2007). Iris on the Move "Biometric Consortium Conference," IEEE Proceedings,.
6. Masek, L., and Kovesi, P. (2003). *MATLAB Source Code for a Biometric Identification System Based on Iris Patterns*, The University of Western Australia.
7. Boles, W. W., and Boashash, B. (1998). A human identification technique using images of the iris and wavelet transform. *Signal Process. IEEE Trans.* **46**(4).
8. Sanchez-Avila, C., Sanchez-Reollo, R., and Martin-Roche, D. (2002). Iris-based biometric recognition using dynamic wavelet transform. *IEEE Aerosp. Electron. Syst. Mag.* **17**, 3–6.
9. Lim, Sl., Lee, K., Byeon, O., and Kim, T. (2001). Efficient iris recognition through improvement of feature vector and classifier. *ETRI J.* **23**(2), 61–70.
10. Muron, A., Kois, P., and Pospísil, J. (2001). Identification of persons by means of the Fourier spectra of the optical transmission binary models of the human irises. *Opt. Commun.* **192**(3-6), 161–167.
11. Wildes, R. P., Asmuth, J. C., Green, G. L., Hsu, S. C., Kolczynski, R. J., Matey, J. R., and McBride, S. E. (1996). A machine vision system for iris recognition. *Mach. Vis. Appl.* **9**, 1–8.
12. Ma, L., Tan, T., Wang, Y., and Zhang, D. (2003). Personal identification based on iris texture analysis. *IEEE Trans. Pattern Anal. Mach. Intell.* **25**(12), 1519–1533.
13. Ma, L., Tan, T., Wang, Y., and Zhang, D. (2004). Efficient iris recognition by characterizing key local variations. *IEEE Trans. Image Process* **13**(6), 739–750.
14. Du, Y., Ives, R. W., Etter, D. M., and Welch, T. B. (2006). Use of one-dimensional iris templates to rank iris pattern similarities. *Opt. Eng.* **45**(3), 037201-1–037201-10.
15. Du, Y., Bonney, B., Ives, R. W., Etter, D. M., and Schultz, R. (2005). Analysis of partial iris recognition using a 1D approach. *Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*. Vol. II, pp. 961–964.

16. Dorairaj, V., Schmid, N. A., and Fahmy, G. Performance evaluation of iris-based recognition system implementing PCA and ICA encoding techniques. *Proceedings of SPIE 5779*. pp. 51–58, Orlando, FL, 2005.
17. Flom, L., and Safir, A. (1987). *Iris Recognition System*, United States Patent No. 4,641,349 (issued February 3), U.S. Government Printing Office, Washington DC.
18. Du, Y., Chang, C.-I., Ren, H., D'Amico, F. M., and Jensen, J. (2004). A new hyperspectral discrimination measure for spectral similarity. *Opt. Eng.* **43**(8), 1777–1786.

## FURTHER READING

IEEE Trans. Pattern Anal. Mach. Intell.
IEEE Trans. Inf. Forensic Secur.

# SPECTRALLY ADAPTIVE NANOSCALE QUANTUM DOT SENSORS

Woo-Yong Jang, Biliana Paskaleva, Majeed M. Hayat, and Sanjay Krishna
*Department of Electrical and Computer Engineering and the Center for High Technology Materials at the University of New Mexico, Albuquerque, New Mexico*

## 1 INTRODUCTION

Advances in hyperspectral (HS) and multispectral (MS) sensing and imaging in the infrared (IR) spectrum have enabled numerous remote-sensing applications. These include military surveillance (i.e. target recognition, identification, and classification), medical imaging (i.e. medical diagnosis), and monitoring geographical terrain, only to name a few. Conventional HS/MS systems offer spectral information of a scene (target or an agent) in a spectral band by sensing a wide range of narrow segments of the IR spectrum in a spectral range of interest. This can be achieved by using a broadband IR detector in conjunction with dispersive optics (e.g. a bank of IR optical filters) that can be utilized to specify the spectral bands to be sensed. Alternatively, multiple sensors, each sensitive to a designated spectral range, can be employed to sense a wide spectral range. However, either one of these complex conventional methods is of relatively large physical size and high cost. Nanoscale and spectrally adaptable sensors are emerging as a highly desirable alternative to conventional MS/HS sensing strategies that feature simplicity through its single-detector nature (or array of identically fabricated detectors)

without requiring dispersive elements. To this end, a new class of IR photodetectors based on nanoscale epitaxial quantum dots (QDs) have recently been proposed and developed [1, 2]. A key feature of this technology is that it exploits intersubband transitions between quantum-confined energy levels in a self-assembled dots-in-a-well (DWELL) structure in an InAs/GaAs/$Al_XGa_{1-X}As$ semiconductor material system [3]. Potential advantages of this detector technology are low dark current, high operating temperature, and notably bias-controlled tunability [4]. The quantum-confined Stark effect applied to the system comprising dots in an asymmetric well results in a bias-dependent spectral response and also introduces a red shift (spectral shift) with significant spectral overlap [5] as the bias is varied in nominal range. Hence, a single photodetector can be operated as multiple detectors simply by applying different bias: the bias-dependent photocurrents of a single detector can be regarded as the outputs, resulting from spectrally overlapping bands. Recently, DWELL-based focal plane array (FPA) grown and processed at the Center for High Technology Materials (CHTM) at the University of New Mexico had successfully demonstrated multicolor sensing capability [6] in both midwave infrared (MWIR) and long-wave infrared (LWIR) regions. Figure 1 shows representative imagery showing the DWELL-based FPA's capability to sense MWIR and LWIR radiation.

In order to maximally exploit the features of bias-dependent and spectrally overlapping spectra from the DWELL photodetector, two sets of signal-processing algorithms were developed and tested to further bring about the following two extended enabling functionalities that are based on post-processing of data. The first is the capability for continuous spectral tuning [7–9], which enables a so-called *DWELL-based algorithmic spectrometer* and the second is the capability for application-specific, optimal hyperspectral feature selection, which, in turn, enables target recognition [10]. The rationale behind either one of these algorithms is to judiciously fuse multiple bias-dependent photocurrents from a single DWELL detector based on precise mathematical rules.

In this article, we report the principles, fabrication, and operation of the spectrally agile and bias-tunable DWELL photodetector. Device growth and processing are briefly reviewed, followed by results on device characterization. Device optimization for improving the DWELL's operating temperature is also described. In addition, two key post-processing strategies for maximal data exploitation are also reviewed and analyzed: the DWELL-based algorithmic spectrometer and hyperspectral feature selection for target recognition.


**FIGURE 1** Two-color image of a DWELL-based FPA in (a) MWIR (3–5 μm) and (b) LWIR (8–12 μm).

## 2 PRINCIPLE OF OPERATION FOR DWELL PHOTODETECTORS

A DWELL detector is a smart hybrid of conventional quantum well (QW) and QD infrared photodetectors. In a heterostructure, InAs QDs are embedded in InGaAs/GaAs multiple QWs as shown in Figure 2 [9]. Just as conventional QD detectors, a DWELL detector is inherently sensitive to normal-incidence radiation and photons. Lower dark current levels are expected since the ground state is lowered with respect to GaAs band edge. Longer intersubband relaxation times in a DWELL structure can achieve a relatively high detectivity [11, 12]. In addition, the reduced thermionic emission inherent in the DWELL technology leads to higher operating temperatures. Due to the quantum-confined Stark effect, a bias-dependent spectral response is evident depending upon the asymmetric electronic potential of a geometrically asymmetric DWELL structure. Two main attributes of this geometry are the shape of the dot and the different thicknesses of the QW above and below the dot, which together lead to variation of the local potential as a function of the applied bias. A DWELL detector could provide better control over the operating wavelength and nature of the allowable energy transitions (bound-to-bound, bound-to-quasi-bound, and bound-to-continuum (barrier)) as shown in Figure 3 [9]. All the DWELL devices considered in this article were fabricated and characterized at CHTM.

### 2.1 Brief Descriptions of Device Growth and Processing

The DWELL structures were grown by V-80 molecular-beam epitaxy (MBE) system, with an $As_2$ cracker source. An average of 2.4 monolayers of InAs dots were deposited on the sample with a rate of 0.053 ML/s. Then the dots were Si-doped at a level of $1–5 \times 10^{10}$ cm$^{-2}$. DWELL consists of 30 stacks of InAs/GaAs/AlGaAs heterostructures between two $n^+$ GaAs contact layers. DWELL detectors were then processed using standard contact-lithography, plasma-etching, and metallization techniques in a class 100

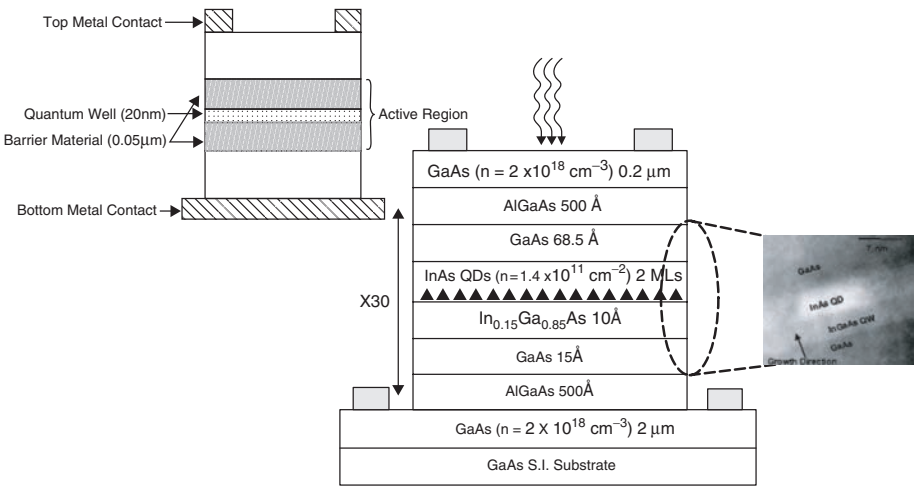



**FIGURE 2** General schematic of the DWELL heterostructure (top, left), example of the DWELL growth schematic (middle) and cross-sectional transmission electron microscopy (TEM) image (right) (adapted from Fig. 1 in Ref. 9).

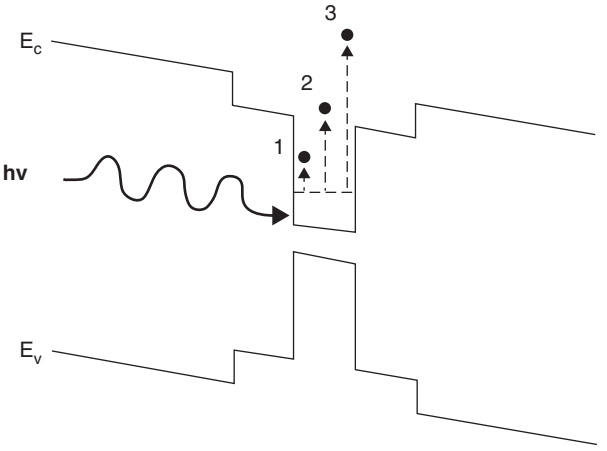



**FIGURE 3** DWELL energy band diagram describing: (1) bound-to-bound, (2) bound-to-quasi-bound, and (3) bound-to-continuum transitions (adapted from Fig. 2 in Ref. 9).

clean-room environment. Each 400 μm square n-i-n mesas with top pixel apertures, ranging from 25 to 300 μm in diameter, were lithographically defined in the top metal contact [4, 9].

### 2.2 Device Characterization

Spectral response measurements were performed on single pixel InGaAs-DWELL detectors with a Nicolet 870 FTIR (Fourier transform infrared) spectrometer and a Keithley 428 current amplifier, which controls the electrical bias to the detectors. Multiple measurements of experimental photocurrents and dark currents are taken at different biases using a HP parameter analyzer. The bias-dependent spectral measurements and the corresponding experimental photocurrents of the DWELL detector are shown in Figure 4 [9]. Due to a red shift (spectral shift), there exists two different peaks at LWIR region, one around 9.5 μm with negative bias and the other at 10.5 μm with positive bias. However, the drawback of the current DWELL is the limited operating temperature because of the dominance of the dark current at higher device temperatures [9]. In Figure 5 [9], the spectral response of DWELL starts degrading remarkably as the operating temperature of the device exceeds 60 K. Also the working range of applied bias becomes narrower. Especially at 77 K, it is to be noted that no spectral variation is observed for the applied bias range. More details of the characterization can be found in Ref. 9.

### 2.3 Higher Operating Temperature DWELL ("Double DWELL")

Higher temperature operation is most crucial to reduce device size and cost since the required cooling system is bulky and expensive. By achieving up to near-room temperature levels, this DWELL photodetector can be more effective due to its tunability as compared to the current state of art detectors. To further increase the operating temperature, the present InAs quantum dots/InGaAs/GaAs/GaAs/AlGaAs DWELL growth structure is further modified by the increase in the shoulder of the GaAs well and the addition of shoulders on both sides of the InGaAs well, so it becomes the complete

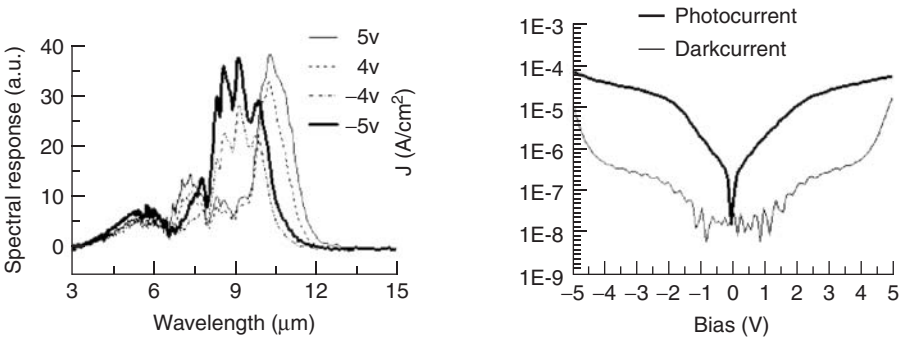



**FIGURE 4** Bias-dependent spectral responses of DWELL detector (left) and its photocurrent characteristic (right) (adapted from Fig. 6 in Ref. 9).

double DWELL (DDWELL) structure. The optimizations of the growth procedure and the processing technique can potentially lower the dark current level to obtain higher operating temperature of the device. In Figure 6 [11, 12], the bias-dependent DDWELL spectral response is observed until the device temperature of 120 K and the spectral shift are still present in LWIR. However, at 120 K, the device photocurrent is dominated by noise mainly due to the high dark current level.

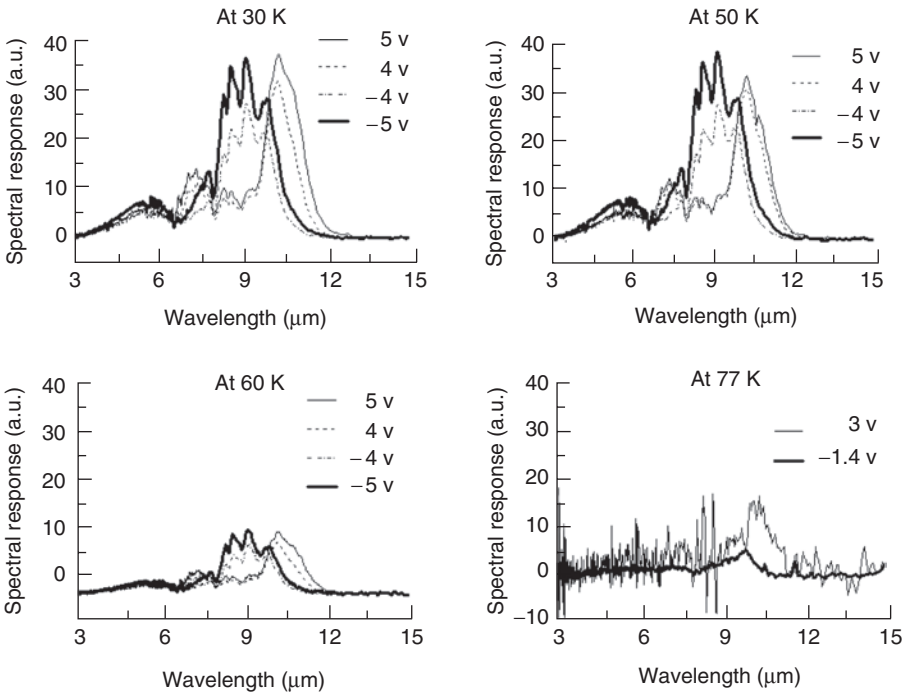



**FIGURE 5** Bias-dependent spectral responses of DWELL detector as a function of different operating temperatures at 30 K (top, left), 50 K (top, right), 60 K (bottom, left), and 77 K (bottom, right) (adapted from Fig. 7 in Ref. 9).

## 3 DESCRIPTION OF THE DWELL -BASED ALGORITHMIC SPECTROMETER

The concept of the spectral-tuning algorithm in conjunction with the DWELL-based detector is thoroughly reviewed here to describe the role of algorithmic spectrometer, drawing freely from our earlier published works [7, 8]. Assume that the object (target) of interest is illuminated by a black-body broadband radiation source and a DWELL detector probes the illuminated object applying different electrical biases, producing a group of bias-dependent photocurrents. The goal is to exploit these bias-dependent photocurrents to estimate (approximately reconstruct) the spectrum of the object of interest without the utilization of any physical dispersive optics or a spectrometer. The spectral estimation procedure is described as follows. First, a series of hypothetical, narrowband tuning filters, each with a prescribed center wavelength and transmittance, are defined by sweeping across the desired center wavelength of narrowband tuning filter in a spectral region of interest. Second, a set of superposition weights are calculated by estimating the spectrum of a DWELL detector with the choice of the tuning filters. Third, for each defined filter, the spectral reconstruction of object is performed by forming a weighted superposition of the DWELL spectral responses with predetermined superposition weights. With this step completed, the so-called "*synthesized photocurrent*", defined as the target reconstruction with weights, is shown to best approximate the ideal photocurrent obtained by sensing the same object of interest using an ideal broadband (with a spectrally flat response) detector

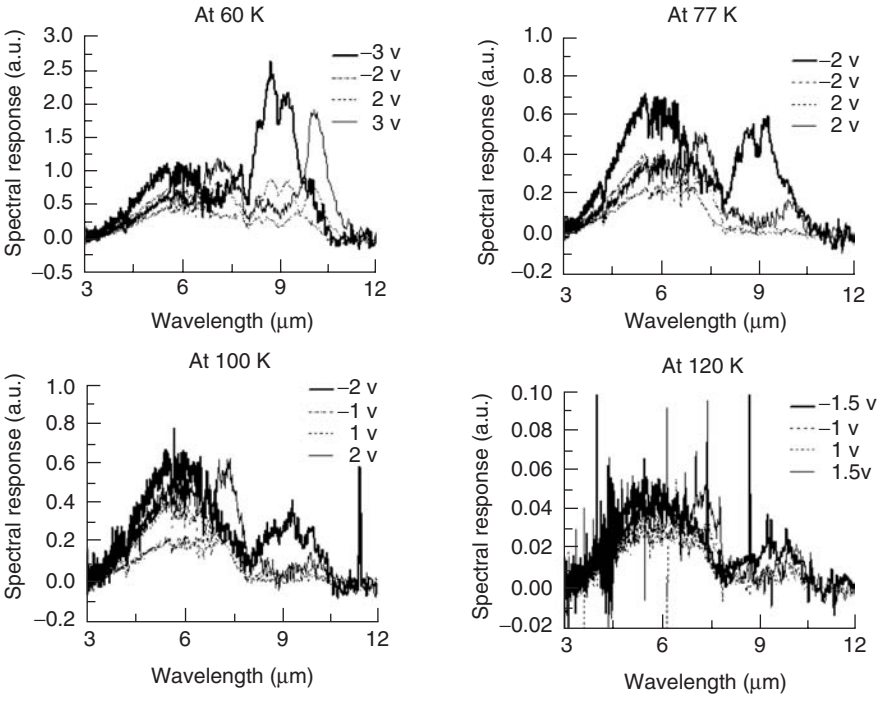



**FIGURE 6** Bias-dependent spectral responses of DDWELL detector as a function of different operating temperatures at 60 K (top, left), 77 K (top, right), 100 K (bottom, left), and 120 K (bottom, right) (adapted from Refs. 11, 12).

looking at the object through the spectral tuning filter. This approximation results in the minimization of the mean-square-error (MSE) between the synthesized photocurrent and the ideal response. Finally, the third step is repeated for every tuning wavelength and the spectrum is reconstructed within the prescribed wavelength range. In Figure 7 [9], the conventional spectrometer with an ideal broadband IR detector and a group of optical IR filters is schematically compared with the proposed algorithmic spectrometer for describing their functional equivalence.

### 3.1 Mathematical Description

Mathematically, the reconstructed target spectrum $\hat{I}_{\lambda_n}$ (Eq. (1) in Ref. 9) at a desired tuning wavelength $\lambda_n$ is formulated as

$$\hat{I}_{\lambda_n} = \sum_{i=1}^{k} w_{n,i} I_i \tag{1}$$

The weight vector, $\mathbf{w}_n = [w_{n,1}, \ldots, w_{n,K}]^{\mathrm{T}}$, is determined by computing the following expression (Eq. (18) in Ref. 8)

$$\mathbf{w}_n = [\mathbf{A}^{\mathrm{T}}\mathbf{A} + \Phi + \alpha\mathbf{Q}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}\mathbf{A}\mathbf{Q}]^{-1}\,[\mathbf{A}^{\mathrm{T}}\mathbf{r}_{\lambda_n}], \tag{2}$$

where $\mathbf{A}$ is a set of spectral responses of DWELL $= [\mathbf{R}_1, \ldots, \mathbf{R}_K]$ and each $\mathbf{R}_k = [R_k(\lambda_{\min}), \ldots, R_k(\lambda_{\max})]^{\mathrm{T}}$, ranging from a minimum value of $\lambda$ ($\lambda_{\min}$) to a maximum value of $\lambda$ ($\lambda_{\max}$). In addition, $\Phi$ is a diagonal noise-equivalent matrix whose $k$th diagonal entry is $\mathbf{R}_k{}^{\mathrm{T}}\mathbf{R}_k/\mathrm{SNR}_k{}^2$, where $\mathrm{SNR}_k$ represents the signal-to-noise ratio determined by the following formula (Eq. (3) in [9]),

$$\mathrm{SNR}_k = y_{p,k}/\sigma_{N,k}, \tag{3}$$

where $y_{p,k}$ is the experimentally averaged photocurrent (over 100 realizations) and $\sigma_{N,k}$ is the standard deviation of the dark current, also calculated empirically from the dark-current realizations. Then the remaining term named the *regularization term*, $\alpha\mathbf{Q}^{\mathrm{T}}\mathbf{A}^{\mathrm{T}}\mathbf{A}\mathbf{Q}$, limits spurious fluctuations in the approximation, where $\mathbf{Q}$ and $\alpha$ are the Laplacian operator and the regularization weight, respectively.

## 4 EXPERIMENTAL DEMONSTRATION OF ALGORITHMIC SPECTROMETER

Here we review an experimental application of the DWELL-based algorithmic spectrometer drawing from our earlier work reported in Ref. 9. Arbitrarily chosen targets in the LWIR region are considered and examined. First the spectral responses of the DWELL photodetector were measured at different biases varied between $-5$ and 5 V at a temperature of 30 K. Then the corresponding experimental photocurrent and dark current are obtained by illuminating the LWIR target with the FTIR source at each bias. As described in earlier section, measured spectral responses of the DWELL photodetector in conjunction with hypothetical, narrowband tuning filters determine the superposition weights in

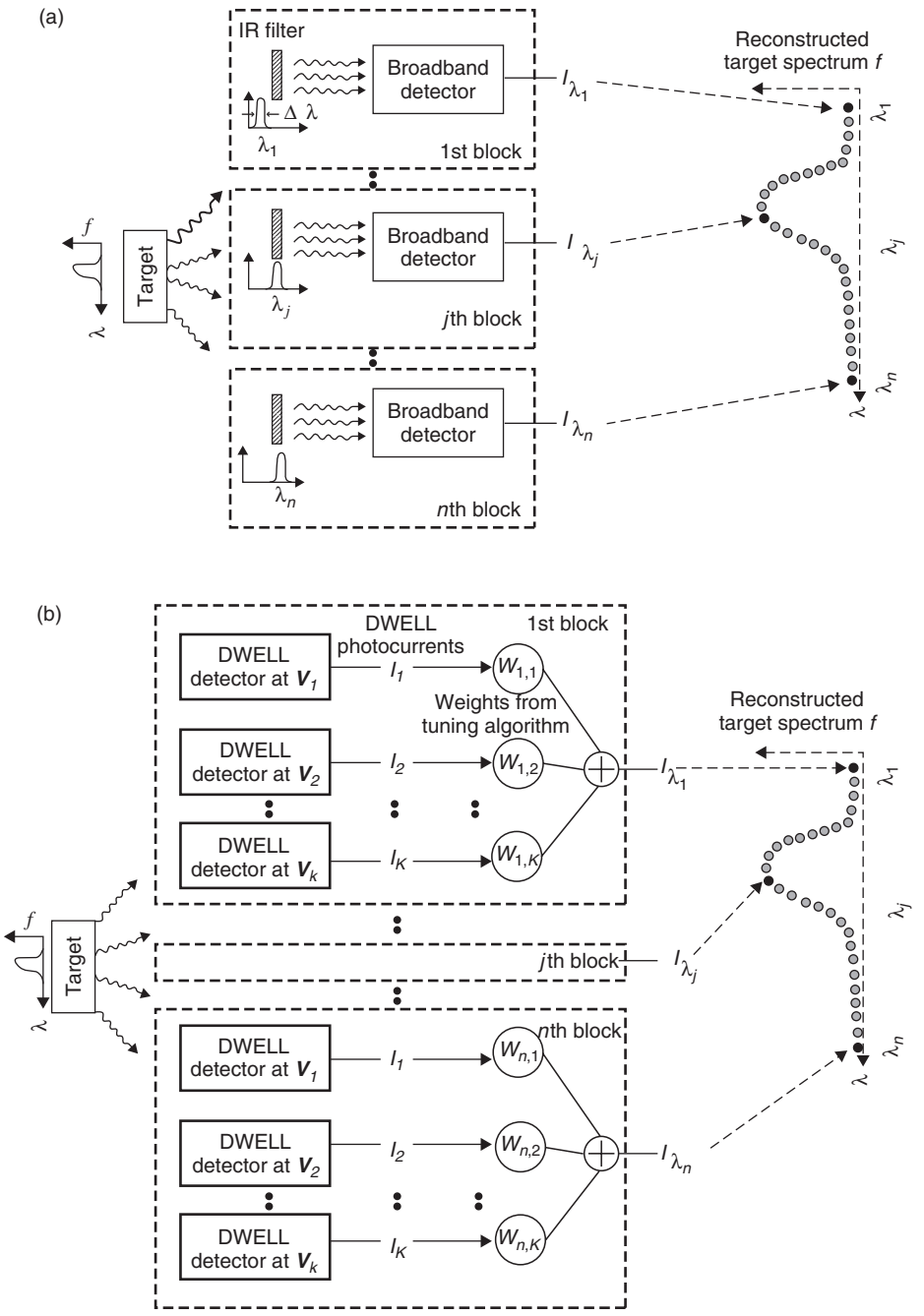



**FIGURE 7** (a) A conventional spectral sensing method using a standard broadband IR detector and a family of optical IR filters. (b) The proposed algorithmic-spectrometer equivalent of (a). Initially, several photocurrents (of the target spectrum $f$) are taken at different bias voltages $v_1 \ldots v_k$. Then, the measured responses at each bias are algebraically combined with predetermined weights $w_{i,n}$ that are used to match a desired filter centered at wavelength $n$. By changing the weights, the effect of different desired filters (similar to the ones used in (a)) is synthesized, albeit, without the use of any optical filters (adapted from Fig. 10 in Ref. 9).

a spectral region of interest. Then the experimentally obtained photocurrents are synthesized to give the weighted superposition representing each reconstructed point of the target at a desired tuning wavelength. The reconstruction results for four different target spectra, shown in Figure 8, are obtained by continuously tuning from 2.55 to 12.5 μm in steps of 0.05 μm. The solid curve is the true spectrum of target sensed by the standard broadband detector; whereas the dotted curve is the experimental reconstruction of algorithmic spectrometer incorporated with DWELL photodetector. The comparison of these two spectra clarifies the validation of algorithmic spectrometer. However, one limitation is evident that since the DWELL detector lacks its spectral information beyond 11.5 μm, the algorithmic spectrometer does not accurately reconstruct the long wavelength edge of target $f_2(\lambda)$ as shown in Figure 8(b).

## 5 REFINING THE ALGORITHMIC SPECTROMETER: REDUCTION OF REQUIRED BIASES AND HIGHER OPERATING TEMPERATURES

In an actual system, however, it may not be practical to use a large number of biases for operating the algorithmic spectrometer due to device limitations and the computational inefficiency as described later. Device limitations are related to the operation of the DWELL photodetector in which a reduction in the operating range of the bias is seen at high operating temperatures. With less biases required by the tuning algorithm, the

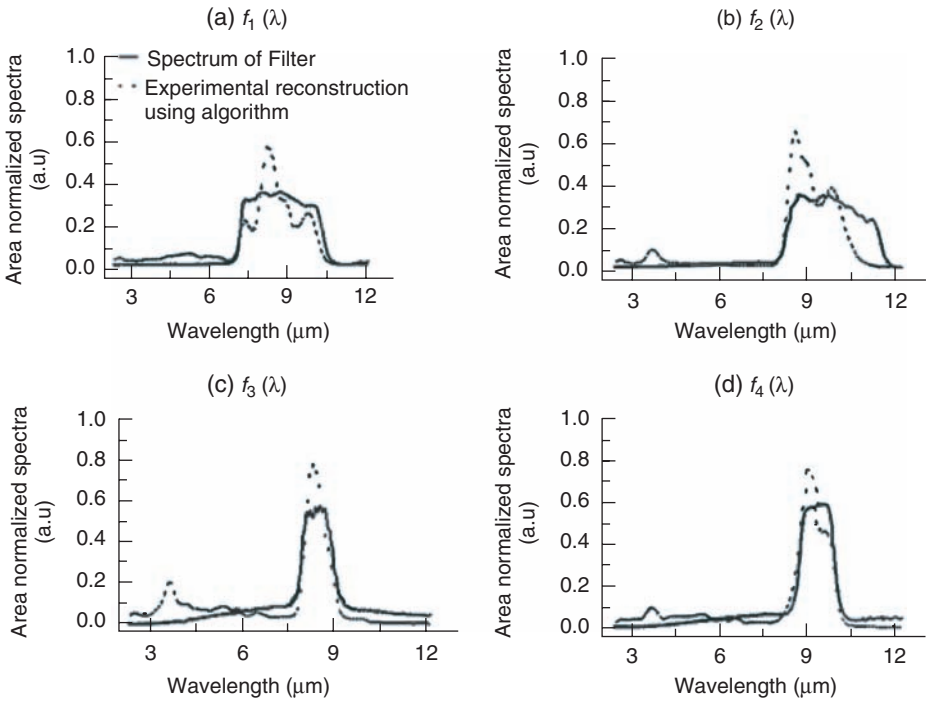



**FIGURE 8** Experimental reconstructions using algorithmic spectrometer incorporated with DWELL detector. Solid curves represent the actual responses of the targets and the dotted curves represent the reconstructed spectra using tuning algorithm (adapted from Fig. 13 in Ref. 9).

implementation of the algorithmic spectrometer simplifies, leading to increased speed, which may be suitable for near real-time applications. To this end, the algorithmic spectrometer is further refined by introducing the bias-selection scheme to reduce the number of required biases for acceptable target reconstruction. Bias-selection [13] is performed as follows: first, we find the threshold for the superposition weights, which can be predetermined from the analysis of the ordinary algorithmic spectrometer. Dominant weights are then selected while others are discarded based on the threshold.

Also, the DDWELL-based detector described earlier is used with this enhanced algorithmic spectrometer to test the performance against the detector operating temperature. Here we first measured the spectral responses of DDWELL detector for 30 biases available in the range between $-5$ and 5 V. The spectral measurement was repeated for different operating temperatures from 60 to 120 K. As illustrated in Figure 6, the operating bias range at 120 K is significantly reduced by the increase in device temperature, causing larger dark currents. Then one of LWIR targets described in Figure 8 was tested for a reconstruction using the algorithmic spectrometer with reduced number of biases; the minimum 10 biases originally from 30 biases were determined and required for achieving the reasonable target reconstruction. This algorithmic target reconstruction was repeated for incremental DDWELL operating temperatures (60, 77, 100, and 120 K). The results shown in Figure 9 are generally good at the device temperatures 60 and 77 K, yet at 100 K or above, the performance of algorithmic spectrometer is significantly degraded due to the lack of spectral information available from the DDWELL detector.

## 6 CANONICAL CORRELATION FEATURE SELECTION ALGORITHM AND ITS APPLICATION TO DWELL DETECTORS

Because of the capability to tune the quantum dot infrared photodetector (QDIP) responsivity continuously in its central wavelength and shape with the applied bias voltage, a single QDIP can be exploited as a multispectral or even hyperspectral IR sensor [8, 10]; the photocurrents measured at different operational biases can be viewed as outputs of different spectral bands. Unlike more traditional sensors, the spectral responsivities of QDIPs are broad $\sim$ μm and overlapping, thereby producing a high level of redundancy at the output photocurrents. Furthermore, the noise level at the photocurrents also varies continuously depending upon the bias applied, yielding band-dependent signal-to-noise ratio (SNR). These attributes of QDIP sensors necessitate the development of alternative methods for spectral feature-selection that will enable more efficient utilization of such sensors [10].

A novel, problem-specific spectral feature-selection algorithm termed the *Canonical Correlation Feature Selection* (CCFS) was rigorously developed for a general class of multispectral/hyperspectral sensors whose bands are both overlapping and noisy [10]. The approach is based on minimum mean-square-error (MMSE) criterion in conjunction with a canonical correlation (CC) analysis framework. The criterion ranks the best linear combinations of noisy and overlapping bands, termed *superposition bands*, guaranteeing minimal distances between each of the centers of the classes and their reconstructions in the space spanned by the sensor's bands [10]. In particular, for a given spectral pattern $p$, the algorithm selects an optimal superposition band, $f = \sum_{i=1}^{k} a_i f_i$, represented by the weight vector $\mathbf{a}^* = (a_1, \ldots, a_k)^T$, defined as solution of the constrained minimization

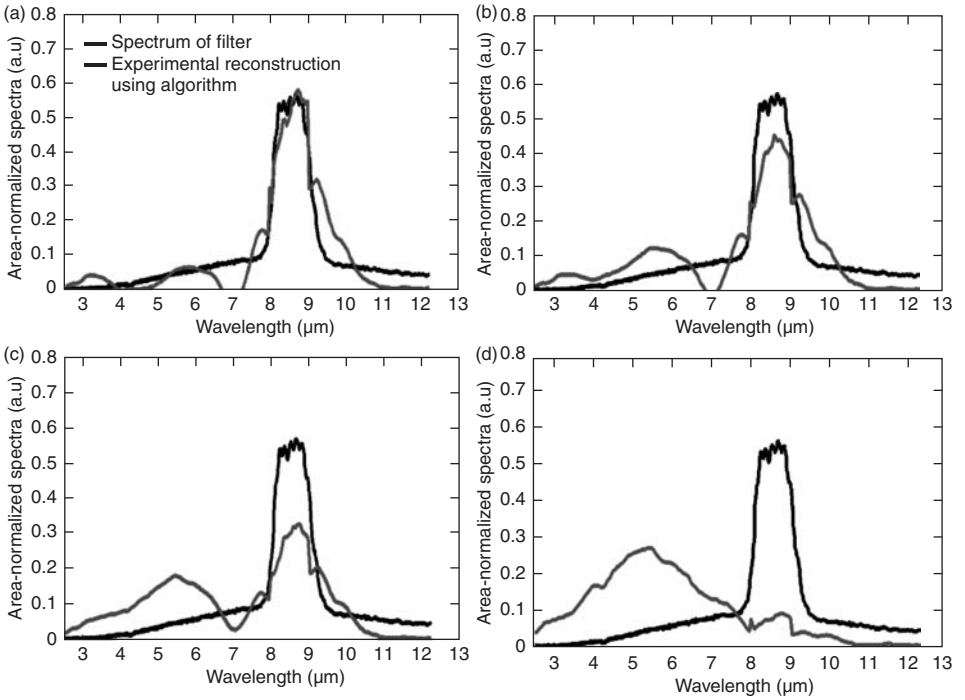



**FIGURE 9** Experimental reconstructions of a LWIR target using algorithmic spectrometer incorporated with DDWELL detector. Black curve represents the actual spectrum of the target and blue curves represent the reconstructed spectra with reduced biases (i.e. 10 biases) at different detector operating temperatures (a) 60 K, (b) 77 K, (c) 100 K and (d) 120 K (adapted from Ref. 12).

problem:

$$\mathbf{a}^* = \underset{\mathbf{a}\in R^K, \|f\|=1}{\arg\min} \; E\left[\left\| p - \sum_{i=1}^{k}\sum_{j=1}^{k} a_i a_j \left(\langle p, f_i\rangle + N_i\right) f_j \right\|^2\right] \tag{4}$$

where $N_i$ is the $i$th noise component associated with the sensor band $f_i$. The quantity

$$\tilde{I} = \sum_{i=1}^{k} a_i \left(\langle p, f_i\rangle + N_i\right) = \sum_{i=1}^{k} a_i I_i \tag{5}$$

is termed a *superposition photocurrent*, and it can be interpreted as the output photocurrent of the superposition band $f$. Moreover, the superposition photocurrent can be viewed as the optimal in an MMSE sense single spectral feature that can represent the spectral pattern $p$ in the space spanned by the sensor bands in the presence of noise.

The concept of optimal superposition band and photocurrent presented in Eq. (4) is then extended to a canonical feature-selection algorithm by utilizing the idea of the CC analysis [10]. Based on a computed sequence of principal angles $\theta_k$ between any two finite-dimensional Euclidean spaces, $U$ and V, the CC analysis yields the so-called *CC coefficients*, $\rho_k = \cos(\theta_k)$, between the two spaces. The first CC coefficient is computed

as $\rho_1 = \max_{i,j} \mathbf{u}_i^T \mathbf{v}_i$, where vectors $\mathbf{u}_i$, $i = 1, \ldots, m$, and $\mathbf{v}_i$, $i = 1, \ldots, n$, are unit length vectors that span the two spaces, respectively [10]. The two vectors for which the maximum is attained are then removed, and $\rho_2$ is computed from the reduced sets of the bases. This process is repeated until one of the remaining subspaces becomes empty.

When the inner product between two vectors is perturbed by additive noise as in the case of the photocurrent seen in Eq. (5), the CC analysis approach cannot be applied directly. A stochastic version of "principal angle" is introduced in Eq. (4) and used for ordering and selection of the optimal spectral features. The superposition band selection procedure described by Eq. (4) is repeated sequentially as many times as the number of the classes of interest, producing a canonical set of superposition bands. Following the general principle of CC analysis, at each stage, the algorithm excludes the class that has been selected in the prior stage from the search for the optimal direction and every superposition band is selected from a subspace of the sensor space that is in the orthogonal complement of the previously selected superposition directions.

Application of the CCFS algorithm to the problem of separability and classification analysis of seven rock classes [10] has demonstrated the efficacy of the proposed approach in a challenging remote-sensing task. A number of spectra of common rock samples in different grain size were selected from the Advanced Spaceborne Thermal Emission and Reflection Radiometer (ASTER) hyperspectral database to create training and two testing data sets. To extend the training and testing data sets, the endmebers in each rock-class were perturbed with different mixing materials, using a simple two-component linear mixing model [10]. QDIP spectral responses measured at different biases voltages varied in the range $-4.2$ to 2.6 V and at a temperature of 30 K were used to simulate the operation of a single-pixel, multispectral DWELL sensor.

In the presence of noise, for different SNR cases (10, 20, 30, and 60 dB) and using Bayesian classifier, the separability and classification results for the CCFS algorithm were compared with four different feature-selection strategies, each using seven spectral features. Here the number of selected superposition features is determined by number of classes of interest—seven. The first strategy was termed *deterministic CCFS* (DCCFS) and it employs the proposed CC feature-selection but without accounting for the photocurrent noise during the feature-selection process. In the second case, termed *noise-adjusted projection pursuit* (NAPP), seven features were extracted using the NAPP algorithm. The last two cases correspond to the classifiers that use seven QDIP and seven Multispectral Thermal Imager (MTI) bands.

From the results presented in Figure 10, right and left, we can conclude that embedding the noise statistics in the canonical feature-selection leads to a significant improvement in the classification. For the first three SNR cases (Fig. 10, right and left) the CCFS algorithm performs almost twice as good as the DCCFS algorithm. In the limiting case of a very high SNR, the performance of the CCFS and DCCFS algorithms becomes almost identical, as expected, and the classification error drops to 10–15%.

Comparison with the NAPP algorithm, as seen in Figure 10, shows that the CCFS algorithm outperforms the NAPP technique in the cases of low (10 dB) and high (60 dB) SNRs confirming further that CCFS offers enhanced robustness with respect to the photocurrent noise. These results indicate a great potential for operating QDIP sensors at higher temperatures, in the range 50–70 K, and thus leading to remote-sensing instruments with reduced size and cost.

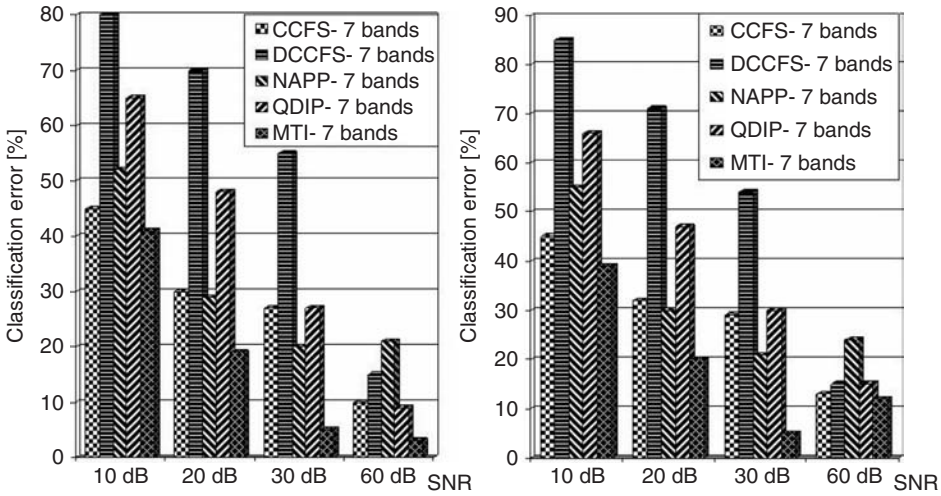



**FIGURE 10** Comparison in rock-type separation for CCFS, DCCFS, NAPP, QDIP bands and MTI bands in presence of noise with average SNR values of 10, 20, 30 and 60 dB. Left: Test Set-1. Right: Test Set-2 (adapted from Fig. 5 in Ref. 10).

## REFERENCES


1. Raghavan, S., Rotella, P., Stintz, A., Fuchs, B., Krishna, S., Morath, C., Cardimona, D. A., and Kennerly, S. W. (2002). High responsivity, normal-incidence long-wave infrared (l; 7.2mm) InAs/In0.15Ga0.85As dots-in-a-well detector. *Appl. Phys. Lett*. **81**, 1369–1371.
2. Phillips, J., Bhattacharya, P., Kennerly, S. W., Beekman, D. W., and Dutta, M. (1999). Self-assembled InAs–GaAs quantum-dot inter-subband detectors. *IEEE J. Quant. Elect*. **35**, 936–942.
3. Krishna, S. (2005). InAs/InGaAs Quantum Dots in a Well Photodetectors. *J. Phys. D (Appl. Phys.)* **38**, 2142–2150.
4. Krishna, S., Rotella, P., Raghavan, S., Stintz, A., Hayat, M. M., Tyo, S. J., and Kennerly, S. W. (2002). Bias-dependent tunable response of normal incidence long wave infrared quantum dot detectors. *Proc. IEEE/LEOS Ann. Meeting* **2**, 754–755.
5. Krishna, S., Hayat, M. M., Tyo, J. S., Raghavan, S. and Sakoğlu, Ü. (2007). Detector with tunable spectral response. US Patent No. 7,217,951.
6. Varley, E. S., Lenz, M., Lee, S. J., Brown, J. S., Ramirez, D. A., Stintz, A., Krishna, S., Reisinger, A. and Sundaram, M. (2007). Single bump, two-color quantum dot camera. *Appl. Phys. Lett*. **91**, 081120-1–081120-3.
7. Sakoğlu, Ü., Tyo, J. S., Hayat, M. M., Raghavan, S., and Krishna, S. (2004). Spectrally adaptive infrared photodetectors using bias-tunable quantum dots. *J. Opt. Soc. Am. B*. **21**, 7–17.
8. Sakoğlu, Ü., Hayat, M. M., Tyo, J. S., Dowd, P., Annamalai, S., Posani, K. T., and Krishna, S. (2006). A statistical method for adaptive sensing using detectors with spectrally overlapping bands. *Appl. Opt*. **45**, 7224–7234.
9. Jang, W.-Y., Hayat, M. M., Tyo, J. S., Attaluri, R. S., Vandervelde, T. E., Sharma, Y. D., Shenoi, R., Stintz, A., Cantwell, E. R., Bender, S., and Krishna, S. (2008). Demonstration of Bias Controlled Algorithmic Tuning of Quantum Dots in a Well Mid-infrared Detectors. *IEEE J. Quant. Elect*., submitted for publication.

10. Paskaleva, B., Hayat, M. M., Wang, Z., Tyo, S., and Krishna, S. (2008). Canonical Correlation Feature Selection for Sensors with Overlapping Bands:Theory and Application. *IEEE Trans. Geosci. & Remote Sens*., **46**, 3346–3358.
11. Vandervelde, T. E., Lenz, M. C., Varley, E., Barve, A., Shao, J., Shenoi, R., Ramirez, D. A., Jang, W.-Y., Sharma, Y. D. and Krishna, S. (2008). Quantum dots-in-a-well infrared photodetectors. *SPIE Defense and Security Symposium. March 16–20, Orlando, Florida*.
12. Matthews, M. R., Steed, R. J., Frogley, M. D., Phillips, C. C., Attaluri, R. S. and Krishna, S. (2007). Transient photoconductivity measurements of carrier lifetimes in an InAs/In0.15Ga0.85As dots-in-a-well detector. *Appl. Phys. Lett*. **90**, 103519-1–103519-3.
13. Jang, W.-Y., Hayat, M. M., Bender, S., Sharma, Y. D., Shao, J. and Krishna, S. (2008). Performance enhancement of an algorithmic spectrometer with quantum-dots-in-a-well infrared detectors. *International Symposium on Spectral Sensing Research, June 23–27, Hoboken, NJ*.

## FURTHER READING

Rogalski, A. (1999). Assessment of HgCdTe photodiodes and quantum well infrared photoconductors for long wavelength focal plane arrays. *Infrared Phys. Technol*. **40**, 279–294.

Levine, B. F. (1993). Quantum-well infrared photodetectors. *J. Appl. Phys*. **74**, 1–81.

Björck, and Golub, G.H. (1973). Numerical methods for computing angles between linear subspaces. *Math. Comput*., **27**(123), 579–594.

Knyazev, V., and Argentati, M.E. (2002). Principal angels between subspaces in a A-based scalar product: Algorithms and perturbation estimates. *SIAM J. Sci. Comput*., **23**(6), 2009–2041.

# FINDING INADVERTENT RELEASE OF INFORMATION

ROHINI K. SRIHARI

*University at Buffalo, Buffalo, New York*

## 1 INTRODUCTION

Inadvertent release of information is an important aspect of homeland security. Traditional cybersecurity techniques can be used to safeguard unauthorized access to such information, that is, preventing unauthorized users from being able to even see such information. Intrusion detection is an example of such a cybersecurity technique. This

article approaches the problem from a different perspective, namely the content of the information. That is, assuming that the information was accessed through proper means, could a reader be able to gain information that was not meant to be released? A typical example of such a scenario is cross-domain information sharing, where a document classified at a higher level may be inadvertently released to users not authorized to see it. To prevent such situations, techniques that examine the content of the document must be deployed as a backup measure to traditional cross-domain information dissemination security measures. More subtle but equally catastrophic cases of inadvertent information release can occur with publicly disseminated information such as web pages. It is often the case that a document collection, such as a set of web pages, reveals interesting information other than what is explicitly stated. The hidden information may be a consequence of multiple sources and authors working independently, which may pose issues with respect to information security. Although the content on an individual page may be innocuous, inferences across multiple pages could lead to inadvertent information release. This article surveys different scenarios of inadvertent information release along with techniques to prevent such occurrences. It is important to note that in many cases, automatic techniques can be used to suggest instances of sensitive information; the final decision must be taken by a human reviewing the output.

## 2 BACKGROUND

Various approaches have been taken to address this problem depending on the particular scenario of inadvertent information release being considered. In order to fully appreciate the challenges to solving this problem, it is useful to first look in more detail at scenarios for sensitive information as well as different data sources that must be examined. This is followed by a discussion of relevant technologies to this problem.

### 2.1 Sensitive Information

Sensitive information can be explicitly marked on a document basis, or implicitly inferred. There are several definitions put forth for sensitive information by various government agencies, ranging from "information that if released, could pose threats to national security" to a more benign "information to be used on a need-to-know basis". One common source of inadvertent release of information is classified documents, those that have some security classification attached to either the entire document or individual paragraphs. These classifications typically restrict dissemination based on secret, top-secret, no-foreign, and so on, restrictions. This is referred to as *cross-domain dissemination*.

More subtle cases of sensitive information are manifested when no explicit marking is present. For example, a chart that shows the amount of expenditure due to security-related measures at various airports is interesting. Because of this, one could deduce that one airport is more vulnerable than another, a fact that could be exploited for harmful purposes. Similarly, by combining information from multiple announcements about an individual's scheduled public appearances, it may be possible to synthesize a very detailed schedule of his or her itinerary thus creating a potential security risk. Finally, detailed policy guidelines that are publicly debated can sometimes be mined for unintended intelligence such as the conditions for providing seats to (armed) off-duty air marshals.

### 2.2 Data Sources

There are several sources of information that can contribute to inadvertent information release besides explicitly classified material. An important source that must be examined in terms of homeland security interests is publicly accessible web pages. Since an organization attempts to disseminate useful information about its activities, websites often contain valuable and dynamically changing content. The problem can become even more complex due to web pages containing links to pages outside the organization. In such cases, it becomes extremely difficult to detect potential vulnerabilities. E-mail, due to its convenience and preferred mode of communication, is a prime source of inadvertent information release. It is important to consider not only the text within an e-mail (or other document), but also to examine any attachments. Attachments often contain charts and diagrams, which provide quantitative data that could be subjected to data mining and used for criminal intent. Multimedia presentations may reveal identities of key people or other background clues that could be considered sensitive.

### 2.3 Relevant Technologies

Several technologies are applicable to detecting inadvertent release of information. These include machine learning techniques [1], especially text categorization [2]. A text categorization system is trained on numerous examples of hand-annotated documents corresponding to different categories or classes. In order for the system to perform accurately, it must be trained on sufficiently representative and diverse examples. Various text categorization techniques may be utilized, ranging from simpler Naïve Bayes techniques to more sophisticated support vector machines.

Natural language processing (NLP), especially information extraction technology [3], may be used for more in-depth processing of textual content. While text categorization techniques use coarser representations of information content such as word frequencies (known as *bag-of-words* model), NLP techniques are able to detect finer-grained linguistic characteristics. Information extraction techniques are able to detect named entities corresponding to names of people, organizations, locations, and so on. Thus, they are useful in deriving measures of intrinsic information content. Information extraction systems are also able to extract key relationships between entities, for example, that a person is affiliated with a certain organization.

Data mining techniques [4] are useful in applications such as trend analysis. For example, by mining the numeric data associated with expenditure on fortification of the nation's telecommunication systems on a periodic basis, it may be possible to detect aging systems. Data mining techniques take large quantities of typically numeric data as input, and output significant patterns or correlations that are automatically detected. They can also be used to compare different data sets based on temporal or spatial changes.

Finally, state-of-the-art text mining techniques [5] can be used to make inferences between concepts across documents. These techniques were initially proposed for bioinformatics applications, including Swanson's research that discovered connections between fish oil and Raynaud's disease [6, 7]. Text mining techniques have been used in a wide variety of applications ranging from multidocument summarization to detecting aviation accident precursors. They are often based on statistical methods, including latent semantic analysis [8]. More recent text mining approaches use sophisticated machine learning methods based on probabilistic graphical models [9].

## 3 THREATS, CHALLENGES, AND SOLUTIONS

In this section, specific cases of inadvertent information release are discussed along with current approaches for detecting such scenarios.

### 3.1 Inadvertent Cross-Domain Release of Individual Documents

Classified documents are often restricted to certain types of information networks such as SIPRNet and JWICS in order to control restrictions on dissemination to the appropriate domains However, inadvertent release can occur through many channels, a common one being the e-mailing of such a document to an unauthorized person. Several techniques may be brought to bear to address such type of situations. The most obvious is technology related to cybersecurity for the specific purpose of security policy implementation and support. Recognizing that such techniques may not be sufficient, particularly when a document has been incorrectly marked, other techniques must be used as back-up measures. Chief among these are text categorization techniques that can automatically classify documents or individual paragraphs with the appropriate classification level by examining the content.

Although text categorization techniques are robust and can achieve the required levels of accuracy when sufficient training data is available, they have some weaknesses. Such techniques may not be sufficient to capture the intuitive notion that documents containing highly specific information about an individual (such as his contact information) or an organization may be sensitive. NLP techniques, specifically, information extraction techniques are capable of capturing this type of information. Finally, text categorization techniques may not perform well on documents containing charts and diagrams.

### 3.2 Inadvertent Release of Sensitive Information through Hidden Text

There have been cases reported of information being leaked through hidden text or metadata embedded in electronic documents such as Microsoft Word [10]. Examples of hidden text include text from other documents that are automatically opened, e-mail headers, names of document authors, and so on. A case in point was the accidental release of the names of four civil servants who worked on a controversial document related to Iraq in the United Kingdom; these names were part of the hidden text. In order to counter this, various measures are in place ranging from required checks for hidden data to mandated use of document formats such as portable document format (PDF).

### 3.3 Mining of Publicly Accessible Information by Intelligent Agents

This scenario concerns the use of intelligent agents to automatically visit and subsequently mine information from publicly available information such as websites [11]. Reference 12 gives the example of companies providing package tracking numbers over the internet to enable customers to track the status of their purchases. However, such information could be used by another company to gain competitive advantage. It is possible to use a web agent that queries the tracking site for packages through an automatically generated list of valid package numbers. This in turn may lead to valuable information about how the company routes packages, as well as the best business areas geographically, not to

mention actual identities of large accounts. It is not difficult to see how such technologies could pose threats to homeland security if the sites being monitored corresponded to merchant vessel cargo. Thus, the combination of publicly available information and intelligent data mining agents could lead to inadvertent information release.

Several techniques can be used to mitigate the impact of such threats. Organizations should routinely review their system logs to see who has been accessing their site, with the goal of spotting anomalous activity. Misleading information could intentionally be introduced in an attempt to thwart such predators. The lifetime of information should also be limited based on reasonable estimates of genuine use.

### 3.4 Dissemination of Sensitive Information across Multiple Documents

Open source document collections reflect diverse sources and authors; they often reveal interesting information other than what is explicitly stated. The goal of information analysts is to sift through these extensive document collections and find interesting links that connect facts, assertions, or hypotheses that may be otherwise missed. This is the most difficult scenario to handle, since the sensitivity of information is based on inferences across multiple documents. Reference 13 refers to this case of inadvertent information release as *unintended* (or *unapparent* in benign situations) *information revelation* (UIR). Figure 1 illustrates the overall framework for solving this problem. It is assumed that an off-line process has (i) processed a document collection of interest (e.g. a website consisting of hundreds or thousands of pages), (ii) extracted concepts contained in the documents based on an appropriate domain ontology, and (iii) generated a graphical representation of the content where nodes correspond to concepts or topics and edges correspond to associations between concepts. The task of a UIR toolkit is to examine sets of pages (corresponding to sets of important concepts) and generate alerts if inferences can be made that connect these concepts such that the information revealed crosses a threshold.

Although this seems like a hopelessly complex task, significant advances have already been made. Information analysts can use search engines to produce an incidence matrix of pages mapped to keywords or topics. This is illustrated in Table 1. Presumably, analysts are knowledgeable about which keywords or topics are important, and furthermore, which combinations of topics are particularly sensitive. On the basis of the matrix, they can manually inspect pages, or sets of pages, corresponding to key topics. Any page that could lead to inadvertent release of information is either removed or edited. Such a process was actually carried out by the FAA shortly after 9/11. In spite of modern technology such as search engines, the process can still be painstakingly laborious. Since there are many ways in which a particular topic can be expressed, it is necessary to map keywords (reflecting instances of a topic) into the topic category to which it best belongs. Recent advances in topic modeling [14] are very useful in performing this task in a data-driven manner: topic labels are manually assigned based on inspection of the set of keywords.

The UIR solution presented in [13] represents an automated solution to this problem whereby information analysts do not need to manually check multiple pages for potential inferences that could reveal sensitive information. This system focuses on detecting how concepts are linked across multiple text documents by generating an *evidence trail* explaining the connection. A traditional search involving, for example, two or more person names will attempt to find documents mentioning both these individuals. This system focuses on a different interpretation of such a query: what is the best evidence trail across

**TABLE 1 Topic-Document Incidence Matrix**

| Topic | URL1 | URL2 | . . . | E-mail1 | E-mail2 | . . . |
|---|---|---|---|---|---|---|
| Safety control | | | | | | |
| Crosswind correction, anomaly detection, directional control | X[a] | | | X | X | |
| Certification | | | | | | |
| Airworthiness certification, medical certification, and aviation medical examiners | X | X | | | X | |
| FAA regulations | | | | | | |
| Hazardous materials regulations and financial responsibility | | X | | X | | |

[a]X means that the indicated topic has occurred in the corresponding document (or web page, or email . . . ).

documents that explains a connection between these individuals? For example, all may be good golfers. A generalization of this task involves query terms representing general concepts (e.g. indictment and foreign policy). This system uses a hybrid text mining approach combining the robustness of information retrieval systems, with the granularity of information extraction systems. The corpus is first processed by an NLP system; a graphical representation of salient concepts and links between concepts is generated. Links between concepts are generated based on their participation in subject–verb–object relationships. Graph matching is first performed using the query concepts: this results in a matching subgraph where concept chains reflect virtual edges between nodes. Finally,

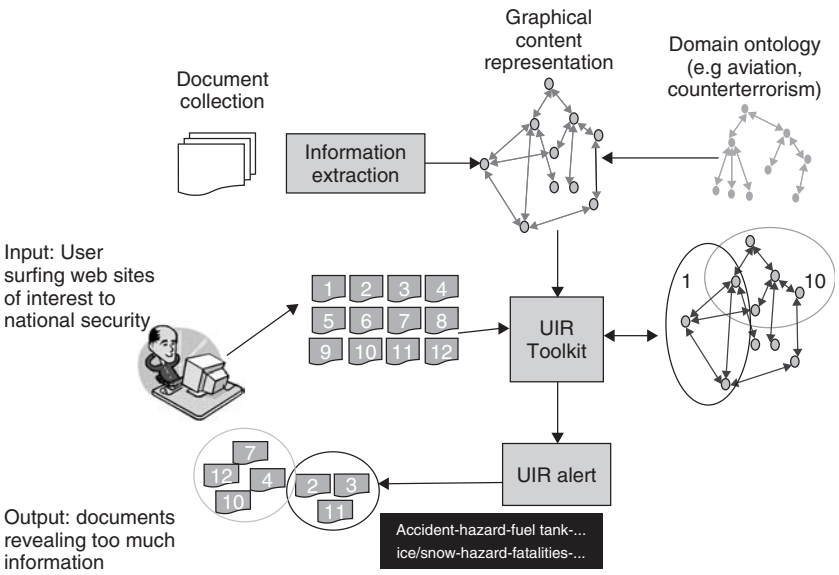



**FIGURE 1** General framework for system to detect inadvertent release of information.

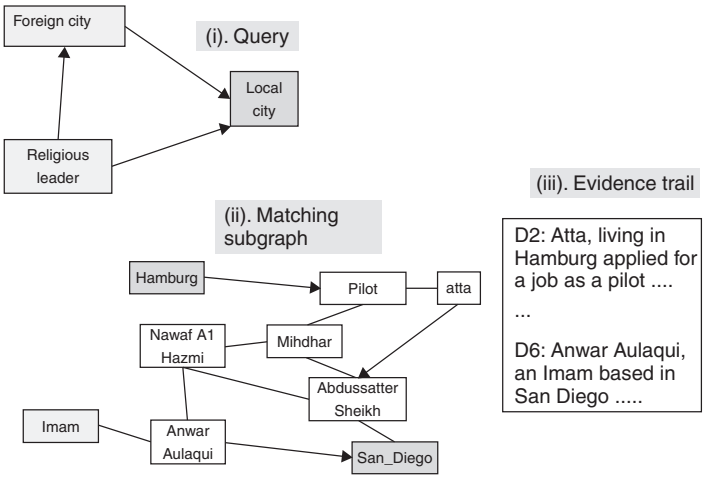



**FIGURE 2** UIR query and resulting evidence trail.

a graphical content model (based on topic and language models) is used to generate the evidence trail (i.e. set of sentences) corresponding to the matching subgraph. Since multiple subgraphs, and thus multiple evidence trails must be considered, a stand-alone evaluation system for evidence trails is used to rank the resulting evidence trails.

Figure 2 illustrates a query; it is based on a corpus of documents relating to 9/11. The analyst is looking for patterns involving a religious leader participating in some activity involving both US and foreign city. The query is simply a graph representing these three key concepts. Part (ii) of the figure shows the specific matching subgraph in the corpus based on the evidence trail shown in part (iii). The sentences are prefixed by the documents from which they are extracted. The subgraph in part (ii) is the corpus-specific match that is generated.

There are various criteria for ranking evidence trails, including (i) recency, (ii) most interesting, (iii) most plausible, and (iv) going through certain specified concepts. The primary focus is on finding chains that are *coherent* [15], that is, make sense, and *informative*. For example, if person A eats breakfast and person B also eats breakfast, then although eating breakfast is a valid connection, it is not of interest. On the other hand, if both of them have a liking for exotic spicy food from Southeast Asia, the connection starts to get more interesting. An alternate approach that could be used in the UIR problem that is specific to web pages (where URLs denote associations between concepts across pages) involving electricity analogs and information flows is discussed in [16].

There may be other instances of inadvertent release of information not covered here. However, the above categories cover the most significant classes of threats based on the sophistication of technology required to detect and defend against such scenarios.

## 4 FUTURE RESEARCH DIRECTIONS

Obviously, this is an open problem and requires significant research if risk of such threats to homeland security are to be mitigated. In general, there needs to be more work on automatic mapping of content to domain models to understand what information is reflected

in a collection of documents. It should be easy to visualize what type of information a set of documents contains, and its connection to other documents. This requires work on domain ontologies, as well as automatic mapping of content into these ontologies. The area of text mining is relatively new, and significant research is required, especially in drawing inferences across documents. Processing multimedia content, especially tables and figures is still in its infancy.

In order to make headway into this problem, a combination of content mining and usage mining techniques (see Further Reading on web mining) must be developed. Content mining has been discussed previously; usage mining reflects the sudden interest in a particular collection or sequence of information by parties of interest. Both these must be combined to both detect and prevent inadvertent release of information.

## 5 CONCLUSIONS

This article has examined various scenarios for inadvertent release of information. The problem is made difficult by the fact that there is no quantifiable metric for judging sensitive information, except for policy guidelines, along with the adage, "you know it when you see it". Document formats such as PDF have eliminated many of the previous risks due to hidden text or metadata; there is much more awareness for these types of risks now. Specific instances of inadvertent release, such as the accidental release of classified documents may have tractable solutions since the guidelines are governed by a classification system. Inadvertent release through data mining agents can also be limited by more careful monitoring of access to such information, along with modern technology such as "captchas", which are designed to prevent agent access. However, the most subtle forms of inadvertent information release that involve inferences across multiple pages may be very difficult to control. The problem is exacerbated through the links to pages outside the organization. Nevertheless, it is an important area to pursue since the results may not only impact national security but also have tremendous implications for areas such as bioinformatics and aviation security.

## REFERENCES

1. Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*, Springer, Science, Business Media LLC, New York.
2. Sebastiani, F. (2002). Machine learning in automated text categorization. *ACM Comput. Surv.* **34**, 1–47.
3. Srihari, R. K., Li, W., Niu, C., and Cornell, T. (2008). InfoXtract: a customizable intermediate level information extraction engine. *Proc. J. Nat. Lang. Eng.* **14**(1), 33–69.
4. Han, J., and Kamber, M. (2006). *Data Mining: Concepts and Techniques*, Morgan Kaufmann, San Fransisco, CA.
5. Weiss, S., Indurkhya, N., Zhang, T., and Damerau, F. (2004). *Text Mining: Predictive Methods for Analyzing Unstructured Information*, Springer, New York.
6. Swanson, D. R. (1988). Migraine and magnesium: eleven neglected connections. *Proc. Perspect. Biol. Med.* **31**(4), 552–557.
7. Srinivasan, P. (2004). Text mining: generating hypotheses from medline. *Proc. JASIST* **55**, 396–413.

8. Landauer, T. K., and Dumais, S. T. (1997). A solution to plato's problem: the latent semantic analysis theory of the acquisition, induction, and representation of knowledge. *Proc. Psychol. Rev.* **104**(2), 211–240.
9. Wang, X., Mohanty, N., and McCallum, A. (2005). Group and topic discovery from relations and text. *Proceedings of the 3rd International Workshop on Link Discovery*, Chicago, IL, pp. 28–35.
10. Forrester, J., and Irwin, B. (2005). An investigation into unintentional information leakage through electronic publication. *Proceedings of the ISSA 2005 New Knowledge Today Conference*, Gauteng, South Africa.
11. Wagner, C., and Turban, E. (2002). Are INTELLIGENT E-Commerce Agents PARTNERS or PREDATORS? *Proc. Commun. ACM Arch.* **45**(5), 84–90.
12. Sheng, Y. P., Mykytyn, P. P. Jr., and Litecky, C. R. (2005). Competitor analysis and its defenses in the e-marketplace. *Proc. Commun. ACM Arch.* **48**(8), 107–112.
13. Srihari, R. K., Xu, L., and Saxena, T. (2007). Use of ranked cross document evidence trails for hypothesis generation. *Proceedings of the 13th International Conference on Knowledge Discovery and Data Mining (KDD)*. San Jose, CA, pp. 677–686.
14. Barzilay, R., and Lee, L. (2004). Catching the Drift: Probabilistic Content Models, with Applications to Generation and Summarization, In *Proceedings of HLT-NAACL 2004*, Boston, MA, D. M. Susan Dumais, and S. Roukos, Eds. Association for Computational Linguistics, East Stroudsburg, PA, pp. 113–120.
15. Barzilay, R., and Lapata, M. (2005). Modeling local coherence: an entity-based approach. *Proceedings of the the 43rd Annual Meeting of the ACL*, Ann Arbor, MI, pp. 141–148.
16. Faloutsos, C., McCurley, K. S., and Tomkins, A. (2004). Fast discovery of connection subgraphs. *Proceedings of the 10th ACM SIGKDD International Conference KDD*, Seattle, WA, pp. 118–127.

## FURTHER READING

Baeza-Yates, R., and Ribeiro-Net, B. (1999). *Modern Information Retrieval*, Addison Wesley, New York.

Liu, B. (2007). *Web Data Mining—Exploring Hyperlinks, Contents and Usage Data*, Springer, Berlin, Heidelberg, NY.

Manning, C., Raghavan, P., and Schütze, H. (2008). *Introduction to Information Retrieval*, Cambridge University Press, New York.

Chakrabarti, S. (2003). *Mining the Web: Discovering Knowledge from Hypertext Data*, Morgan-Kaufmann Publishers, San Fransisco, CA.

Defense Technical Information Center. *Other Federal Agencies and the public may obtain copies from the U. S. Department of Commerce*. U. S. Department of Commerce, National Technical Information Service, Springfield, VA. Available at http://web7.whs.osd.mil.

# CONTENTS

# CONTRIBUTORS

**Dulcy M. Abraham**, Purdue University, West Lafayette, Indiana, *Consequence Mitigation*

**Anthony F. Adduci**, Argonne National Laboratory, Argonne, Illinois, *Geospatial Data Support for Infrastructure Interdependencies Analysis*

**Arlene M. Albert**, Anthropology Department, University of North Carolina Wilmington, Wilmington, North Carolina, *Craniofacial Aging*

**Julie A. Albrecht**, University of Nebraska-Lincoln, Lincoln, Nebraska, *Risk Assessment, Risk Management, and Preventive Best Practices for Retailers and Foodservice Establishments*

**Evangelyn C. Alocilja**, Biosystems and Agricultural Engineering, Michigan State University, East Lansing, Michigan, *Microbiological Biosensors for Food Defense and Safety Applications*

**S. Massoud Amin**, University of Minnesota, Minneapolis, Minnesota, *Robustness, Resilience, and Security of National Critical Infrastructure Systems; and Self-healing and Resilient Energy Systems*

**Paul R. Amyx**, Imagecat, Inc., Long Beach, California, *Technologies for Real-Time Data Acquisition, Integration, and Transmission*

**Andrew Anderson**, Sionex Corporation, Bedford, Massachusetts, *A Tandem Mobility Spectrometer for Chemical Agent and Toxic Industrial Chemical Monitoring*

**Robert W. Anthony**, Institute for Defense Analyses, Alexandria, Virginia, *Deterrence: An Empirical Psychological Model*

**George E. Apostolakis**, Engineering Systems Division and Department of Nuclear Science and Engineering, Massachusetts Institute of Technology Cambridge, Massachusetts, *Probabilistic Risk Assessment (PRA)*

**C. Warren Axelrod**, Bank of America, Charlotte, North Carolina, *Cyber Security for the Banking and Finance Sector*

**Bilal M. Ayyub**, Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland, *Defeating Surprise Through Threat Anticipation and Possibility Management; Memetics for Threat Reduction in Risk Management; Modeling Population Dynamics for Homeland Security Applications; Quantitative Representation of Risk; Terrorism Risk: Characteristics and Features; and Risk Analysis Frameworks for Counterterrorism*

**Andrew Bach**, NYSE Euronext, New York, New York, *Cyber Security for the Banking and Finance Sector*

**Rakesh Bahadur**, Science Applications International Corporation, McLean, Virginia, *Prevention of Contamination of Drinking Water in Buildings and Large Venues*

**Scott D. Bailey**, Argonne National Laboratory, Argonne, Illinois, *Geospatial Data Support for Infrastructure Interdependencies Analysis*

**George H. Baker**, James Madison University, Harrisonburg, Virginia, *Time-Domain Probabilistic Risk Assessment Method for Interdependent Infrastructure Failure and Recovery Modeling*

**J. M. Barbaree**, Department of Biological Sciences, Auburn University, Auburn, Alabama, *General Detector Capabilities for Food Safety Applications*

**Kevin Barry**, Depository Trust and Clearing Corporation, New York, New York, *Cyber Security for the Banking and Finance Sector*

**Jennifer L. Bayuk**, Consultant, Towaco, New Jersey, *Cyber Security for the Banking and Finance Sector*

**Steven M. Becker**, University of Alabama at Birmingham School of Public Health, Birmingham, Alabama, *Social, Psychological, and Communication Impacts of an Agroterrorism Attack*

**Dan Benigni**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Cyber Security Standards*

**Craig H. Benson**, University of Wisconsin, Madison, Wisconsin, *Decontamination and Disposal of Contaminated Foods*

**Kavita M. Berger**, American Association for the Advancement of Science, Washington, D.C., *Biodefense Workforce*

**Budhendra Bhaduri**, Oak Ridge National Laboratory, Oak Ridge, Tennessee, *Ultrascale Computing for Emergency Evacuation*

**Vicki Bier**, Center for Human Performance and Risk Analysis, University of Wisconsin-Madison, Madison, Wisconsin, *Risk Assessment and Safety of the Food Supply*

**Betty E. Biringer**, Security Risk Assessment Department, Sandia National Laboratories, Albuquerque, New Mexico, *Defending Against Malevolent Insiders Using Access Control*

**Regina Birner**, International Food Policy Research Institute, Washington, D.C., *The Use of Threat, Vulnerability, and Consequence (TVC) Analysis for Decision Making on the Deployment of Limited Security Resources*

**Bruce M. Biwer**, Argonne National Laboratory, Argonne, Illinois, *Decontamination Methods for Wastewater and Stormwater Collection and Treatment Systems*

**Paul E. Black**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Cyber Security Metrics and Measures*

**Cobus L. Block**, University of Wyoming, Laramie, Wyoming, *The Global Food Supply Chain*

**Edward J. Boone**, Statistics Department, Virginia Commonwealth University, Richmond, Virginia, *Craniofacial Aging*

**Ricardo P. Borja**, Malcolm Pirnie, Inc., White Plains, New York, *Prevention of Contamination of Drinking Water in Buildings and Large Venues*

**Jerry P. Brashear**, ASME Innovative Technologies Institute, LLC, Washington, D.C., *Risk Analysis and Management for Critical Asset Protection*

**Richard C. Brenner**, U.S. Environmental Protection Agency, Office of Research and Development, Cincinnati, Ohio, *Homeland Security and Wastewater Treatment*

**Robert Browitt**, Sandia National Laboratories, Albuquerque, New Mexico, *Carver + Shock: Food Defense Software Decision Support Tool*

**Theresa Brown**, Sandia National Laboratories, Albuquerque, New Mexico, *Infrastructure Dependency Indicators*

**Elgin Brunner**, Center for Security Studies (CSS), ETH Zurich, Switzerland, *Australia; Austria; Brazil; Canada; Estonia; Finland; France; Germany; Hungary; India; Italy; Japan; Republic of Korea; Malaysia; the Netherlands; New Zealand; Norway; Poland; Russia; Singapore; Spain; Sweden; Switzerland; United Kingdom; United States; European Union (EU); The Forum of Incident Response and Security Teams (FIRST); Group of Eight (G8); North Atlantic Treaty Organization (NATO); Organization for Economic Co-Operation and Development (OECD); United Nations (UN); and the World Bank Group*

**Cory Bryant**, Food and Drug Administration, Silver Spring, Maryland, *Carver + Shock: Food Defense Software Decision Support Tool*

**Donald L. Buckshaw**, Innovative Decisions, Inc., Vienna, Virginia, *Logic Trees: Fault, Success, Attack, Event, Probability, and Decision Trees*

**Dennis Buede**, Innovative Decisions, Inc., Vienna, Virginia, *Bayesian Networks*

**David E. Burchfield**, Hamilton Sundstrand Corporation, Pomona, California, *A Tandem Mobility Spectrometer for Chemical Agent and Toxic Industrial Chemical Monitoring*

**Peter Burgherr**, Paul Scherrer Institut (PSI), Laboratory for Energy Systems Analysis, Villigen PSI, Switzerland, *Comparative Risk Assessment for Energy Systems: A Tool for Comprehensive Assessment of Energy Security*

**Steve Cain**, Extension Disaster Education Network, Purdue University, West Lafayette, Indiana, *The EDEN Homeland Security Project: Educational Opportunities in Food and Agrosecurity*

**Kitty F. Cardwell**, United States Department of Agriculture, Washington, D.C., *Early Detection and Diagnosis of High-Consequence Plant Pests in the United States*

**John Carlson**, BITS, Washington, D.C., *Cyber Security for the Banking and Finance Sector*

**Todd P. Carpenter**, Adventium Labs, Minneapolis, Minnesota, *Protecting Security Sensors and Systems*

**Terry Carpenter**, National Center for Medical Intelligence, Frederick, Maryland, *Foreign Dengue Virus Presents a Low Risk to U.S. Homeland*

**Brian D. Carrier**, Basis Technology, Cambridge, Massachusetts, *File Forensics And Conversion*

**Frank Castelluccio**, Options Clearing Corporation, Chicago, Ilinois, *Cyber Security for the Banking and Finance Sector*

**Myriam Dunn Cavelty**, Center for Security Studies (CSS), ETH Zurich, Switzerland, *Critical Information Infrastructure Protection, Overview*

**Peter Chalk**, RAND, Santa Monica, California, *Vulnerability of the Domestic Food Supply Chain*

**Stephanie Chang**, University of British Columbia, Vancouver, BC, Canada, *Characterizing Infrastructure Failure Interdependencies to Inform Systemic Risk*

**Rama Chellappa**, Center for Automation Research and Department of Electrical and Computer Engineering, University of Maryland, College Park, Maryland, *Knowledge Extraction from Surveillance Sensors*

**S. Y. Chen**, Argonne National Laboratory, Argonne, Illinois, *Decontamination Methods for Wastewater and Stormwater Collection and Treatment Systems*

**B. A. Chin**, Materials Engineering, Auburn University, Auburn, Alabama, *General Detector Capabilities for Food Safety Applications*

**Anton Chuvakin**, LogLogic, San Jose, California, *Advanced Attacker Detection and Understanding with Emerging Honeynet Technologies*

**Robert M. Clark**, Cincinnati, Ohio, *Potential Contamination Agents of Interest*

**Kathryn L. Clark**, National Center for Medical Intelligence, Frederick, Maryland, *Foreign Dengue Virus Presents a Low Risk to U.S. Homeland*

**Shirley E. Clark**, Pennsylvania State University, Harrisburg, Middletown, Pennsylvania, *Water Infrastructure and Water Use in the United States*

**Glenn Coghlan, CPP**, Founder and CEO, Coghlan Associates, Inc., Springfield, Virginia, *Vulnerability Assessment*

**Marc J. Cohen**, International Food Policy Research Institute, Washington, D.C., *The Use of Threat, Vulnerability, and Consequence (TVC) Analysis for Decision Making on the Deployment of Limited Security Resources*

**Roger M. Cooke**, Department of Mathematics, Delft University of Technology, Delft, the Netherlands, *Experience with Expert Judgment: The TU Delft Expert Judgment Data*

**Kara L. F. Cooper**, Centers for Disease Control and Prevention, Atlanta, Georgia, *Pulsenet: A Program to Detect and Track Food Contamination Events*

**Kenneth L. Cox**, USAF, MC, SFS, TRICARE Management Activity (TMA), Office of the Assistant Secretary of Defense (Health Affairs), Falls Church, Virginia, *ESSENCE: A Practical Systems for Biosurveillance*

**Joe Crossett**, High Street Consulting Group, Pittsburgh, Pennsylvania, *Roles and Implications of Transportation Systems in Homeland Security*

**Kenneth G. Crowther**, Center for Risk Management of Engineering Systems, Department of Systems and Information Engineering, University of Virginia, Charlottesville, Virginia, *Scenario Analysis, Cognitive Maps, and Concept Maps*

**Michel Cukier**, University of Maryland, College Park, Maryland, *Risk Analysis Methods for Cyber Security*

**John Cummings**, Sandia National Laboratories, Albuquerque, New Mexico, *Protection and Prevention: An Overview*

**Christopher T. Cyr**, Critigen, Portland, Oregon, *Emergency Response Planning for Drinking Water Systems*

**Nicklas Dahlström**, Lund University School of Aviation, Ljungbyhed, Sweden, *Security and Safety Synergy*

**Jeffrey Danneels**, Sandia National Laboratories, Albuquerque, New Mexico, *Carver + Shock: Food Defense Software Decision Support Tool*

**John Davies-Cole**, Center for Policy, Planning and Epidemiology, DC Department of Health, Washington, D.C., *Biosurveillance Tradecraft*

**Sandra Davis**, ECO Resource Group, Bainbridge Island, Washington, *Emergency Response Planning for Drinking Water Systems*

**Robert M. DeBell**, Gaithersburg, Maryland, *Qualitative Representation of Risk*

**Sidney Dekker**, Lund University School of Aviation, Ljungbyhed, Sweden, *Security and Safety Synergy*

**Sharon M. DeLand**, Sandia National Laboratories, Albuquerque, New Mexico, *Critical Infrastructure Protection Decision Making*

**Po-Ching DeLaurentis**, Purdue University, West Lafayette, Indiana, *Consequence Mitigation*

**Kevin A. Delin**, SensorWare Systems, Inc., Pasadena, California, *The Sensor Web: Advanced Technology for Situational Awareness*

**Rance J. DeLong**, Santa Clara University, Santa Clara, California and LynuxWorks, San Jose, California, *High Assurance: Provably Secure Systems and Architectures*

**Dan DeWaal**, Options Clearing Corporation, Chicago, Ilinois, *Cyber Security for the Banking and Finance Sector*

**Lana Deyneka**, General Communicable Disease Control Branch, North Carolina Division of Public Health, Department of Health and Human Services, Raleigh, North Carolina, *The North Carolina Biosurveillance System*

**Sagar Dhakal**, Nortel Networks Inc., Richardson, Texas, *Dynamic Load Balancing for Robust Distributed Computing in the Presence of Topological Impairments*

**James S. Dickson**, Department of Animal Science, Iowa State University, Ames, Iowa, *Mitigating Consequences of Pathogen Inoculation into Processed Food*

**David Dietz**, Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, New Mexico, *Dynamic Load Balancing for Robust Distributed Computing in the Presence of Topological Impairments*

**Robin L. Dillon-Merrill**, McDonough School of Business, Georgetown University, Washington, D.C., *Logic Trees: Fault, Success, Attack, Event, Probability, and Decision Trees*

**Joseph DiRenzo III**, United States Coast Guard, *Security Assessment Methodologies for U.S. Ports and Waterways*

**Christopher W. Doane**, United States Coast Guard, *Security Assessment Methodologies for U.S. Ports and Waterways*

**Ian Dobson**, University of Wisconsin-Madison, Madison, Wisconsin, *Analysis of Cascading Infrastructure Failures*

**Ronald C. Dodge Jr.**, United States Military Academy, West Point, New York, *Advanced Attacker Detection and Understanding with Emerging Honeynet Technologies*

**Paul D. Domich**, CIP Consulting, Inc., Boulder, Colorado, *System and Sector Interdependencies: An Overview of Research and Development*

**Don Donahue**, Depository Trust and Clearing Corporation, New York, New York, *Cyber Security for the Banking and Finance Sector*

**Daniel H. Doughty**, SION Power Corp, Tucson, Arizona, *Nano-Enabled Power Sources*

**M. Ellin Doyle**, University of Wisconsin, Madison, Wisconsin, *Decontamination and Disposal of Contaminated Foods*

**Larry Drymon**, Space and Naval Warfare Systems Center, San Diego, California, *Less Lethal Payloads for Robotic and Automated Response Systems*

**Yingzi Du**, Indiana University-Purdue University Indianapolis, Indianapolis, Indiana, *New Approaches to IRIS Recognition: One-Dimensional Algorithms*

**David Ekern**, Virginia Department of Transportation, Richmond, Virginia, *Roles and Implications of Transportation Systems in Homeland Security*

**David Engaldo**, Options Clearing Corporation, Chicago, Ilinois, *Cyber Security for the Banking and Finance Sector*

**Angela M. Ervin**, Department of Homeland Security Science and Technology Directorate, Washington, D.C., *Sensing Dispersal of Chemical and Biological Agents in Urban Environments*

**Delores M. Etter**, Southern Methodist University, Dallas, Texas, *New Approaches to IRIS Recognition: One-Dimensional Algorithms*

**Lee Eubanks**, Sandia National Laboratories, Albuquerque, New Mexico, *Carver+ Shock: Food Defense Software Decision Support Tool*

**Robert P. Evans**, Idaho National Laboratory, Idaho Falls, Idaho, *Inherently Secure Next-Generation Computing and Communication Networks for Reducing Cascading Impacts*

**Hobart Ray Everett**, Space and Naval Warfare Systems Center, San Diego, California, *Less Lethal Payloads for Robotic and Automated Response Systems*

**Bernie Eydt**, Booz Allen Hamilton, McLean, Virginia, *Wireless Security*

**M. Anthony Fainberg**, Institute for Defense Analyses, Alexandria, Virginia, *Application of a Conditional Risk Assessment Methodology for Prioritization of Critical Infrastructure*

**David Ferraiolo**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Authentication, Authorization, Access Control, and Privilege Management*

**Robert Finkelstein**, Robotic Technology Inc., University of Maryland University College, Adelphi, Maryland, *Memetics for Threat Reduction in Risk Management*

**Ronald E. Fisher**, Argonne National Laboratory, Argonne, Illinois, *Geospatial Data Support for Infrastructure Interdependencies Analysis; and System and Sector Interdependencies: An Overview*

**Jacqueline Fletcher**, Oklahoma State University, Stillwater, Oklahoma, *Microbial Forensics and Plant Pathogens: Attribution of Agricultural Crime*

**Kim R. Fox**, National Homeland Security Research Center, U.S. Environmental Protection Agency, Cincinnati, Ohio, *Treatability of Contaminants in Conventional Systems*

**Mark G. Frank**, University at Buffalo, State University of New York, Buffalo, New York, *Human Behavior and Deception Detection; and Training for Individual Differences in Lie Detection Ability*

**Michael J. Frankel**, EMP Commission, Washington, D.C., *Defending Against Directed Energy Weapons: RF Weapons and Lasers; High Consequence Threats: Nuclear; High Consequence Threats: Electromagnetic Pulse*

**Oscar Franzese**, Center for Transportation Analysis, Oak Ridge National Laboratory, National Transportation Research Center, Knoxville, Tennessee, *Population Evacuations*

**Adrian V. Gheorghe**, Old Dominion University (ODU), Norfolk, Virginia University Politechnica, Bucharest, Romania, *Critical Infrastructures at Risk: A European Perspective*

**Forrest Gist**, CH2M HILL, Portland, Oregon, *Drinking Water Supply, Treatment, and Distribution Practice in the United States*

**Hans Glavitsch**, Swiss Federal Institute of Technology, Zurich, Switzerland, *Large-Scale Electricity Transmission Grids: Lessons Learned from the European Electricity Blackouts*

**Marc Goodner**, Microsoft, Redmond, Washington, *Security of Web Application and Services and Service-Oriented Architectures*

**Louis L. H. J. Goossens**, Department of Safety Science, Delft University of Technology, Delft, the Netherlands, *Experience with Expert Judgment: The TU Delft Expert Judgment Data*

**J. Richard Gorham**, United States Public Health Service, Food and Drug Administration, Xenia, Ohio, *Insects as Vectors of Foodborne Pathogens*

**Tim Grance**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Cyber Security Standards*

**Kelly Grant**, Space and Naval Warfare Systems Center, San Diego, California, *Less Lethal Payloads for Robotic and Automated Response Systems*

**D. Anthony Gray**, Syracuse Research Corporation, North Syracuse, New York, *Sensing Releases of Highly Toxic and Extremely Toxic Compounds*

**Walter M. Grayman**, W.M. Grayman Consulting Engineer, Cincinnati, Ohio, *Designing an Optimum Water Monitoring System; and Prevention of Contamination of Drinking Water in Buildings and Large Venues*

**Brenton C. Greene**, Northrop Grumman Corporation, McLean, Virginia, *President's Commission on Critical Infrastructure Protection*

**Frank W. Griffin**, Sandia National Laboratories, NWS DoD Program Design & Implementation, Albuquerque, New Mexico, *RADAR and LiDAR Perimeter Protection Sensors*

**Neil S. Grigg**, Colorado State University, Fort Collins, Colorado, *Water Infrastructure Interdependencies*

**Gigi Kwik Gronvall**, Center for Biosecurity of the University of Pittsburgh Medical Center, Baltimore, Maryland, *Medical Countermeasures against Emerging Threat Agents*

**Yong Guan**, Iowa State University, Ames, Iowa, *Attack Traceback and Attribution*

**Rebecca Haffenden**, Los Alamos National Laboratory, Los Alamos, New Mexico, *Implications of Regulation on the Protection of Critical Infrastructures*

**Amy D. Hagerman**, Texas A&M University, College Station, Texas, *Economic Impact of a Livestock Attack*

**Yacov Y. Haimes**, Center for Risk Management of Engineering Systems, University of Virginia, Charlottesville, Virginia, *Input–Output Modeling for Interdependent Infrastructure Sectors; and Scenario Analysis, Cognitive Maps, and Concept Maps*

**Virgil B. Hammond**, Argonne National Laboratory, Argonne, Illinois, *Inherently Secure Next-Generation Computing and Communication Networks for Reducing Cascading Impacts*

**Rida Hamza**, Honeywell International, Golden Valley, Minnesota, *Eye and Iris Sensors*

**R. Kevin Hanson**, National Center for Medical Intelligence, Frederick, Maryland, *Foreign Dengue Virus Presents a Low Risk to U.S. Homeland*

**Jiawei Han**, University of Illinois at Urbana-Champaign, Champaign, Illinois, *Classification and Clustering for Homeland Security Applications*

**Pete A. Harlan**, Division of Integrated Biodefense, Imaging Science and Information Systems, Georgetown University Medical Center, Washington, D.C., *Data Sources for Biosurveillance*

**Glen Harrison**, Transportation Policy and Planning Group, Center for Transportation Analysis, Energy and Transportation Science Division, Oak Ridge National Laboratory, Knoxville, Tennessee, *Harden Security of High-Risk and Critical Supply Chains*

**David M. Hartley**, Department of Radiology, Georgetown University School of Medicine, Washington, D.C., *Data Sources for Biosurveillance; and Potential for Human Illness from Animal Transmission or Food-Borne Pathogens*

**Yakir J. Hasit**, CH2M HILL, Philadelphia, Pennsylvania, *Drinking Water Supply, Treatment, and Distribution Practice in the United States*

**Majeed M. Hayat**, Department of Electrical and Computer Engineering and Center for High Technology Materials, University of New Mexico, Albuquerque, New Mexico, *Dynamic Load Balancing for Robust Distributed Computing in the Presence of Topological Impairments; and Spectrally Adaptive Nanoscale Quantum Dot Sensors*

**Edward J. Hecker**, U.S. Army Corps of Engineers, Washington, D.C., *Application of a Conditional Risk Assessment Methodology for Prioritization of Critical Infrastructure*

**Craig Hedberg**, Division of Environmental Health Sciences, University of Minnesota School of Public Health, Minneapolis, Minnesota, *Mitigating Public Health Risks from an Agroterror Attack*

**Christopher D. Hekimian**, DXDT Engineering and Research, LLC, Hagerstown, Maryland, *Terrorist Organizations and Modeling Trends*

**George Hender**, Options Clearing Corporation, Chicago, Ilinois, *Cyber Security for the Banking and Finance Sector*

**Jonathan G. Herrmann**, National Homeland Security Research Center, U.S. Environmental Protection Agency, Cincinnati, Ohio, *Protecting Water Infrastructure in the United States*

**Rex Hesner**, CH2M HILL, Oakland, California, *Drinking Water Supply, Treatment, and Distribution Practice in the United States*

**Susan K. Hinrichs**, University of Illinois at Urbana-Champaign and Network Geographics, Inc., Champaign, Illinois, *Cyber Security Policy Specification and Management*

**Stefan Hirschberg**, Paul Scherrer Institut (PSI), Laboratory for Energy Systems Analysis, Villigen PSI, Switzerland, *Comparative Risk Assessment for Energy Systems: A Tool for Comprehensive Assessment of Energy Security*

**Charles Hofacre**, University of Georgia, Athens, Georgia, *Farm Level Control of Foreign Animal Disease and Food-Borne Pathogens*

**William Hoffman**, Animetrics, Conway, New Hampshire, *2D-To-3D Face Recognition Systems*

**William J. Hoffman**, United States Department of Agriculture, Washington, D.C., *Early Detection and Diagnosis of High-Consequence Plant Pests in the United States*

**Lindsey Holmstrom**, Texas A&M University, College Station, Texas, *Farm Level Control of Foreign Animal Disease and Food-Borne Pathogens*

**Thorsten Holz**, Aachen University, Aachen, Germany, *Advanced Attacker Detection and Understanding with Emerging Honeynet Technologies*

**S. Horikawa**, Materials Engineering, Auburn University, Auburn, Alabama, *General Detector Capabilities for Food Safety Applications*

**Vincent Hu**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Authentication, Authorization, Access Control, and Privilege Management*

**S. Huang**, Materials Engineering, Auburn University, Auburn, Alabama, *General Detector Capabilities for Food Safety Applications*

**William D. Hueston**, Center for Animal Health and Food Safety and National Center for Food Protection and Defense, University of Minnesota, St. Paul, Minnesota, *Livestock Agroterrorism and the Potential Public Health Risk*

**Anne E. Hultgren**, Department of Homeland Security Science and Technology Directorate, Washington, D.C., *Sensing Dispersal of Chemical and Biological Agents in Urban Environments*

**Jeffrey Hunker**, Carnegie Mellon University, Pittsburgh, Pennsylvania, *Policy Development for Homeland Security*

**Regina Hunter**, Sandia National Laboratories, Albuquerque, New Mexico, *Carver+Shock: Food Defense Software Decision Support Tool*

**Rick Hurley**, Sandia National Laboratories, RF and Optics Microsystem Applications, Albuquerque, New Mexico, *RADAR and LiDAR Perimeter Protection Sensors*

**Carolyn M. Hurley**, University of Buffalo, State University of New York, Buffalo, New York, *Training for Individual Differences in Lie Detection Ability*

**Charles K. Huyck**, Imagecat, Inc., Long Beach, California, *Technologies for Real-Time Data Acquisition, Integration, and Transmission*

**Cynthia E. Irvine**, Naval Postgraduate School, Monterey, California, *Multilevel Security*

**Amy I. Ising**, Department of Emergency Medicine, School of Medicine, University of North Carolina, Chapel Hill, North Carolina, *The North Carolina Biosurveillance System*

**Robert W. Ives**, United States Naval Academy, Annapolis, Maryland, *New Approaches to IRIS Recognition: One-Dimensional Algorithms*

**Rich Jackson Jr.**, Chevron Corporation, San Ramon, California, *Industrial Process Control System Security*

**Elizabeth M. Jackson**, George Mason University School of Law, Arlington, Virginia, *Vulnerability Assessment*

**Woo-Yong Jang**, Department of Electrical and Computer Engineering and the Center for High Technology Materials at the University of New Mexico, Albuquerque, New Mexico, *Spectrally Adaptive Nanoscale Quantum Dot Sensors*

**Robert Janke**, U.S. Environmental Protection Agency, Cincinnati, Ohio, *Decontamination Methods for Wastewater and Stormwater Collection and Treatment Systems*

**David A. Jett**, National Institutes of Health/National Institute of Neurological Disorders and Stroke, Bethesda, Maryland, *Biodefense Priorities in Life-Science Research: Chemical Threat Agents*

**Neil F. Johnson**, Booz Allen Hamilton, McLean, Virginia, *Detection of Hidden Information, Covert Channels, and Information Flows*

**David A. Jones**, Argonne National Laboratory, Argonne, Illinois, *President's Commission on Critical Infrastructure Protection*

**J. William Jones**, ASME Innovative Technologies Institute, LLC, Washington, D.C., *Risk Analysis and Management for Critical Asset Protection*

**Mark P. Kaminskiy**, Center for Technology and Systems Management, Department of Civil and Environmental Engineering, University of Maryland, College Park, Maryland, *Modeling Population Dynamics for Homeland Security Applications; and Quantitative Representation of Risk*

**Justin J. Kastner**, Kansas State University, Manhattan, Kansas, *Carcass Disposal Options; The Global Food Supply Chain; and The Role of Food Safety in Food Security*

**Curtis L. Kastner**, Kansas State University, Manhattan, Kansas, *The Role of Food Safety in Food Security*

**Don Kautter**, Food and Drug Administration, Silver Spring, Maryland, *Carver + Shock: Food Defense Software Decision Support Tool*

**Roger L. Kay**, Endpoint Technologies Associates, Inc., Wayland, Massachusetts, *Trusted Platforms: The Root of Security*

**Dan Keller**, Sandia National Laboratories, Strategic Business Enterprise Services, Albuquerque, New Mexico, *RADAR and LiDAR Perimeter Protection Sensors*

**Craig Kiebler**, Georgetown University Medical Center, Argus Research Operations Center, Imaging Science and Information Systems Center, Washington, D.C., *Biosurveillance Tradecraft*

**Robert D. Kirvel**, Lawrence Livermore National Laboratory, Livermore, California, *Health Risk Assessment for Radiological, Chemical, and Biological Attacks*

**Richard Kissel**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Cyber Security Education, Training, and Awareness*

**Greg Kogut**, Space and Naval Warfare Systems Center, San Diego, California, *Less Lethal Payloads for Robotic and Automated Response Systems*

**Bonwoo Koo**, Department of Management Sciences, Faculty of Engineering, University of Waterloo, Ontario, Canada, *The Use of Threat, Vulnerability, and Consequence (TVC) Analysis for Decision Making on the Deployment of Limited Security Resources*

**James F. Kreissl**, Environmental Consultant, Villa Hills, Kentucky, *Homeland Security and Wastewater Treatment*

**Sanjay Krishna**, Department of Electrical and Computer Engineering and the Center for High Technology Materials at the University of New Mexico, Albuquerque, New Mexico, *Spectrally Adaptive Nanoscale Quantum Dot Sensors*

**Radha Krishnan**, Shaw Environmental & Infrastructure, Inc., Cincinnati, Ohio, *Decontamination Methods for Drinking Water Treatment and Distribution Systems*

**Rick Kuhn**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Authentication, Authorization, Access Control, and Privilege Management*

**Howard C. Kunreuther**, Center for Risk Management and Decision Processes, the Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania, *Risk Transfer and Insurance: Insurability Concepts and Programs for Covering Extreme Events*

**David LaFalce**, The Clearing House, New York, New York, *Cyber Security for the Banking and Finance Sector*

**R. S. Lakshmanan**, Materials Engineering, Auburn University, Auburn, Alabama, *General Detector Capabilities for Food Safety Applications*

**Mark Lawley**, Purdue University, West Lafayette, Indiana, *Consequence Mitigation*

**Elizabeth H. Lazzara**, University of Central Florida, Orlando, Florida, *Training and Learning Development for Homeland Security*

**Naomi Lee**, Georgetown University, Washington, D.C., *Social and Psychological Aspects of Terrorism*

**Russell Lee**, Oak Ridge National Laboratory, Oak Ridge, Tennessee, *Transportation Security Performance Measures*

**Earl E. Lee**, University of Delaware, Newark, Delaware, *Network Flow Approaches for Analyzing and Managing Disruptions to Interdependent Infrastructure Systems*

**Seung Hak Lee**, University of Wisconsin, Madison, Wisconsin, *Decontamination and Disposal of Contaminated Foods*

**Vanessa M. Leiby**, The Cadmus Group, Inc., Damascus, Maryland, *Water Supply and Wastewater Management Regulations, Standards, and Guidance*

**Ted G. Lewis**, Center for Homeland Defense and Security, Naval Postgraduate School, Monterey, California, *Critical Infrastructure Protection: Telecommunication*

**Andrew Lewis**, Risk Management Agency, Kansas State University, Manhattan, Kansas, *Optimal Investments in Mitigating Agroterrorism Risks*

**Xiaolei Li**, University of Illinois at Urbana-Champaign, Champaign, Illinois, *Classification and Clustering for Homeland Security Applications*

**Robert M. Liebe**, Innovative Decisions Inc., Vienna, Virginia, *Risk Analysis Frameworks for Counterterrorism*

**Nicholas A. Linacre**, Faculty of Land and Food Resources, the University of Melbourne, Parkville, Victoria, Australia, *The Use of Threat, Vulnerability, and Consequence (TVC) Analysis for Decision Making on the Deployment of Limited Security Resources*

**Eric Lindgren**, Sandia National Laboratories, Albuquerque, New Mexico, *Carver + Shock: Food Defense Software Decision Support Tool*

**Madison Link**, Sandia National Laboratories, Albuquerque, New Mexico, *Carver + Shock: Food Defense Software Decision Support Tool*

**Cheng Liu**, Oak Ridge National Laboratory, Oak Ridge, Tennessee, *Ultra-scale Computing for Emergency Evacuation*

**Douglas G. Luster**, USDA ARS, Fort Detrick, Maryland, *Microbial Forensics and Plant Pathogens: Attribution of Agricultural Crime*

**Duncan R. MacCannell**, Centers for Disease Control and Prevention, Atlanta, Georgia, *Pulsenet: A Program to Detect and Track Food Contamination Events*

**John MacKinney**, U.S. Environmental Protection Agency, Washington, D.C., *Decontamination Methods for Wastewater and Stormwater Collection and Treatment Systems*

**Suzanne M. Mahoney**, Innovative Decisions, Inc., Vienna, Virginia, *Bayesian Networks*

**Marcelo Masera**, European Commission Joint Research Centre, Ispra, Italy, *Critical Infrastructures at Risk: A European Perspective*

**Enrique E. Matheu**, U.S. Department of Homeland Security, Washington, D.C., *Application of a Conditional Risk Assessment Methodology for Prioritization of Critical Infrastructure*

**Lisa J. Mauer**, Department of Food Science, Purdue University, West Lafayette, Indiana, *Mid-Infrared Sensors for the Rapid Analysis of Select Microbial Food-Borne Pathogens*

**Mark Maybury**, Information Technology Center, The MITRE Corporation, Bedford, Massachusetts, *Speech and Video Processing for Homeland Security*

**R. M. Mayo**, U.S. Department of Energy, National Nuclear Security Administration, Washington, D.C., *Radioactive Materials Sensors*

**Amelia D. McCall**, National Homeland Security Research Center, U.S. Environmental Protection Agency, Cincinnati, Ohio, *Protecting Water Infrastructure in the United States*

**Bruce A. McCarl**, Texas A&M University, College Station, Texas, *Economic Impact of a Livestock Attack*

**Andrew W. McCown**, Los Alamos National Laboratory, Threat Reduction Directorate/Decision Applications, Los Alamos, New Mexico, *Interdependent Energy Infrastructure Simulation System*

**Timothy McDaniels**, University of British Columbia, Vancouver, BC, Canada, *Characterizing Infrastructure Failure Interdependencies to Inform Systemic Risk*

**John McFee**, Grand Lake Consulting LLC, Inc., Grand Lake, Colorado, *Decontamination Methods for Drinking Water Treatment and Distribution Systems*

**William L. McGill**, College of Information Sciences and Technology, Pennsylvania State University, University Park, Pennsylvania, *Defeating Surprise Through Threat Anticipation and Possibility Management*

**Jeffrey D. McManus**, The Office of the Secretary of Defense, Washington, D.C., *Protection and Prevention: Threats and Challenges from a Homeland Defense Perspective*

**Ulrich Melcher**, Oklahoma State University, Stillwater, Oklahoma, *Microbial Forensics and Plant Pathogens: Attribution of Agricultural Crime*

**Melissa A. Menasco**, University at Buffalo, State University of New York, Buffalo, New York, *Human Behavior and Deception Detection*

**Mark Merkow**, American Express Company, New York, New York, *Cyber Security for the Banking and Finance Sector*

**Pascal Meunier**, Purdue University CERIAS, West Lafayette, Indiana, *Classes of Vulnerabilities and Attacks*

**Michael D. Meyer**, Georgia Transportation Institute, Georgia Institute of Technology, Atlanta, Georgia, *Transportation System as a Security Challenge*

**Andrea Meyerhoff**, GexGroup Inc, Washington, D.C., and Division of Clinical Pharmacology, Johns Hopkins University School of Medicine, Baltimore, Maryland, *Challenges to Medical Countermeasures against Chemical, Biological, Radiological, and Nuclear (CBRN) Agents*

**Erwann O. Michel-Kerjan**, Center for Risk Management and Decision Processes, the Wharton School, University of Pennsylvania, Philadelphia, Pennsylvania, *Risk Transfer and Insurance: Insurability Concepts and Programs for Covering Extreme Events*

**Michael I. Miller**, Animetrics, Conway, New Hampshire, *2D-To-3D Face Recognition Systems*

**Gay Y. Miller**, University of Illinois, Urbana-Champaign, Illinois,, *Farm Level Control of Foreign Animal Disease and Food-Borne Pathogens*

**Marc A. Mills**, U.S. Environmental Protection Agency, Office of Research and Development, Cincinnati, Ohio, *Homeland Security and Wastewater Treatment*

**Yaroslav Minullin**, IIASA-DYN, Laxenburg, Austria, *Lessons Learned for Regional and Global Energy Security*

**John E. Mitchell**, Rensselaer Polytechnic Institute, Troy, New York, *Network Flow Approaches for Analyzing and Managing Disruptions to Interdependent Infrastructure Systems*

**Charles T. C. Mo**, Northrop-Grumman IT, Los Angeles, California, *Time-Domain Probabilistic Risk Assessment Method for Interdependent Infrastructure Failure and Recovery Modeling*

**Fathali M. Moghaddam**, Georgetown University, Washington, D.C., *Social and Psychological Aspects of Terrorism*

**Hamid Mohtadi**, University of Wisconsin, Milwaukee, Wisconsin and University of Minnesota, Minneapolis, Minnesota, *Developing Risk Metrics to Estimate Risks of Catastrophic Biological and Bioterrorist Events: Applications to the Food Industry*

**Frederick A. Monette**, Argonne National Laboratory, Argonne, Illinois, *Decontamination Methods for Wastewater and Stormwater Collection and Treatment Systems*

**James D. Morgeson**, Institute for Defense Analyses, Alexandria, Virginia, *Application of a Conditional Risk Assessment Methodology for Prioritization of Critical Infrastructure*

**William G. Morris**, General Electric Global Research Center, Niskayuna, New York, *Passive Radio Frequency Identification (RFID) Chemical Sensors for Homeland Security Applications*

**Scott A. Morris**, University of Illinois at Urbana-Champaign, Urbana, Illinois, *Processing and Packaging that Protects the Food Supply Against Intentional Contamination*

**Jianhong Mu**, Texas A&M University, College Station, Texas, *Economic Impact of a Livestock Attack*

**Dale W. Murray**, DoD Security System Analysis Department, Sandia National Laboratories, Albuquerque, New Mexico, *Defending Against Malevolent Insiders Using Access Control*

**Donald E. Neale**, Department of Homeland Security, Washington, D.C., *Vulnerability Assessment*

**Bruce D. Nelson**, Emergency Management Ontario, Ministry of Community Safety and Correctional Services, Toronto, Ontario, Canada, *Managing Critical Infrastructure Interdependencies: The Ontario Approach*

**William Nelson**, FS-ISAC, Dulles, Virginia, *Cyber Security for the Banking and Finance Sector*

**Noele P. Nelson**, Division of Integrated Biodefense, Imaging Science and Information Systems, Georgetown University Medical Center, Washington, D.C., *Data Sources for Biosurveillance*

**William E. Nganje**, Arizona State University, Mesa, Arizona, *Optimal Investments in Mitigating Agroterrorism Risks*

**Kathleen A. Nickel**, National Homeland Security Research Center, U.S. Environmental Protection Agency, Cincinnati, Ohio, *Protecting Water Infrastructure in the United States*

**H. William Niu**, Hamilton Sundstrand Corporation, Pomona, California, *A Tandem Mobility Spectrometer for Chemical Agent and Toxic Industrial Chemical Monitoring*

**James Nutaro**, Oak Ridge National Laboratory, Oak Ridge, Tennessee, *Ultra-scale Computing for Emergency Evacuation*

**Abbey L. Nutsch**, Kansas State University, Manhattan, Kansas, *Carcass Disposal Options; and The Role of Food Safety in Food Security*

**Maureen O'Sullivan**, University of San Francisco, San Francisco, California, *Human Behavior and Deception Detection; and Training for Individual Differences in Lie Detection Ability*

**Sudeshna Pal**, Biosystems and Agricultural Engineering, Michigan State University, East Lansing, Michigan, *Microbiological Biosensors for Food Defense and Safety Applications*

**Rodrigo Palma-Behnke**, Department of Electrical Engineering, University of Chile, Santiago, Chile, *Object-Oriented Approaches for Integrated Analysis of Interdependent Energy Networks*

**John Panchery**, Securities Industry Financial Market Association, New York, New York, *Cyber Security for the Banking and Finance Sector*

**Susmit Panjwani**, University of Maryland, College Park, Maryland, *Risk analysis methods for Cyber Security*

**Michael W. Pariza**, University of Wisconsin, Madison, Wisconsin, *Decontamination and Disposal of Contaminated Foods*

**Roger W. Parker**, DoD Veterinary Food Analysis and Diagnostic Laboratory, Fort Sam Houston, Texas, *Threat from Emerging Infectious Diseases*

**Gregory S. Parnell**, Department of Systems Engineering, United States Military Academy, West Point, New York, and Innovative Decisions Inc., Vienna, Virginia *Logic Trees: Fault, Success, Attack, Event, Probability, and Decision Trees; Multi-objective Decision Analysis; and Risk Analysis Frameworks for Counterterrorism*

**Biliana Paskaleva**, Department of Electrical and Computer Engineering and the Center for High Technology Materials at the University of New Mexico, Albuquerque, New Mexico, *Spectrally Adaptive Nanoscale Quantum Dot Sensors*

**Eric K. Patterson**, Computer Science Department, University of North Carolina Wilmington, Wilmington, North Carolina, *Craniofacial Aging*

**Donald L. Paul**, Chevron Corporation, San Ramon, California, *Industrial Process Control System Security*

**Julie A. Pavlin**, Uniformed Services University of the Health Sciences, Bethesda, Maryland, *ESSENCE: A Practical Systems for Biosurveillance*

**Vincent Pearce**, U.S. Department of Transportation, Washington, D.C., *Emergency Transportation Operations and Control*

**James P. Peerenboom**, Argonne National Laboratory, Argonne, Illinois, *President's Commission on Critical Infrastructure Protection; and System and Sector Interdependencies: An Overview*

**Terry C. Pellmar**, Armed Forces Radiobiology Research Institute, Uniformed Services University of the Health Sciences, Bethesda, Maryland, *Development of Radiation Countermeasures*

**Brian Peretti**, Department of Treasury, Washington, D.C., *Cyber Security for the Banking and Finance Sector*

**D. Brian Peterman**, United States Coast Guard, *Security Assessment Methodologies for U.S. Ports and Waterways*

**Jorge E. Pezoa**, Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, New Mexico, *Dynamic Load Balancing for Robust Distributed Computing in the Presence of Topological Impairments*

**Haishan Piao**, Greater Cincinnati Water Works, Cincinnati, Ohio, *Decontamination Methods for Drinking Water Treatment and Distribution Systems*

**Irwin M. Pikus**, Consultant, Bethesda, Maryland, *President's Commission on Critical Infrastructure Protection*

**Robert Pitt**, University of Alabama, Tuscaloosa, Alabama, *Water Infrastructure and Water Use in the United States*

**Gennady E. Platoff Jr.**, National Institutes of Health/National Institute of Allergy and Infectious Diseases, Bethesda, Maryland, *Biodefense Priorities in Life-Science Research: Chemical Threat Agents*

**Phillip Pohl**, Sandia National Laboratories, Albuquerque, New Mexico, *Carver + Shock: Food Defense Software Decision Support Tool*

**Radislav A. Potyrailo**, General Electric Global Research Center, Niskayuna, New York, *Passive Radio Frequency Identification (RFID) Chemical Sensors for Homeland Security Applications*

**Dennis R. Powell**, Los Alamos National Laboratory, Los Alamos, New Mexico, *Critical Infrastructure Protection Decision Making*

**Robert W. Proctor**, Department of Psychological Sciences, Purdue University, West Lafayette, Indiana, *Human Sensation and Perception*

**Ellen Raber**, Lawrence Livermore National Laboratory, Livermore, California, *Health Risk Assessment for Radiological, Chemical, and Biological Attacks*

**Paul Randall**, U.S. Environmental Protection Agency, Cincinnati, Ohio, *Decontamination Methods for Drinking Water Treatment and Distribution Systems*

**Dorothy A. Reed**, University of Washington, Seattle, Washington, *Characterizing Infrastructure Failure Interdependencies to Inform Systemic Risk*

**Irmak Renda-Tanali**, University of Maryland University College, Adelphi, Maryland, *Terrorist Organizations and Modeling Trends*

**Bradley L. Reuhs**, Department of Food Science, Purdue University, West Lafayette, Indiana, *Mid-Infrared Sensors for the Rapid Analysis of Select Microbial Food Borne Pathogens*

**Edward P. Rhyne**, Department of Homeland Security Science and Technology Directorate, Washington, D.C., *Sensing Dispersal of Chemical and Biological Agents in Urban Environments*

**Efrain M. Ribot**, Centers for Disease Control and Prevention, Atlanta, Georgia, *Pulsenet: A Program to Detect and Track Food Contamination Events*

**Karl Ricanek Jr**, Computer Science Department, University of North Carolina Wilmington, Wilmington, North Carolina, *Craniofacial Aging*

**Steven M. Rinaldi**, Sandia National Laboratories, Albuquerque, New Mexico, *The Military Roots of Critical Infrastructure Analysis and Attack*

**J. A. Roberson**, American Water Works Association, Washington, D.C., *Roles of Federal, State, and Local Authorities in Water Infrastructure Security*

**Marcus K. Rogers**, Purdue University, West Lafayette, Indiana, *Cyber Forensics*

**David Ropeik**, Risk Communication, Ropeik & Associates, Concord, Massachusetts, *Risk Communication—An Overlooked Tool in Combating Terrorism*

**Michael A. Rosen**, Department of Psychology, Institute for Simulation and Training, University of Central Florida, Orlando, Florida, *Naturalistic Decision Making, Expertise, and Homeland Security*

**Eduardo Salas**, Department of Psychology, Institute for Simulation and Training, University of Central Florida, Orlando, Florida, *Naturalistic Decision Making, Expertise, and Homeland Security; and Training and Learning Development for Homeland Security*

**Phil A. Sallee**, Booz Allen Hamilton, McLean, Virginia, *Detection of Hidden Information, Covert Channels, and Information Flows*

**Michael E. Samsa**, Argonne National Laboratory, Argonne, Illinois, *Critical Infrastructure Protection Decision Making*

**William B. Samuels**, Science Applications International Corporation, McLean, Virginia, *Prevention of Contamination of Drinking Water in Buildings and Large Venues*

**Aswin C. Sankaranarayanan**, Center for Automation Research and Department of Electrical and Computer Engineering, University of Maryland, College Park, Maryland, *Knowledge Extraction from Surveillance Sensors*

**Joost R. Santos**, Center for Risk Management of Engineering Systems, University of Virginia, Charlottesville, Virginia, *Input–Output Modeling for Interdependent Infrastructure Sectors*

**Michael Sardelis**, National Center for Medical Intelligence, Frederick, Maryland, *Foreign Dengue Virus Presents a Low Risk to U.S. Homeland*

**Karen Scarfone**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Cyber Security Metrics and Measures; and Cyber Security Standards*

**Leo Schrattenholzer**, Visiting Professor of the Royal Institute of Technology, Sweden, (deceased), *Lessons Learned for Regional and Global Energy Security*

**Paul Schuepp**, Animetrics, Conway, New Hampshire, *2D-To-3D Face Recognition Systems*

**Dan Schutzer**, Financial Services Technology Consortium, New York, New York, *Cyber Security for the Banking and Finance Sector*

**James Scouras**, Defense Threat Reduction Agency, Fort Belvoir, Virginia, *Qualitative Representation of Risk; and Risk Analysis Frameworks for Counterterrorism*

**Yazmin Seda-Sanabria**, U.S. Army Corps of Engineers, Washington, D.C., *Application of a Conditional Risk Assessment Methodology for Prioritization of Critical Infrastructure*

**Amrutha Sethuram**, Computer Science Department, University of North Carolina Wilmington, Wilmington, North Carolina, *Craniofacial Aging*

**Matthew Sexton**, Booz Allen Hamilton, McLean, Virginia, *Wireless Security*

**Shabbir A. Shamsuddin**, Argonne National Laboratory, Argonne, Illinois, *Inherently Secure Next-Generation Computing and Communication Networks for Reducing Cascading Impacts*

**Donna C. Shandle**, Nuclear, Chemical, and Biological Contamination Avoidance, Aberdeen Proving Ground, Maryland, *Design Considerations in Development and Application of Chemical and Biological Agent Detectors*

**John L. Sherwood**, University of Georgia, Athens, Georgia, *Microbial Forensics and Plant Pathogens: Attribution of Agricultural Crime*

**Calvin Shipbaugh**, Arlington, Virginia, *High Consequence Threats: Nuclear*

**Brandon Sights**, Space and Naval Warfare Systems Center, San Diego, California, *Less Lethal Payloads for Robotic and Automated Response Systems*

**Stephan Singleton**, Center for Animal Health and Food Safety, University of Minnesota, St. Paul, Minnesota, *Livestock Agroterrorism and the Potential Public Health Risk*

**Barrett D. Slenning**, Department of Population Health and Pathobiology, College of Veterinary Medicine, North Carolina State University, Raleigh, North Carolina, *Foreign Animal Diseases and Food System Security*

**Edward Small**, Sacramento Metropolitan Fire District, Sacramento, California and FEMA Urban Search and Rescue Team, CA Task Force 7, Sacramento, California, *The Sensor Web: Advanced Technology for Situational Awareness*

**Diana K. Smetters**, PARC, Palo Alto, California, *Cyber Security Technology Usability and Management*

**Edward Smith**, Booz Allen Hamilton, McLean, Virginia, *Wireless Security*

**Gary R. Smith**, Logical Decisions, Fairfax, Virginia, *Qualitative Representation of Risk*

**David Solo**, Corporate Technology Office, Citigroup Inc., New York, New York, *Cyber Security for the Banking and Finance Sector*

**Murugiah Souppaya**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Cyber Security Metrics and Measures*

**Rohini K. Srihari**, University at Buffalo, Buffalo, New York, *Finding Inadvertent Release of Information*

**John A. Stankovic**, University of Virginia, Charlottesville, Virginia, *Security of Distributed, Ubiquitous, and Embedded Computing Platforms*

**Stanley States**, Pittsburgh Water and Sewer Authority, Pittsburgh, Pennsylvania, *Surveillance Methods and Technologies for Water and Wastewater Systems*

**D. L. Stephens**, Pacific Northwest National Laboratory, Richland, Washington, *Radioactive Materials Sensors*

**Catherine H. Strohbehn**, Iowa State University, Ames, Iowa, *Risk Assessment, Risk Management, and Preventive Best Practices for Retailers and Foodservice Establishments*

**Makram T. Suidan**, University of Cincinnati, Cincinnati, Ohio, *Homeland Security and Wastewater Treatment*

**John Sullivant**, $S^3E$–Sisters Three Entrepreneurs Security Consultants Company, West Hollywood, California and Magallanes Associates International (MAI), Thousand Oaks, California, *Strategies for Protecting the Telecommunications Sector*

**Cheryl Surman**, General Electric Global Research Center, Niskayuna, New York, *Passive Radio Frequency Identification (RFID) Chemical Sensors for Homeland Security Applications*

**Ivan Susanto**, Chevron Corporation, San Ramon, California, *Industrial Process Control System Security*

**Manuel Suter**, Center for Security Studies (CSS), ETH Zurich, Switzerland, *Australia; Austria; Brazil; Canada; Estonia; Finland; France; Germany; Hungary; India; Italy; Japan; Republic of Korea; Malaysia; the Netherlands; New Zealand; Norway; Poland; Russia; Singapore; Spain; Sweden; Switzerland; United Kingdom; United States; European Union (EU); The Forum of Incident Response and Security Teams (FIRST); Group of Eight (G8); North Atlantic Treaty Organization (NATO); Organization for Economic Co-Operation and Development (OECD); United Nations (UN); and the World Bank Group*

**Andrew W. Szumlas**, Hamilton Sundstrand Corporation, Pomona, California, *A Tandem Mobility Spectrometer for Chemical Agent and Toxic Industrial Chemical Monitoring*

**Joseph A. Tatman**, Innovative Decisions, Inc., Vienna, Virginia, *Bayesian Networks*

**Lisa Theisen**, Contraband Detection, Sandia National Laboratories, Albuquerque, New Mexico, *Threat Signatures of Explosive Materials*

**Ken Thompson**, CH2M HILL, Englewood, Colorado, *Drinking Water Supply, Treatment, and Distribution Practice in the United States*

**Jimmy L. Tickel**, Emergency Programs Division, North Carolina Department of Agriculture and Consumer Services, Raleigh, North Carolina, *Foreign Animal Diseases and Food System Security*

**G. Loren Toole**, Los Alamos National Laboratory, Threat Reduction Directorate/Decision Applications, Los Alamos, New Mexico, *Interdependent Energy Infrastructure Simulation System*

**Edward T. Toton**, Toton, Incorporated, Reston, Virginia, *Defending Against Directed Energy Weapons: RF Weapons and Lasers*

**Wade R. Townsend**, U.S. Department of Homeland Security, Washington, D.C., *Vulnerability Assessment Methodologies for Interdependent Systems*

**Monique Mitchell Turner**, Center for Risk Communication Research, Department of Communication, University of Maryland, College Park, Maryland, *Risk Communication*

**Shawn S. Turner**, United States Marine Corps, Arlington, Virginia, *Risk Communication*

**Marc Vaillant**, Animetrics, Conway, New Hampshire, *2D-To-3D Face Recognition Systems*

**Luis S. Vargas**, Department of Electrical Engineering, University of Chile, Santiago, Chile, *Object-Oriented Approaches for Integrated Analysis of Interdependent Energy Networks*

**Ashok Veeraraghavan**, Center for Automation Research and Department of Electrical and Computer Engineering, University of Maryland, College Park, Maryland, *Knowledge Extraction from Surveillance Sensors*

**Kim-Phuong L. Vu**, Department of Psychology, California State University, Long Beach, California, *Human Sensation and Perception*

**William A. Wallace**, Rensselaer Polytechnic Institute, Troy, New York, *Network Flow Approaches for Analyzing and Managing Disruptions to Interdependent Infrastructure Systems*

**Anna E. Waller**, Department of Emergency Medicine, School of Medicine, University of North Carolina, Chapel Hill, North Carolina, *The North Carolina Biosurveillance System*

**Ronald A. Walters**, Pacific Northwest National Laboratory, Richland, Washington, *Biosurveillance Tradecraft; and Data Sources for Biosurveillance*

**Enoch Wang**, Intelligence Community, Washington, D.C., *Nano-Enabled Power Sources*

**Keith B. Ward**, Department of Homeland Security Science and Technology Directorate, Washington, D.C., *Sensing Dispersal of Chemical and Biological Agents in Urban Environments*

**Linda Warren**, Launch Consulting, Richland, Washington, *Emergency Response Planning for Drinking Water Systems*

**David M. Weinberg**, Practical Risk LLC, Rio Rancho, New Mexico, *Threats and Challenges to Homeland Security*

**Rand Whillock**, Honeywell International, Golden Valley, Minnesota, *Eye and Iris Sensors*

**Jack F. Williams**, Georgia State University, Atlanta, Georgia, *Terrorist Threat Analysis*

**Cecelia Williams**, Sandia National Laboratories, Albuquerque, New Mexico, *Carver + Shock: Food Defense Software Decision Support Tool*

**Henry H. Willis**, RAND Corporation, Pittsburgh, Pennsylvania, *Using Risk Analysis to Inform Intelligence Analysis*

**Mark Wilson**, National Institute of Standards and Technology, Gaithersburg, Maryland, *Cyber Security Education, Training, and Awareness*

**James M. Wilson**, Georgetown University Medical Center, Argus Research Operations Center, Imaging Science and Information Systems Center, Washington, D.C., *Biosurveillance Tradecraft*

**William Wilson**, North Dakota State University, Fargo, North Dakota, *Optimal Investments in Mitigating Agroterrorism Risks*

**Gordon Woo**, Risk Management Solutions, London, United Kingdom, *Terrorism Risk*

**Anthony D. Wood**, University of Virginia, Charlottesville, Virginia, *Security of Distributed, Ubiquitous, and Embedded Computing Platforms*

**Jon Woody**, Food and Drug Administration, Silver Spring, Maryland, *Carver + Shock: Food Defense Software Decision Support Tool*

**Ken Wright**, Depository Trust and Clearing Corporation, New York, New York, *Cyber Security for the Banking and Finance Sector*

**Lorna Zach**, Center for Human Performance and Risk Analysis, University of Wisconsin-Madison, Madison, Wisconsin, *Risk Assessment and Safety of the Food Supply*

**Thomas Zacharia**, Oak Ridge National Laboratory, Oak Ridge, Tennessee, *Ultra-scale Computing for Emergency Evacuation*

**Linfeng Zhang**, Iowa State University, Ames, Iowa, *Attack Traceback and Attribution*

**Rae Zimmerman**, Institute for Civil Infrastructure Systems (ICIS), New York University, Wagner Graduate School of Public Service, New York, New York, *Understanding the Implications of Critical Infrastructure Interdependencies for Water*

**Ludek Zurek**, Kansas State University, Departments of Entomology and Diagnostic Medicine and Pathobiology, Manhattan, Kansas, *Insects as Vectors of Foodborne Pathogens*

# INDEX